NovaScale 9006 Server Hardware Console

User's Guide

NOVASCALE

REFERENCE
86 A1 70FA 00

NOVASCALE

NovaScale 9006 Server Hardware Console

User's Guide

Hardware

September 2009

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 70FA 00

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of NEC Computers and/or its licensors. NEC Computers and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC Computers is prohibited.

The Bull product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by Bull.

Trademarks

NEC ESMPRO, NEC DianaScope, NEC MWA, and ExpressBuilder are trademarks or registered trademarks of NEC Corporation.

NovaScale is a registered trademark of Bull SAS.

Adobe, and Adobe Acrobat are registered trademarks of Adobe Systems, Incorporated.

Microsoft, Microsoft Windows, Windows NT, Windows 95, Windows 98, Windows2000 and Windows Server 2003 are all registered trademarks of Microsoft Corporation.

MS-DOS is a registered trademark of Microsoft Corporation.

Intel and Xeon are registered trademarks of Intel Corporation.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

Suggestions and criticisms concerning the form, content, and presentation of this manual are invited. A form is provided at the end of this manual for this purpose.

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

Table of Contents

List of Figures

List of Tables

Legal Information

Regulatory Declarations and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with:

- European Union EMC Directive 2004/108/EC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 2006/95/EC, using standard EN60950
- International Directive IEC 60297 and US ANSI Directive EIA-310-E

Safety Compliance Statement

- UL 60950 (USA)
- IEC 60950 (International)
- CSA 60950 (Canada)

European Community (EC) Council Directives

This product is in conformity with the protection requirements of the following EC Council Directives:

Electromagnetic Compatibility

- 2004/108/EC

Low Voltage

- 2006/95/EC

EC Conformity

- 93/68/EEC

Telecommunications Terminal Equipment

- 1999/5/EC

Neither the provider nor the manufacturer can accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

Compliance with these directives requires:

- An EC declaration of conformity from the manufacturer
- An EC label on the product
- Technical documentation

Mechanical Structures

- IEC 60297
- EIA-310-E

FCC Declaration of Conformity

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer are responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Pursuant to Part 15.21 of the FCC Rules, any changes or modifications to this equipment not expressly approved by Bull SAS may cause harmful interference and void the FCC authorization to operate this equipment.

An FCC regulatory label is affixed to the equipment.

Canadian Compliance Statement (Industry Canada)

This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This product is in conformity with the protection requirements of the following standards:

- ICES-003
- NMB-003

Laser Compliance Notice (if applicable)

This product that uses laser technology complies with Class 1 laser requirements.

A CLASS 1 LASER PRODUCT label is affixed to the laser device.

Class 1 Laser Product
Luokan 1 Laserlaite
Klasse 1 Laser Apparat
Laser Klasse 1

Safety Information

Definition of Safety Notices

DANGER
A *Danger* notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

CAUTION
A *Caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

WARNING
A *Warning* notice indicates an action that could cause damage to a program, device, system, or data.

Electrical Safety

The following safety instructions shall be observed when connecting or disconnecting devices to the system.

DANGER
The Customer is responsible for ensuring that the AC electricity supply is compliant with national and local recommendations, regulations, standards and codes of practice.
An incorrectly wired and grounded electrical outlet may place hazardous voltage on metal parts of the system or the devices that attach to the system and result in an electrical shock.
It is mandatory to remove power cables from electrical outlets before relocating the system.

CAUTION
This unit has more than one power supply cable. Follow procedures for removal of power from the system when directed.

Laser Safety Information (if applicable)

The optical drive in this system unit is classified as a Class 1 level Laser product. The optical drive has a label that identifies its classification.

The optical drive in this system unit is certified in the U.S. to conform to the requirements of the Department of Health and Human Services 21 Code of Federal Regulations (DHHS 21 CFR) Subchapter J for Class 1 laser products. Elsewhere, the drive is certified to conform to the requirements of the International Electrotechnical Commission (IEC) 60825-1: 2001 and CENELEC EN 60825-1: 1994 for Class 1 laser products.

CAUTION
Invisible laser radiation when open. Do not stare into beam or view directly with optical instruments.

Class 1 Laser products are not considered to be hazardous. The optical drive contains internally a Class 3B gallium-arsenide laser that is nominally 30 milliwatts at 830 nanometers. The design incorporates a combination of enclosures, electronics, and redundant interlocks such that there is no exposure to laser radiation above a Class 1 level during normal operation, user maintenance, or servicing conditions.

Data Integrity and Verification

WARNING
Bull product are designed to reduce the risk of undetected data corruption or loss. However, if unplanned outages or system failures occur, users are strongly advised to check the accuracy of the operations performed and the data saved or transmitted by the system at the time of outage or failure.

Waste Management

This product has been built to comply with the Restriction of Certain Hazardous Substances (RoHS) Directive 2002/95/EC.

This product has been built to comply with the Waste Electrical and Electronic (WEEE) Directive 2002/96/EC.

Preface

This guide explains how to use the Hardware Console to manage your server.

Note The Bull Support Web site may be consulted for product information, documentation, updates and service offers:
http://support.bull.com

Intended Readers

This guide is intended for use by Bull System Administrators and Operators.

Highlighting

The following highlighting conventions are used in this guide:

Bold	Identifies the following: • Interface objects such as menu names, labels, buttons and icons. • File, directory and path names. • Keywords to which particular attention must be paid.
Italics	Identifies references such as manuals or URLs.
`monospace`	Identifies portions of program codes, command lines, or messages displayed in command windows.
< >	Identifies parameters to be supplied by the user.
⧉	Identifies the FRONT of a component.
⧉	Identifies the REAR of a component.

Related Publications

- *Site Preparation Guide,* 86A140FA
  explains how to prepare a Data Processing Center for Bull Systems, in compliance with the standards in force. This guide is intended for use by all personnel and trade representatives involved in the site preparation process.
- *NovaScale 9006 Server Installation Guide,* 86A169FA
  explains how to install and start the server for the first time. This guide is intended for use by qualified support personnel.
- *NovaScale 9006 Service Guide*, 86A768FA
  explains how to service the server. This guide is intended for use by qualified support personnel.
- *iCare Console User's Guide,* 86A171FA
  explains how to use the console to monitor and maintain Bull Systems. This guide is intended for use by Bull System Administrators and Operators and qualified support personnel.
- *Resource and Documentation CD*
  contains the tools and documentation required to configure, operate and maintain the equipment.

Chapter 1. Getting Started

This chapter describes Hardware Console features and explains how to start and stop the console from a Web browser. It includes the following topics:

- Starting the Hardware Console, on page 1-2
- Hardware Console Overview, on page 1-4
- Stopping the Hardware Console, on page 1-7
- Initial Configuration, on page 1-7
- Configuration Data Backup/Restore Tool, on page 1-8

1.1. Starting the Hardware Console

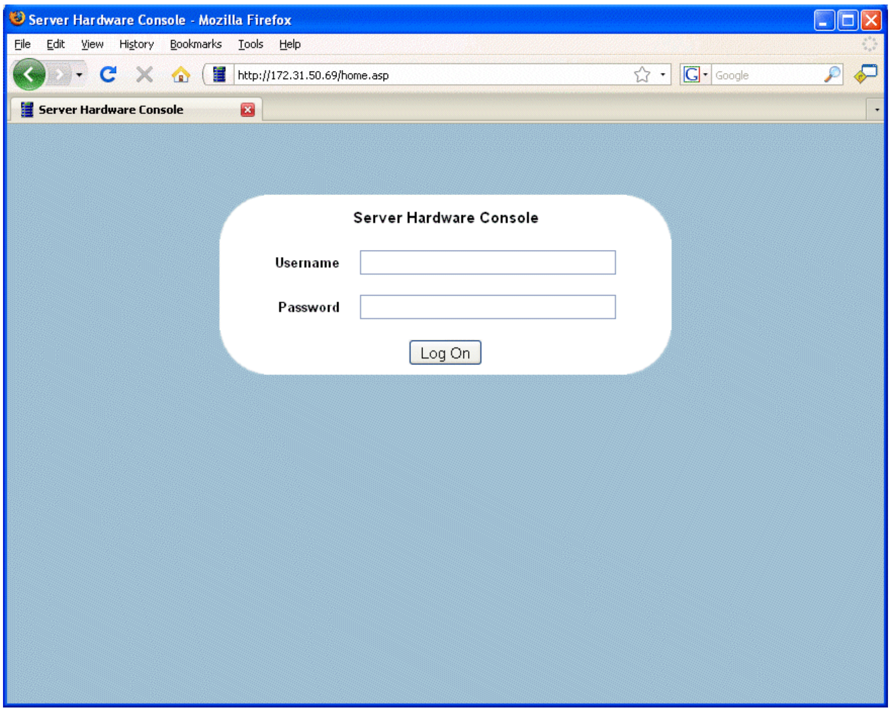
The hardware console is launched from a web browser using a standard or secure IP address or host name, according to settings.

Prerequisites

- The server is connected to the site power supply and to the enterprise LAN.

Procedure

1. Launch your web browser and and enter the standard or secure IP address or host name, according to settings. The authentication page opens.



Hardware Console	
Username	Factory-default name: **super**
Password	Factory-default password: **pass**

Figure 1. Authentication page description

2. Complete the **Username and Password** fields and click **Log On**. Once you are authenticated, the **Power Management** page opens.

Important **It is strongly recommended to change the factory-default super user password once initial setup is completed, taking care to record your new account details for subsequent connections. You are advised to use the same password for all your managed resources. This will enable you to interface easily with the iCare Console.**
If you lose your account details and are unable to connect to the console, please contact your Customer Service Representative.

Related Topics

- Modifying your Password, on page 4-24
- Stopping the Hardware Console, on page 1-7
- Configuring or Modifying Network Settings, on page 4-4
- Enabling/Disabling Encryption, on page 4-33

What To Do if an Incident Occurs?

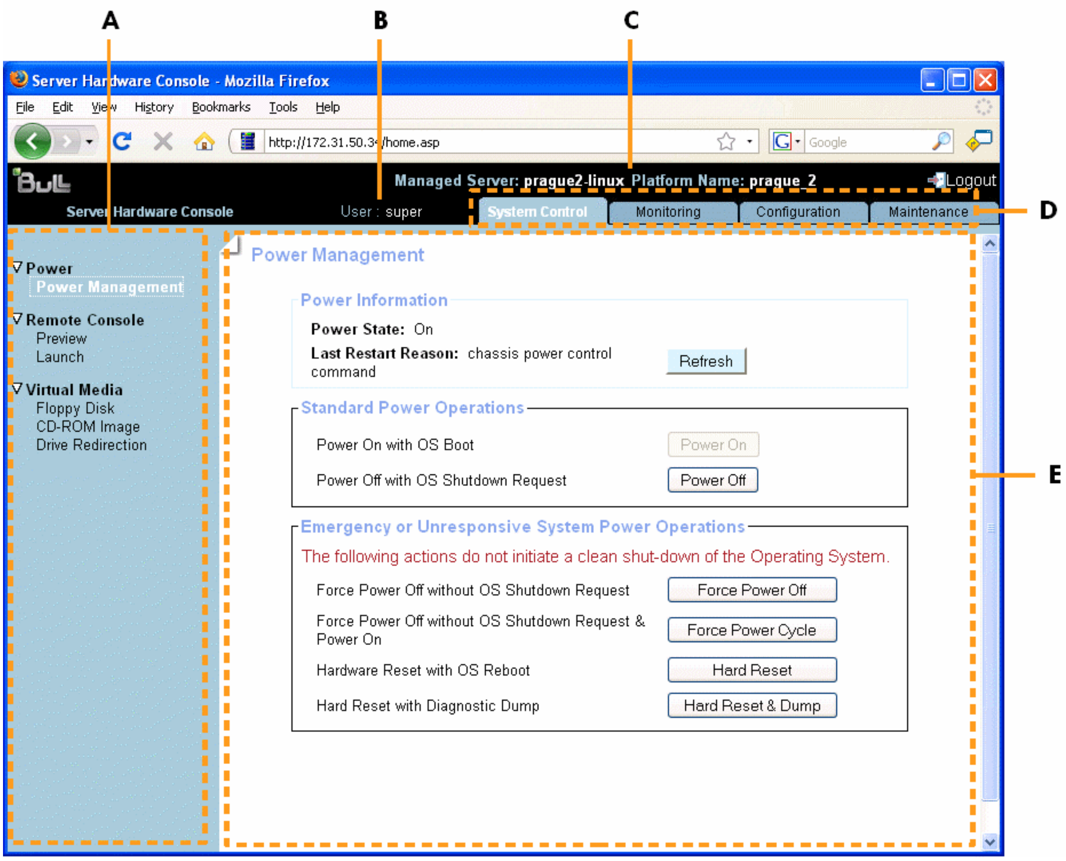
If you cannot connect to the console or if the web pages are displayed incorrectly, one of the following problems may be the cause:

- Network failure.
- Incorrect network settings.
- Incorrect browser settings (proxy configuration).

1.2. Hardware Console Overview

The Hardware Console is a web-based administration application embedded on the I/O Legacy Board (ILB). It allows you to remotely operate, monitor and configure your server via the enterprise LAN using a Microsoft Internet Explorer or Mozilla Firefox browser.

Important **Several users can access the hardware console simultaneously. If configuration changes are made, they may not be visible to other users unless they refresh the hardware console display. You can view the list of connected users by selecting Maintenance Operations > Connected Users.**


A
B
C
D
E
Server Hardware Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.31.50.3/home.asp
Google
BULL
Server Hardware Console
Logout
System Control
Monitoring
Configuration
Maintenance
Power
Power Management
Remote Console
Preview
Launch
Virtual Media
Floppy Disk
CD-ROM Image
Drive Redirection
Power Management
Power Information
Refresh
Standard Power Operations
Power On with OS Boot
Power On
Power Off with OS Shutdown Request
Power Off
Emergency or Unresponsive System Power Operations
Force Power Off without OS Shutdown Request
Force Power Off
Force Power Off without OS Shutdown Request & Power On
Force Power Cycle
Hardware Reset with OS Reboot
Hard Reset
Hard Reset with Diagnostic Dump
Hard Reset & Dump

Managed Server: prague2-linux Platform Name: prague_2

User : super

Power State: On

Last Restart Reason: chassis power control command

The following actions do not initiate a clean shut-down of the Operating System.

Hardware Console Overview	
A: Navigation tree	The navigation tree provides access to console features. Note that displayed features differ according to the tab selected.
B	User logon name
C	Name given to the server for easy identification
D: Tabs	Four tabs allow access to four families of features accessible from the associated navigation trees: **System Control**, **Monitoring**, **Configuration** and **Maintenance**.
E: Work pane	The work pane displays the commands and information associated with the item selected in the navigation tree.

Figure 2. Hardware Console overview

Hardware Console Interface Features

The following table lists the features available from the interface and the permissions required to use them.

Tab	Tree Node		Feature	Permission
System Control	Power	Power Management	Power Information	*None*
			Standard Power Operations	Power Control
			Emergency Power Operations	
	Remote Console	Preview	Preview	Remote Control Access
		Launch	-	Remote Control Access
	Virtual Media	Floppy Disk	Floppy Image Upload	Virtual Media Upload
		CD-ROM Image	Microsoft Windows Share Image	
		Drive Redirection	Drive Redirection	
		Options	Virtual Media Options	
Monitoring	System Health	Sensors	Sensor Status	*None*
		System Event Log	Viewing and Refreshing	
			Clearing	Alert Settings & Clear SEL
		Messages	Viewing and Clearing	Security/Log/Authentication
Configuration	Global Settings	Platform	Platform Settings	Network Settings
		Managed Server	Managed Server Name	
	BMC Settings	Network	Network Settings	Network Settings SSH/Telnet Access (necessary to use options available in the Network Settings page)
		Date-Time	Date-Time Settings	Date/Time Settings
		SNMP	SNMP Settings	SNMP Settings
		Messages	Board, Security & Remote Console Message Settings	Security/Log/Authentication
	BMC User Management	Users	User Management	User/Group Management
		Groups	Group Management	
		Password	Password Management	Change Password
	Security	Encryption	Encryption Management	Security/Log/Authentication
		SSL Certificate	SSL Certificate Management	SSL Certificate Management
		User Logon Policy	User Logon Policy Management	Security/Log/Authentication
		Authentication	Authentication Management	
		Power Button Lockout	Power Button Lockout Management	Security/Log/Authentication
		User Lockout	User Lockout Management	Security/Log/Authentication

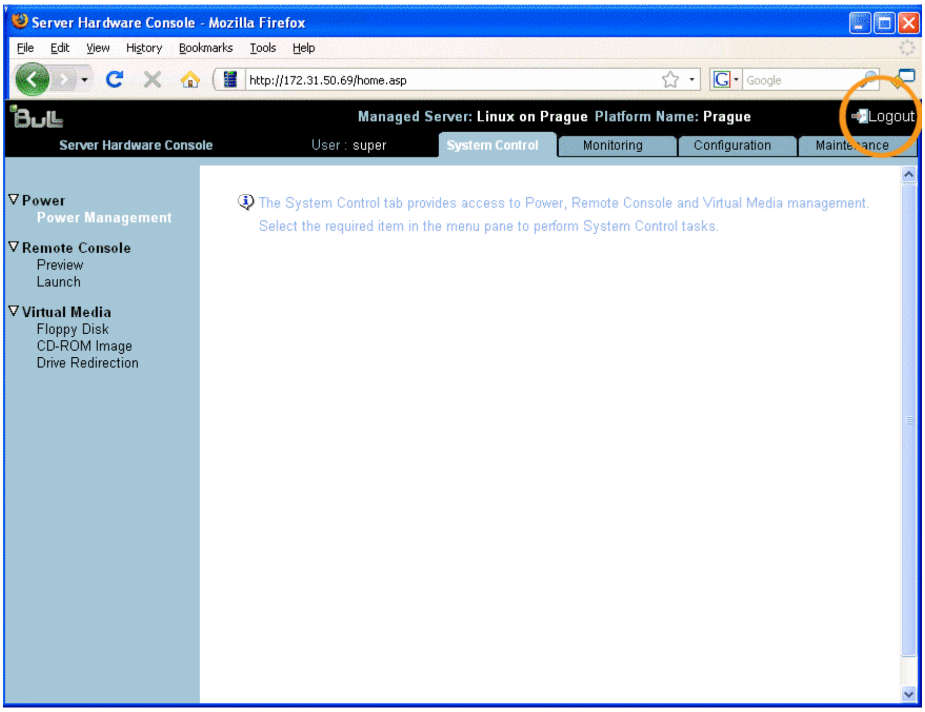
Tab	Tree Node		Feature	Permission
Configuration	Remote Console Settings	User Specific	User Specific RC Settings	Remote Console Access
			Transmission Encoding	RC Settings (Encoding)
			Miscellaneous RC Settings	RC Settings (Exclusive Access)
			Mouse Hotkey	RC Settings (Hotkeys)
			Remote Console Button Key	RC Settings (Monitor Mode)
		Keyboard/Mouse	Keyboard/Mouse	RC Keyboard/Mouse Settings
	Alert Settings	Filters	Filter Settings	Alert Settings & Clear SEL
		Policies	Policy Settings	
		LAN Destinations	LAN Destination Settings	
		General	General Settings	
Maintenance	Hardware Information	Management Board	Management Board Information	*None*
		FRU	FRU Information	
		Firmware Version	Firmware Information	
	Firmware Update	*Listed firmware (MBC, MTBC...)*	Firmware Upload	Firmware Update
	Maintenance Operations	Unit Reset	Reset Operations	Maintenance/Board Reset
		Identification LED	ID LED Management	Alert Settings & Clear SEL
		Hardware Exclusion	Hardware Exclusions	Maintenance/Board Reset
		Connected Users	Connected Users Information	*None*

Table 1. Interface features and permissions

1.3. Stopping the Hardware Console

Procedure

You can stop the console at any time by clicking the **Logout** link in the upper-right corner of the console:



The System Control tab provides access to Power, Remote Console and Virtual Media management. Select the required item in the menu pane to perform System Control tasks.

Figure 3. Logout link

Related Topics

- Starting the Hardware Console, on page 1-2

1.4. Initial Configuration

When the server is first delivered, you will need to perform a few basic configuration tasks to ensure correct operation and identification by management software. These configuration tasks are explained in detail in Chapter 4. Configuring the Server Embedded Management Controller and are listed below by order of priority:

- Configuring or Modifying Network Settings, on page 4-4
- Configuring Platform Identification Settings, on page 4-2
- Setting the Managed Server Name, on page 4-3
- Modifying Internal Clock Settings, on page 4-7
- Configuring Remote System Console Settings, on page 4-43

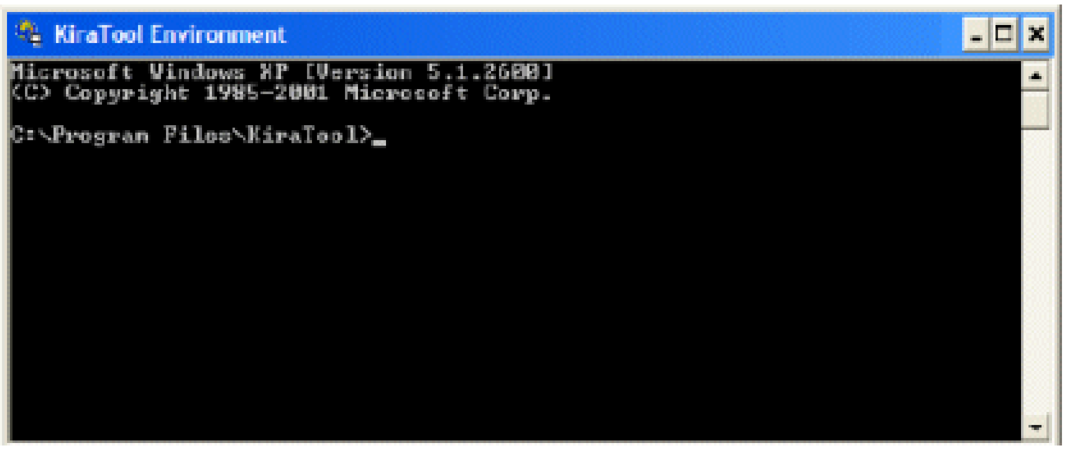
Note The other configuration tasks detailed in Chapter 4. can be performed when required.

1.5. Configuration Data Backup/Restore Tool

A *KiraTool Environment utility* allowing you to backup and restore your configuration data is available on the *Resource and Documentation CD*.

To install this utility, just copy the executable file to your hard disk and invoke it from there.

Once you have installed the *KiraTool Environment utility*, the KiraTool Environment icon will appear on your desktop. Double-clicking this icon will open the KiraTool Environment dialogue box.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\KiraTool>_
```

Figure 4. KiraTool Environment utility

Refer to the associated *KiraTool Environment utility* documentation for further information.

Chapter 2. Using Server Controls

This chapter explains how to use server controls. It includes the following topics:

- Using Server Power Management Features, on page 2-2
- Using the Remote System Console, on page 2-12

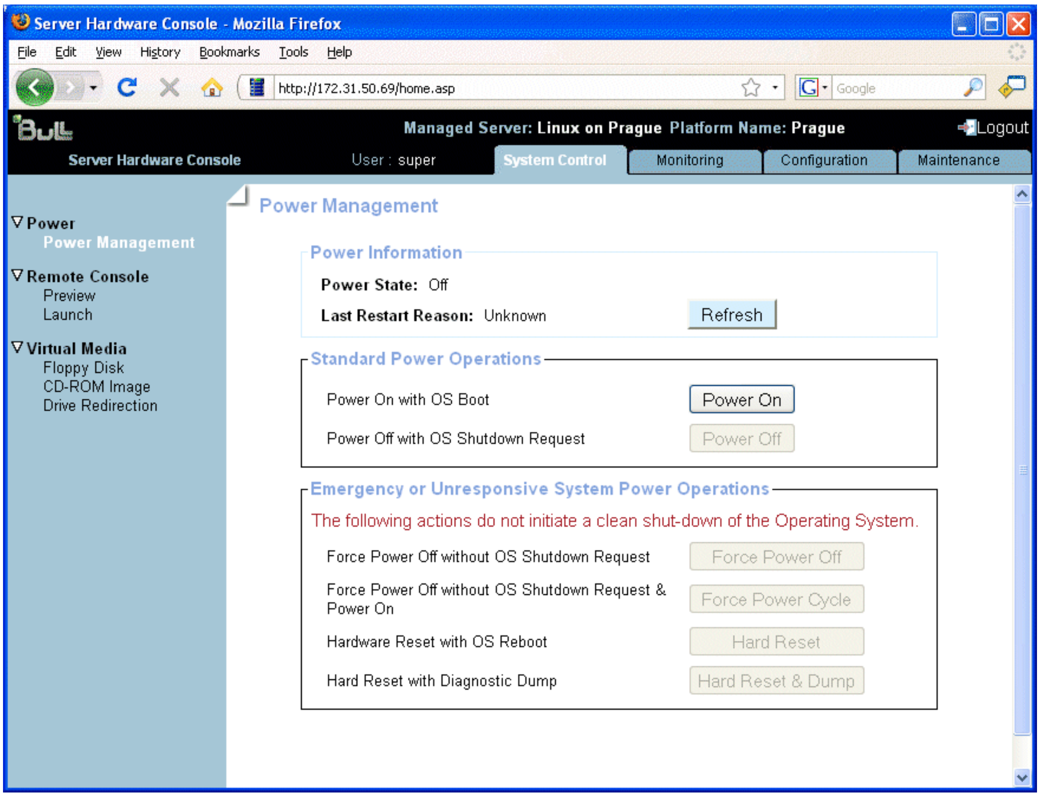
2.1. Using Server Power Management Features

The **Power Management** page allows you to check system power status, perform standard power on and power off sequences, and forcibly power off and/or retrieve the system after a crash or in the event of an emergency.

Power management options are described in Figure 5 below.

Procedure

- From the **System Control** tab, click **Power > Power Management** to open the **Power Management** page.



Managed Server: Linux on Prague Platform Name: Prague

User : super

Power Management

Power Information

Power State: Off

Last Restart Reason: Unknown

Standard Power Operations

Power On with OS Boot

Power Off with OS Shutdown Request

Emergency or Unresponsive System Power Operations

The following actions do not initiate a clean shut-down of the Operating System.

Force Power Off without OS Shutdown Request

Force Power Off without OS Shutdown Request & Power On

Hardware Reset with OS Reboot

Hard Reset with Diagnostic Dump

The **Power Management** page is divided into three areas:

- Power Information
  used to check system power status.

- Standard Power Operations
  used to perform routine power on / off sequences.

- Emergency or Unresponsive System Power Operations
  used to perform power on / off sequences after a system crash or in the event of an emergency.

Power Information Box	
Power State	2 possible values: • **On** • **Off**
Last Restart Reason	Several possible values expliciting which action last caused a restart.
Refresh button	Allows you to update displayed data.
Standard Power Operations Box	
Power On button	Accessible only when the system is powered off. Launches the power up sequence. During this sequence, hardware is powered up from the standby power mode to the main power mode and the Operating System is booted. Note: If an error occurs during this sequence, the system is automatically powered down to standby.
Power Off button	Accessible only when the system is powered on. Requests the Operating System to perform a graceful power down. During this sequence the Operating System saves data, closes open applications and shuts down, and hardware is powered down from the main power mode to the standby power mode. Note: The Operating System must be configured to accept the power off request.
Emergency or Unresponsive System Power Operations Box	
Important: **These buttons should only be used if the Operating System is unable to respond to a standard (graceful) power off request. These sequences may result in data loss and file corruption.**	
Force Power Off button	Performs a power down sequence independently of the Operating System.
Force Power Cycle button	Performs a power down sequence independently of the Operating System and automatically re-launches the powering up sequence.
Hard Reset button	Performs a power cycle (power off / power on) sequence independently of the Operating System and is used as a last resort to forcibly retrieve the system when it freezes. All cache information is erased.
Hard Reset & Dump button	Writes a crash dump and then performs a power cycle (power off / on) independently of the Operating System. All cache information is written to the dump file and can be used for problem analysis.

Figure 5. Power Management page

Related Topics

- Viewing Server Power Status, on page 2-4
- Powering On the Server, on page 2-6
- Powering Off the Server, on page 2-8
- Forcibly Powering Off / Resetting the Server, on page 2-10

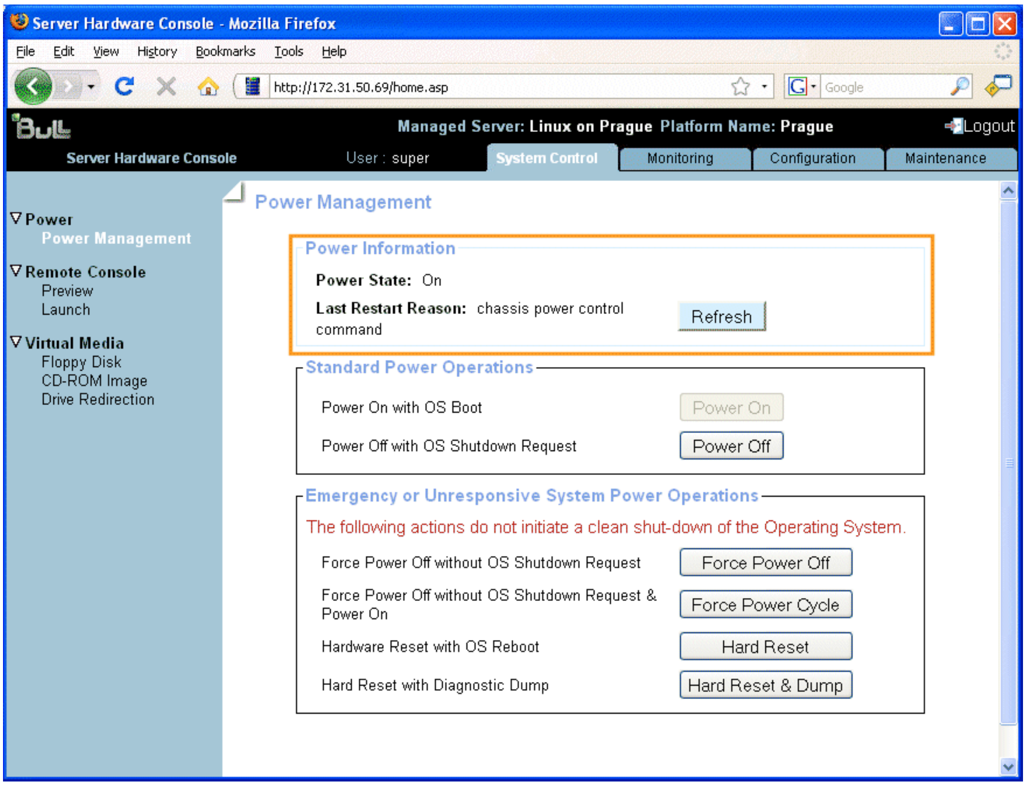
2.1.1. Viewing Server Power Status

System power status can be checked at all times from the **Power Management** page **Power Information** box.

Important **The Power status display is not updated dynamically, therefore displayed status may not reflect actual status. You can update power status by using the Refresh button.**

Procedure

- From the **System Control** tab, click **Power** > **Power Management** to open the **Power Management** page.



Managed Server: Linux on Prague Platform Name: Prague

User : super

Power Management

Power Information

Power State: On

Last Restart Reason: chassis power control command

Standard Power Operations

Power On with OS Boot

Power Off with OS Shutdown Request

Emergency or Unresponsive System Power Operations

The following actions do not initiate a clean shut-down of the Operating System.

Force Power Off without OS Shutdown Request

Force Power Off without OS Shutdown Request & Power On

Hardware Reset with OS Reboot

Hard Reset with Diagnostic Dump

Power Information Box
Note: For details on other power management features, see Figure 5, on page 2-3.

Power Information Box (continued)	
Power State	2 possible values: • On • Off
Last Restart Reason	Several possible values expliciting which action last caused a restart, as detailed in Table 2 below.
Refresh button	Allows you to update displayed data.

Figure 6. Power Information box

The following table details the values that may potentially appear in the **Last Restart Reasons** field of the **Power Information** box.

Last Restart Reason	Explanation
Chassis power control command	The server was restarted from the Hardware Console or by IPMITOOL via the LAN.
Reset via push button	The server was reset with the Server Drawer pushbutton.
Power-up via push button	The server was restarted with the Server Drawer pushbutton.
Watchdog expired	The server was automatically restarted when the IPMI watchdog time expired.
Reset via PEF (Platform Event Filtering)	The server was reset further to the transmission of an event configured to automatically perform the reset action.
Power-cycle via PEF	The server was power-cycled further to the transmission of an event configured to automatically perform the power-cycle action.
Power-up due to always-restore power policy	The server was automatically restarted when AC power was applied or returned after a power cut, in compliance with system power management settings.
Power-up due to restore-previous power policy	The server was automatically restarted when AC power was applied or returned after a power cut, in compliance with system power management settings.
OEM	The server was automatically restarted further to the reception of a Wake-on-LAN signal.

Table 2. Power Information box - potential last restart reasons

Related Topics

- Powering On the Server, on page 2-6
- Powering Off the Server, on page 2-8
- Forcibly Powering Off / Resetting the Server, on page 2-10

2.1.2. Powering On the Server

The system can be powered on from the **Power Management** page **Standard Operations** box.

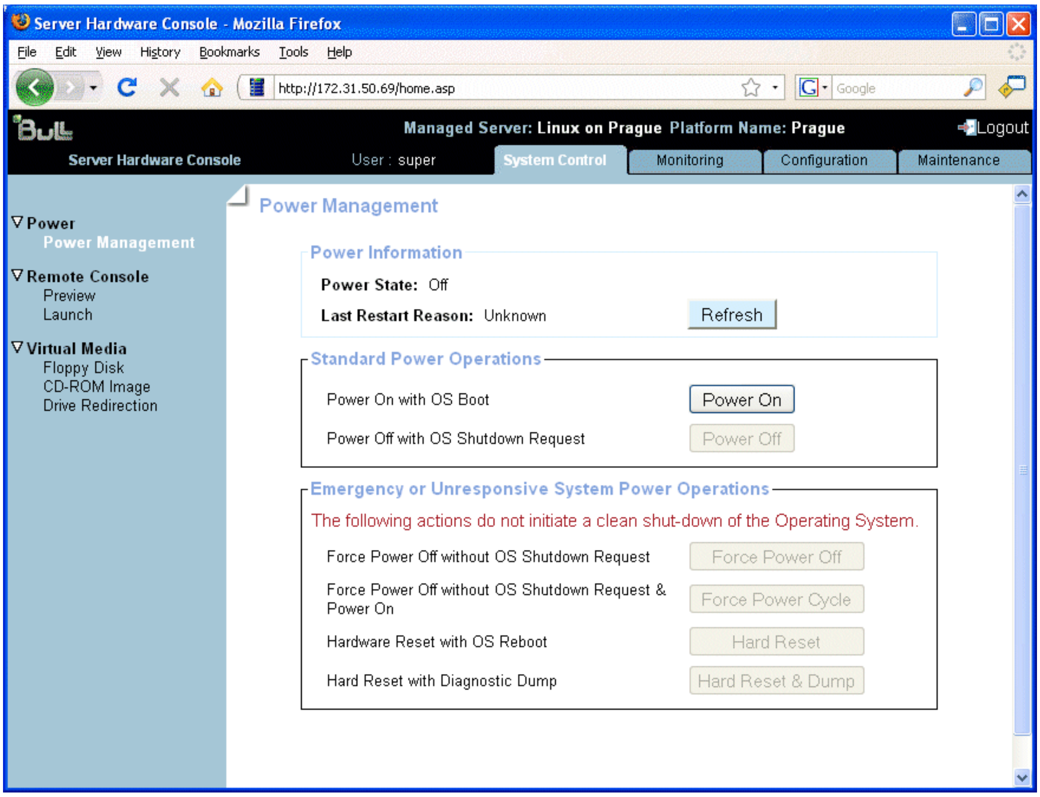
Important **The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and the Power On button may not be enabled although the system is powered off. You can update power status by using the Refresh button.**

Prerequisites

- You have **Power Control** permission.
- The **Power On** button is enabled.

Procedure

1. From the **System Control** tab, click **Power** > **Power Management** to open the **Power Management** page.



Power State: Off

Last Restart Reason: Unknown

Power On with OS Boot

Power Off with OS Shutdown Request

The following actions do not initiate a clean shut-down of the Operating System.

Force Power Off without OS Shutdown Request

Force Power Off without OS Shutdown Request & Power On

Hardware Reset with OS Reboot

Hard Reset with Diagnostic Dump

Standard Power Operations Box	
Note: For details on other power management features, see Figure 5, on page 2-3.	
Power On button	Launches the power up sequence. During this sequence, hardware is powered up from the standby power mode to the main power mode and the Operating System is booted. Note: If an error occurs during this sequence, the system is automatically powered down to standby.
Power Off button	Accessible only when the system is powered on.

Figure 7. Standard Power Operations box - Power On

2. From the **Standard Power Operations** box, click **Power On** to launch the power up sequence, which may take a few minutes to complete.
3. From the **Power Information** box, click the **Refresh** button to update power status. Once the power up sequence has completed, the **Power State** value switches from **Off** to **On** and the **Power Off** button is enabled.
4. Connect to the Remote System Console to follow the power on sequence, as explained in Previewing and Launching the Remote System Console in the *NovaScale 9006 Server Hardware Console User's Guide*.

Important **The physical power button located on the Local Control Panel device should only be used for servicing operations and/or in the event of an emergency or a network failure.**

Related Topics

- Viewing Server Power Status, on page 2-4
- Powering Off the Server, on page 2-8
- Forcibly Powering Off / Resetting the Server, on page 2-10

What To Do if an Incident Occurs?

- The power cable may be detached.
- The power sequence has not completed.
- The power supply may be damaged.

2.1.3. Powering Off the Server

The system can be powered off from the **Power Management** page **Standard Operations** box.

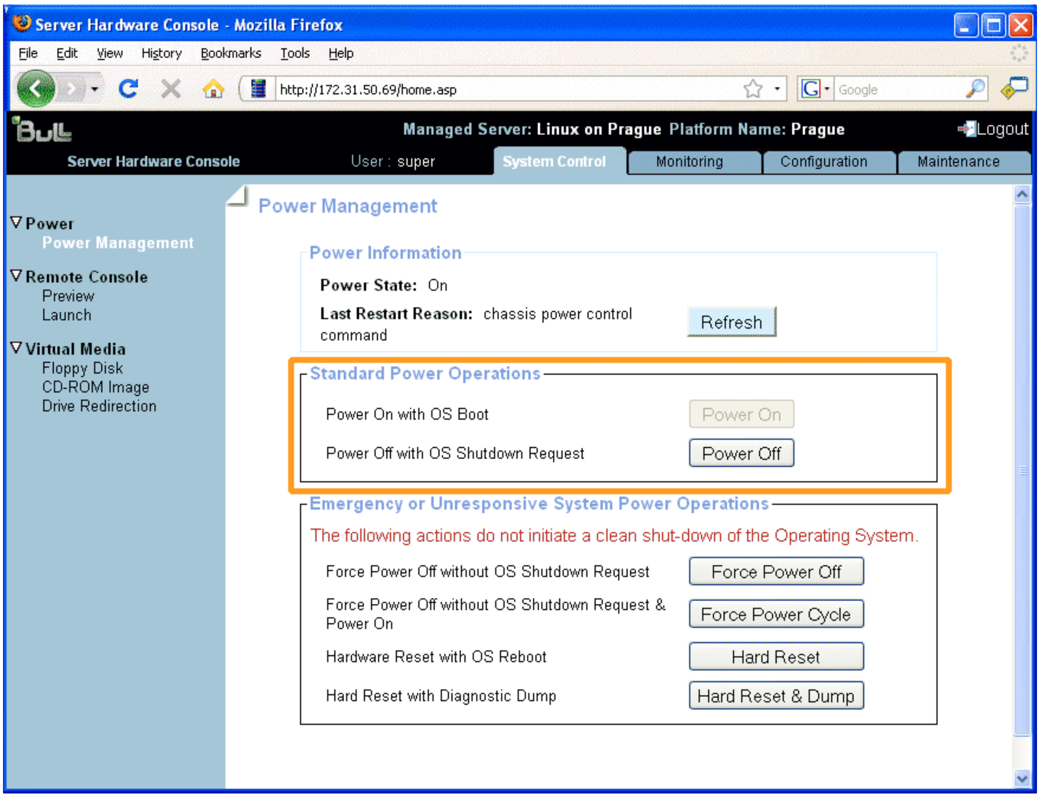
Important **The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and the Power Off button may not be enabled although the system is powered up. You can update power status by using the Refresh button.**

Prerequisites

- You have **Power Control** permission.
- The **Power Off** button is enabled.

Procedure

1. From the **System** tab, click **Power > Power Management** to open the **Power Management** page.



Server Hardware Console - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://172.31.50.69/home.asp

Managed Server: Linux on Prague Platform Name: Prague

Server Hardware Console User : super

Power Management

Power Information

Power State: On

Last Restart Reason: chassis power control command

Refresh

Standard Power Operations

Power On with OS Boot — Power On

Power Off with OS Shutdown Request — Power Off

Emergency or Unresponsive System Power Operations

The following actions do not initiate a clean shut-down of the Operating System.

Force Power Off without OS Shutdown Request — Force Power Off

Force Power Off without OS Shutdown Request & Power On — Force Power Cycle

Hardware Reset with OS Reboot — Hard Reset

Hard Reset with Diagnostic Dump — Hard Reset & Dump

Standard Power Operations Box	
Note: For details on other power management features, see Figure 5, on page 2-3.	
Power On button	Accessible only when the system is powered off.
Power Off button	Requests the Operating System to perform a graceful power down. During this sequence the Operating System saves data, closes open applications and shuts down, and hardware is powered down from the main power mode to the standby power mode. Note: The Operating System must be configured to accept the power off request.

Figure 8. Standard Power Operations box - Power Off

2. From the **Power Operations** box, click **Power Off** to launch the routine power down sequence, which may take a few minutes to complete.
3. From the **Power Information** box, click the **Refresh** button to update power status. Once the power down sequence has completed, the **Power State** value switches from **On** to **Off** and the **Power On** button is enabled.
4. Connect to the Remote System Console to follow the power off sequence, as explained in Previewing and Launching the Remote System Console, on page 2-12.

Important **The physical power button located on the Local Control Panel device should only be used for servicing operations and/or in the event of an emergency or a network failure.**

Related Topics

- Viewing Server Power Status, on page 2-4
- Powering On the Server, on page 2-6
- Forcibly Powering Off / Resetting the Server, on page 2-10

What To Do if an Incident Occurs?

If the system remains in the **Power On** state after a **Power Off** operation, one of the following problems may be the cause:

- The power sequence has not completed.
- The system has frozen.

You may need to forcibly power down the system using one of the power off buttons accessible from the **Emergency or Unresponsive System Power Operations Box**.

2.1.4. Forcibly Powering Off / Resetting the Server

In the event of a system crash or freeze, the system can be forcibly powered off or reset from the Power Management page Emergency or Unresponsive System Power Operations box.

Important **The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and the emergency Power Off / Reset buttons may not be enabled. You can update power status by using the Refresh button.**

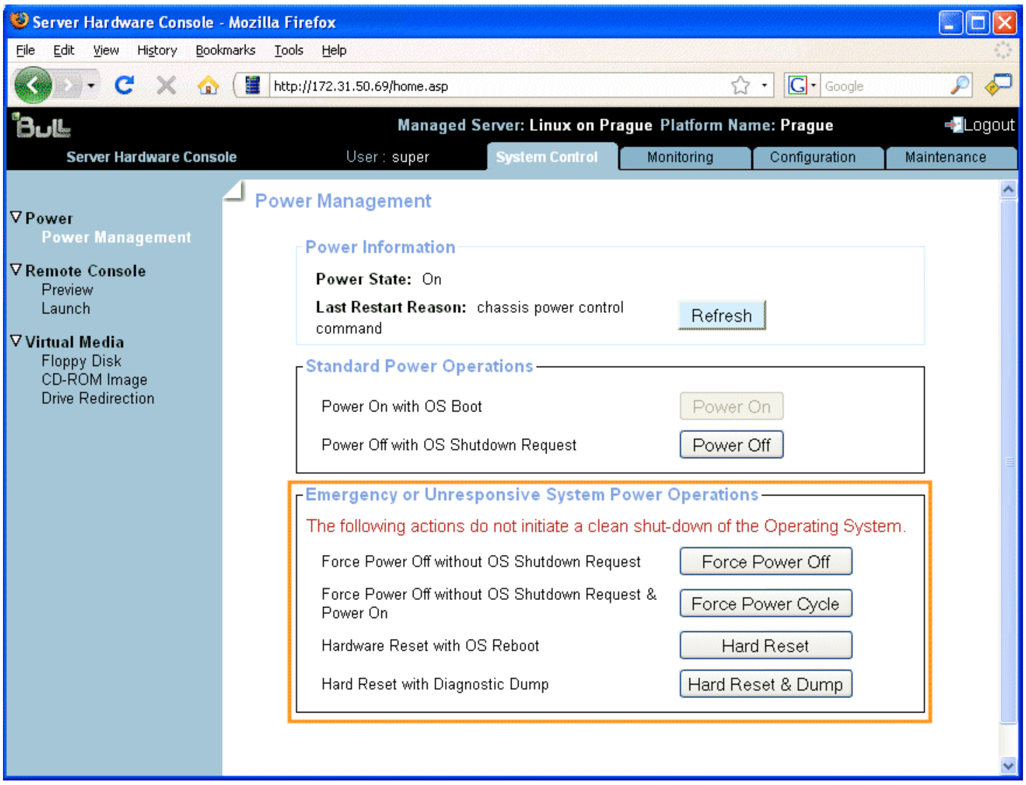
Prerequisites

- You have Power Control permission.
- The system remains in the Power On state after a Power Off operation.

Procedure

WARNING
The Emergency or Unresponsive System Power Operations buttons should only be used if the Operating System is unable to repond to a standard power off request. These sequences may result in data loss and file corruption.

1. From the System Control tab, click Power > Power Management to open the Power Management page and access the Emergency or Unresponsive System Power Operations box.



Managed Server: Linux on Prague Platform Name: Prague

User : super

Power State: On

Last Restart Reason: chassis power control command

Power On with OS Boot

Power Off with OS Shutdown Request

The following actions do not initiate a clean shut-down of the Operating System.

Force Power Off without OS Shutdown Request

Force Power Off without OS Shutdown Request & Power On

Hardware Reset with OS Reboot

Hard Reset with Diagnostic Dump

Emergency or Unresponsive System Power Operations Box	
Important: These buttons should only be used if the Operating System is unable to respond to a standard (graceful) power off request. These sequences may result in data loss and file corruption.	
Note: For details on other power management features, see Figure 5, on page 2-3.	
Force Power Off button	Performs a power down sequence independently of the Operating System.
Force Power Cycle button	Performs a power down sequence independently of the Operating System and automatically re-launches the powering up sequence.
Hard Reset button	Restarts the Operating System without powering down the system. All cache information is erased. Use it as a last resort to forcibly retrieve the Operating System when it freezes.
Hard Reset & Dump button	Writes a crash dump and then restarts the Operating System without powering down the system. All cache information is written to the dump file and can be used for problem analysis.

Figure 9. Emergency or Unresponsive System Power Operations box

2. From the **Emergency or Unresponsive System Power Operations** box, carefully select the required operation and click the corresponding button to launch the selected sequence, which may take a few minutes to complete.
3. From the **Power Information** box, click the **Refresh** button to update power status.

Related Topics

- Viewing Server Power Status, on page 2-4
- Powering On the Server, on page 2-6
- Powering Off the Server, on page 2-8

2.2. Using the Remote System Console

The Remote System Console feature is used to connect directly to the server from the Hardware Console, allowing you to remotely view, use and control the server with the keyboard, video and mouse on your local computer.

This feature can be used in conjunction with the Virtual Media feature to perform remote software and firmware installations.

Note For everyday use, end users will not use the Remote System Console feature provided by the Hardware Console. They will be able to remotely connect to the server by using the remote desktop client compatible with their Operating System (e.g. Terminal Server for Microsoft Windows or Xming for Linux).

Prerequisites

- The Remote System Console is a Java Applet that establishes a TCP connection to the system's embedded management board (BMC) using the RFB protocol and requires the installation of Java Runtime Environment (JRE) version 1.4 or higher on your computer.
- To be able to use the Remote System Console feature, your network must be configured to support the RFB protocol.

Notes

- For further information about how to configure or modify network settings, refer to Configuring or Modifying Network Settings, on page 4-4, or contact your network administrator.
- For further information about how to define Remote System Console options, refer to Remote System Console Options Menu, on page 2-16.

2.2.1. Previewing and Launching the Remote System Console

The Remote System Console can be previewed and/or launched, at any time, directly from the Hardware Console.

Note If a security warning message, prompting you to install and run a Java plug-in, check the plug-in's authenticity and click **Yes** to install and run the plug-in.

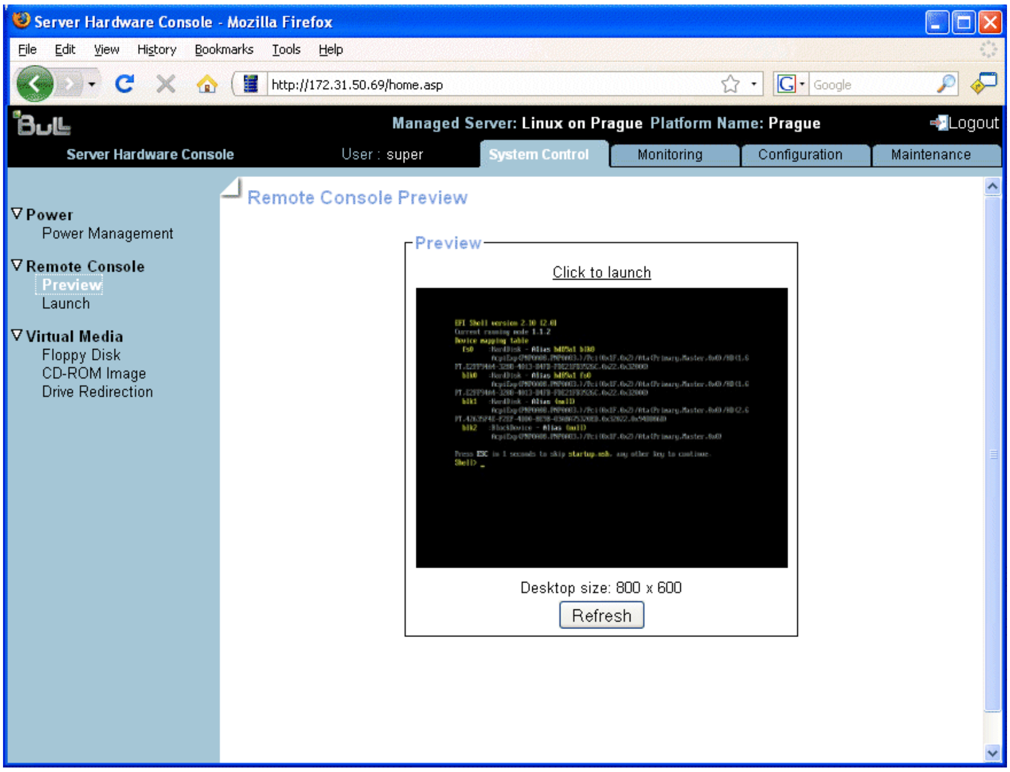
Procedure

This procedure describes how to launch and/or preview the Remote System Console.

- If you want to preview the console before launching, go to step 1.
- If you want to launch the console directly, go to step 3.

1. To preview the console from the Hardware Console, select the **System Control** tab and click **Remote Console > Preview** to open the **Remote Console Preview** page.

   The display is not refreshed dynamically, if required click the **Refresh** button to update the display.



```
EFI Shell version 2.10 [2.0]
Current running mode 1.1.2
Device mapping table
  fs0    :HardDisk - Alias hd0a1 blk0
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(1,G
PT,E2FF94A4-32BB-4013-84FB-F0E21FB3526C,0x22,0x32000)
  blk0   :HardDisk - Alias hd0a1 fs0
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(1,G
PT,E2FF94A4-32BB-4013-84FB-F0E21FB3526C,0x22,0x32000)
  blk1   :HardDisk - Alias (null)
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(2,G
PT,42635F4E-F2EF-4800-8E70-0380A7532083,0x32022,0x9400000)
  blk2   :BlockDevice - Alias (null)
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> _
```

Preview Box	
Click to launch	Click this link to launch the Remote System Console.
Refresh	Click this button to refresh the Remote System Console display.
Desktop size	Current Remote System Console desktop size.

Figure 10. Remote Console Preview page

2. To launch the console from the **Preview** box, click the **Click to launch** link. The Remote System Console opens in a new window.
3. To launch the console from the Hardware Console, select the **System Control** tab and click **Remote Console > Launch**. The Remote System Console opens in a new window.

Related Topics

- Stopping the Remote System Console, on page 2-19

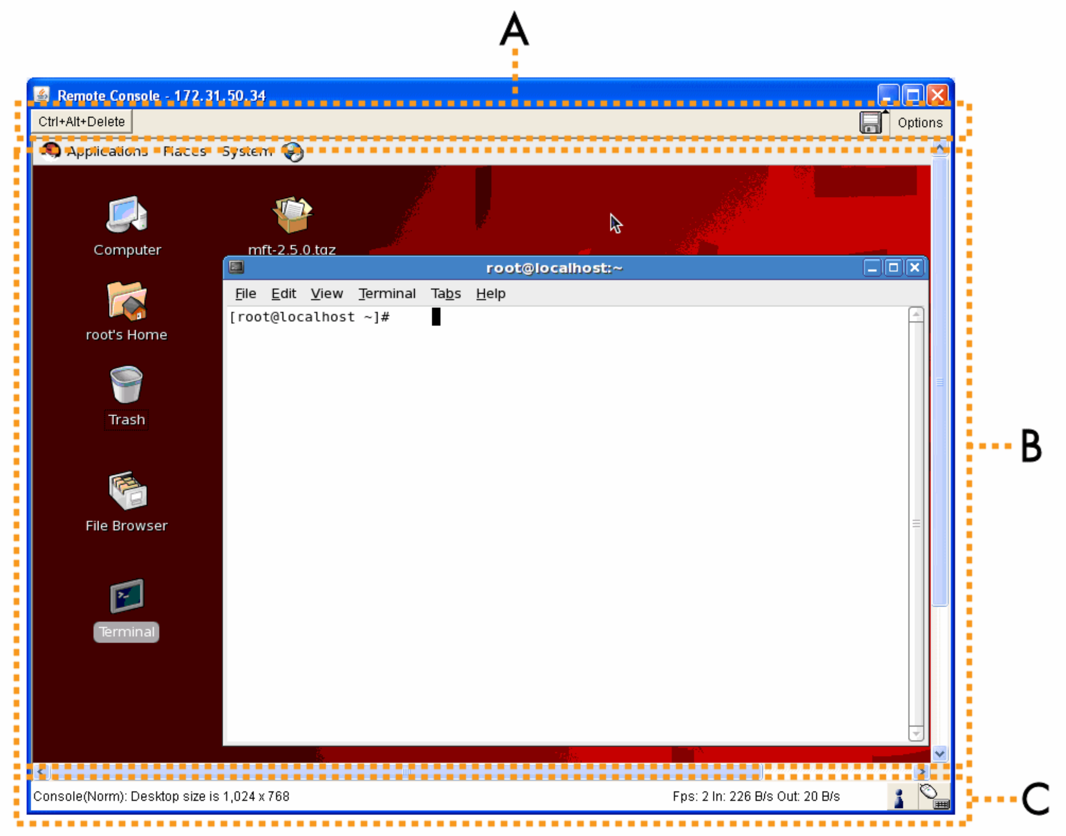
What To Do if an Incident Occurs?

- Network settings are incorrect.
- Your network is not configured to support the RFB protocol.

Contact your network administrator.

2.2.2. Remote System Console Overview

Once you have connected to the Remote System Console, it behaves as if you were sitting in front of the remote system, using your local keyboard and mouse.



```
[root@localhost ~]#
```

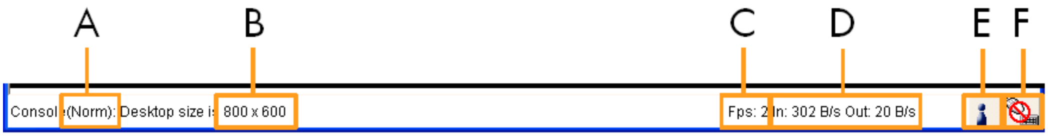
Console(Norm): Desktop size is 1,024 x 768

Fps: 2 In: 226 B/s Out: 20 B/s

Item	Description
A: **Control** bar	The Control bar provides the following buttons:
	Ctrl+Alt+Delete Hotkey to send the **CTRL+ALT+DEL** keystroke combination to the remote system. You can define other hotkey combinations, as described in Configuring Remote System Console Settings, on page 4-43.
	💾 Opens the virtual media **Drive Redirection** menu, as detailed in Using the Drive Redirection Feature, on page 2-17.
	Options Opens the **Options** menu, as detailed in Remote System Console Options, on page 2-16.
B: **Remote** desktop	This area displays the remote system desktop screen.
C: **Status** bar	The status bar provides the information detailed Figure 12.

Figure 11. Remote System Console Overview

This figure explains the information provided in the status bar. For further information about how to define options, refer to Remote System Console Options, on page 2-16.



Consol :(Norm): Desktop size i: 800 x 600 Fps: 2 In: 302 B/s Out: 20 B/s

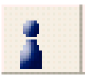
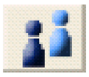
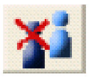
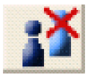
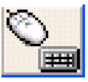
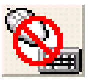
Item	Description
A	Connection type. Two possible values: • **Norm**: standard connection without encryption. • **SSL**: secure connection using Secure Socket Layer.
B	Display resolution, which is the same as that of the remote screen.
C	Number of frame buffer updates (**Fps**).
D	Incoming (**In**) and Outgoing (**Out**) network traffic in KB per seconds. A low value is recommended.
E	Access settings:  A single user is connected.  One or more users are connected.  You have exclusive access.  Another user has exclusive access.
F	Monitor only settings:  You can use your keyboard and mouse (the **Monitor Only** option is not enabled).  You cannot use your keyboard and mouse (the **Monitor Only** option is enabled).

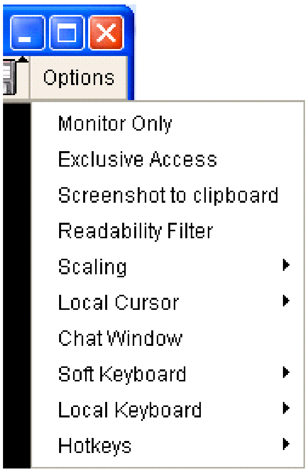
Figure 12. Remote System Console Status Bar information

Related Topics

- Stopping the Remote System Console, on page 2-19

2.2.3. Remote System Console Options Menu

This section describes the features available from the **Options** menu located on the Remote System Console Control bar.



Command	Description
Monitor Only	When enabled, keyboard and mouse interaction is disabled. Currently applied settings are displayed in the status bar.
Exclusive Access	When enabled, forces the remote consoles of all other users to close until the exclusive user disables the option or logs off. Currently applied settings are displayed in the status bar. Reserved for members of the **Admin** group.
Screenshot to clipboard	Allows you to copy the remote system screen to clipboard.
Readability Filter	When enabled, screen readability is enhanced when the remote console window is scaled. Available with JVM 1.4 or higher.
Scaling	Allows you to scale the remote console window. • Select **25%** or **50%** to scale down. • Select **100%** to scale to same resolution as the remote screen. • Select **Scale to fit** to scale to the size of the window.
Local Cursor	Allows you to select a custom mouse pointer shape, which is saved and automatically activated when you log in again.
Chat Window	Displays a chat window allowing you to interact with other users logged on to the remote console.
Soft Keyboard	Allows you to emulate the remote keyboard when language and country mapping differs from your local keyboard (e.g. QWERTY versus AZERTY). • Click **Show** to display the soft keyboard. • Select **Mapping** and the required language to change the soft keyboard language, if necessary. For details, see Using the Remote System Console Soft Keyboard, on page 2-18.
Local Keyboard	Allows you to change language mapping for your local keyboard (e.g. you use a QWERTY keyboard on a French localized computer), if necessary.
Hotkeys	Allows you to send configured keystroke combinations to the remote system. For details, see Configuring Remote System Console Settings, on page 4-43.

Figure 13. Remote System Console Options menu

2.2.4. Using the Drive Redirection Feature

Using the Drive Redirection feature, you can virtualize up to two images or drives, allowing any floppy or CD-ROM image, floppy drive, optical drive and/or USB mass storage device available on your local computer or anywhere on the network to be used from the Remote System Console.

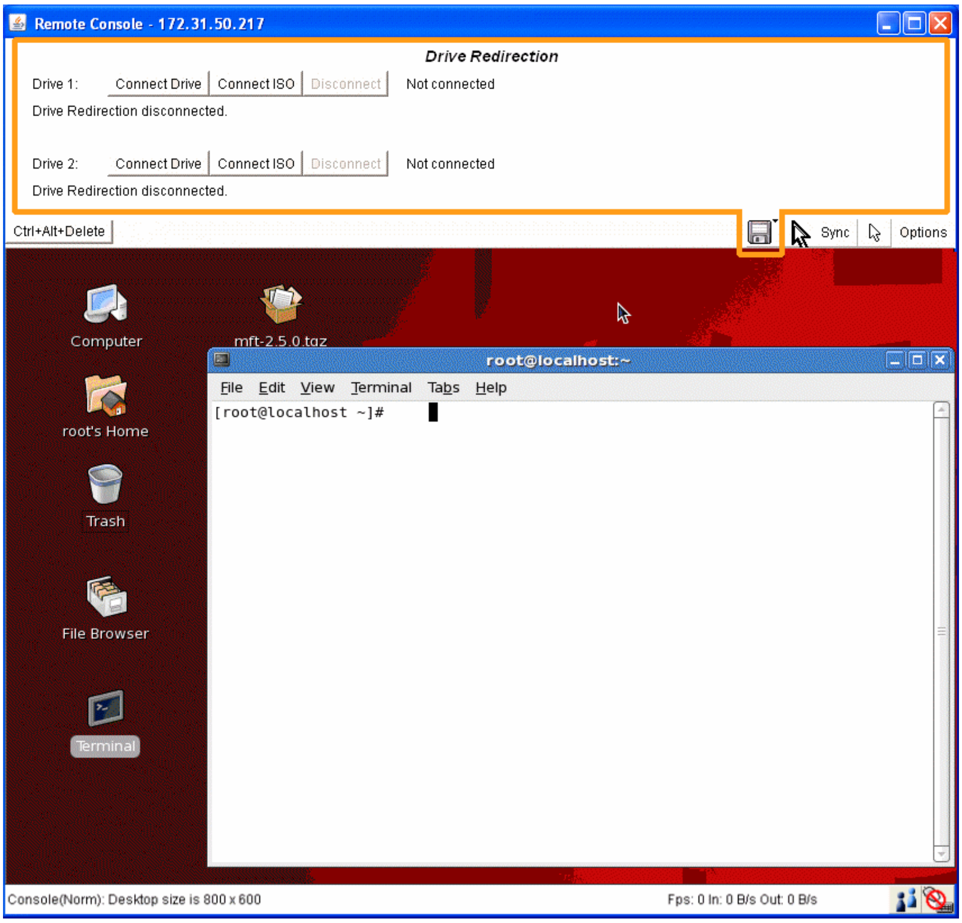
The remote system then has access to the virtual media on your local computer and can read from and write to that media as if it were physically present on the remote system. These virtual drives can then be used for operations such as installing software and firmware, updating drivers or installing new Operating Systems.

Prerequisites

- None.

Procedure

- To use the Drive Redirection feature, click the Floppy button (💾) on the Remote System Console Control bar. The **Drive Redirection** menu appears on the Remote System Console.



Not connected

Drive Redirection disconnected.

Not connected

Drive Redirection disconnected.

```
[root@localhost ~]#
```

Console(Norm): Desktop size is 800 x 600

Fps: 0 In: 0 B/s Out: 0 B/s

Figure 14. Remote System Console Drive Redirection menu

Related Topics

- Creating Image Files, on page 2-20

2.2.5. Using the Remote System Console Soft Keyboard

The Remote System Console Soft Keyboard feature is used when the remote system keyboard language and country mapping differs from that of your local keyboard (e.g. QWERTY versus AZERTY).

To launch the Soft Keyboard, select **Options > Soft Keyboard > Show** from the Remote System Console Control bar. The Soft Keyboard is displayed on the remote system screen.

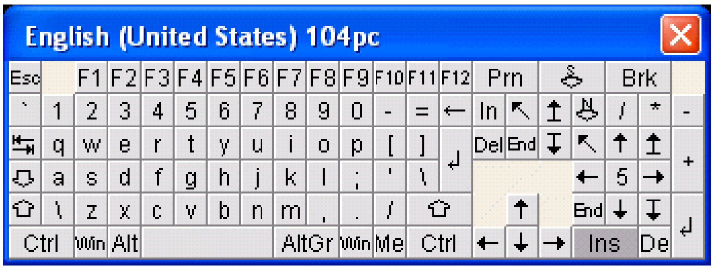

English (United States) 104pc
Esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Prn Brk
` 1 2 3 4 5 6 7 8 9 0 - = ← In ↖ ↥ / * -
q w e r t y u i o p [ ] Del End ↧ ↖ ↑ ↥ +
a s d f g h j k l ; ' \ ← 5 →
\ z x c v b n m , . / ↑ End ↓ ↧
Ctrl Win Alt AltGr Win Me Ctrl ← ↓ → Ins De

Figure 15. Remote System Console Soft Keyboard - QWERTY US example

To enter key codes and sequences, click the appropriate buttons on the screen, taking care to comply with the usage rules set out in Table 3.

Key Type	Example	Command
Standard	• Regular characters • Numbers	Click the required character key once.
Special	• Ctrl • Shift • Alt • Alt Gr • Function keys (Fx) • ...	Click the required key twice, the first time to select the key (the key color changes) and the second time to release the key (the key color changes back again).
Combinations	• Ctrl+C • Ctrl+Fx • AltGr+Shift+Fx • ...	Click each key in the sequence once to select each key (key colors change) and then click the last key in the sequence a second time to release all the keys (key colors change back again).

Table 3. Remote System Console Soft Keyboard usage rules

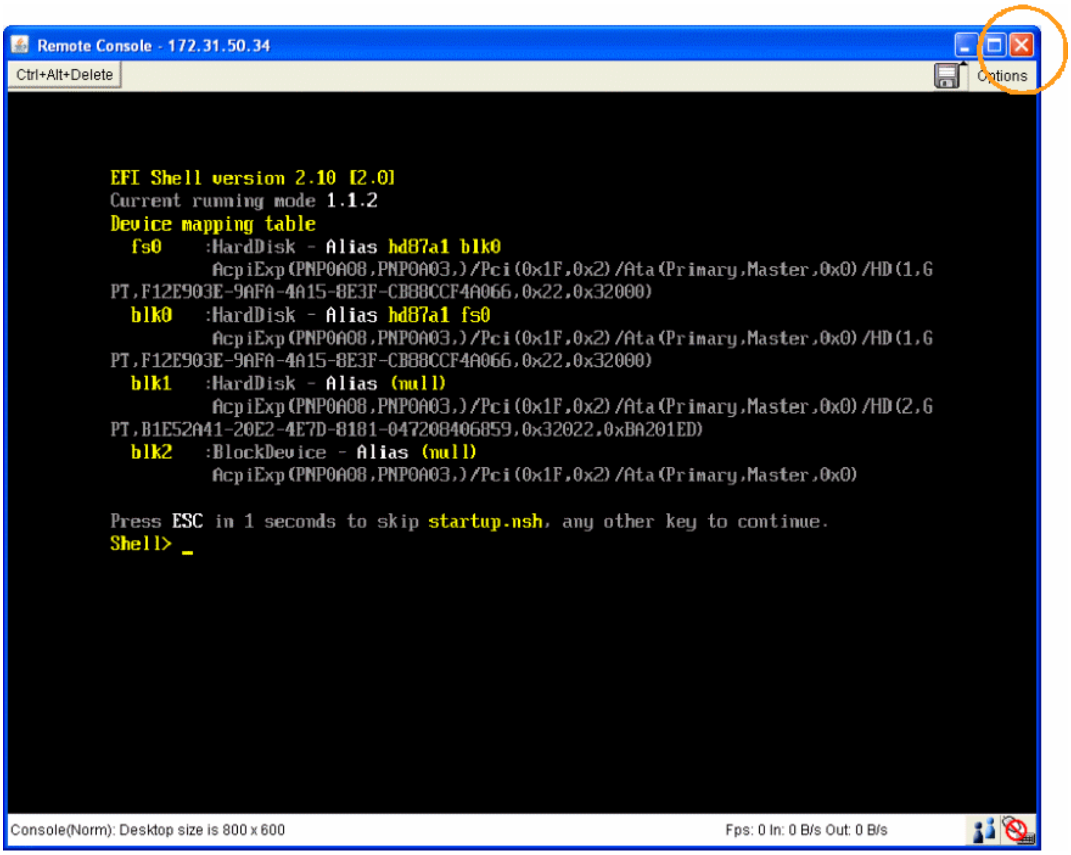
Related Topics

- Configuring Remote System Console Settings, on page 4-43
- Setting Up Keyboard and Mouse Parameters, on page 4-47

2.2.6. Stopping the Remote System Console

Procedure

The Remote System Console can be stopped at any time by clicking the close button in the upper-right corner of the window.



```
EFI Shell version 2.10 [2.0]
Current running mode 1.1.2
Device mapping table
  fs0    :HardDisk - Alias hd87a1 blk0
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(1,G
PT,F12E903E-9AFA-4A15-8E3F-CB88CCF4A066,0x22,0x32000)
  blk0   :HardDisk - Alias hd87a1 fs0
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(1,G
PT,F12E903E-9AFA-4A15-8E3F-CB88CCF4A066,0x22,0x32000)
  blk1   :HardDisk - Alias (null)
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)/HD(2,G
PT,B1E52A41-20E2-4E7D-8181-047208406859,0x32022,0xBA201ED)
  blk2   :BlockDevice - Alias (null)
          AcpiExp(PNP0A08,PNP0A03,)/Pci(0x1F,0x2)/Ata(Primary,Master,0x0)

Press ESC in 1 seconds to skip startup.nsh, any other key to continue.
Shell> _
```

Console(Norm): Desktop size is 800 x 600
Fps: 0 In: 0 B/s Out: 0 B/s

Figure 16. Remote System Console close button

Related Topics

- Previewing and Launching the Remote System Console, on page 2-12

2.2.7. Creating Image Files

When you create floppy or CD-ROM image files, you are advised to proceed according to the following recommendations.

Creating Floppy Image Files for Linux Systems

Use the **dd utility** delivered with your Operating System:

Copy the floppy raw device to a file using the following command:

```
        dd [if=/dev/fd0] [of=/tmp/floppy.image]
```

where `/dev/fd0` is the input device and `/tmp/floppy.image` is the output file.

Creating Floppy Image Files for Windows Systems

Use the **RawWrite for Windows** tool delivered on the *Resource and Documentation CD* delivered with your system:

1. Launch **RawWrite for Windows** and select the **Write** tab.
2. In the **Image File** field, enter or select the file name to which you want to save floppy content.
3. Click **Write** to create the image.

Creating CD-ROM Image Files for Linux Systems

Use the **dd utility** delivered with your Operating System:

Copy the contents of the CD-ROM to a file using the following command:

```
        dd [if=/dev/cdrom] [of=/tmp/cdrom.image]
```

where `/dev/cdrom` is the input device and `/tmp/cdrom.image` is the output file.

Creating CD-ROM Image Files for Windows Systems

Use your usual CD-ROM imaging tool to copy the contents of the disk to a single ISO image file on your hard disk.

Chapter 3. Monitoring the Server

This chapter explains how to monitor server activity and view and manage event logs. It includes the following topics:

3.1. Initial Messaging and Alert Configuration

When the server is first delivered, you will need to perform a few basic configuration tasks to benefit from all the messaging and alert features available. These configuration tasks are explained in detail in Chapter 4. Configuring the Server Embedded Management Controller and are listed below:

- Enabling and Configuring the SNMP Agent, on page 4-8
- Setting Up Board, Security and Remote Console Messages, on page 4-11
- Configuring Alert Settings, on page 4-49

3.2. Viewing Monitoring Sensors

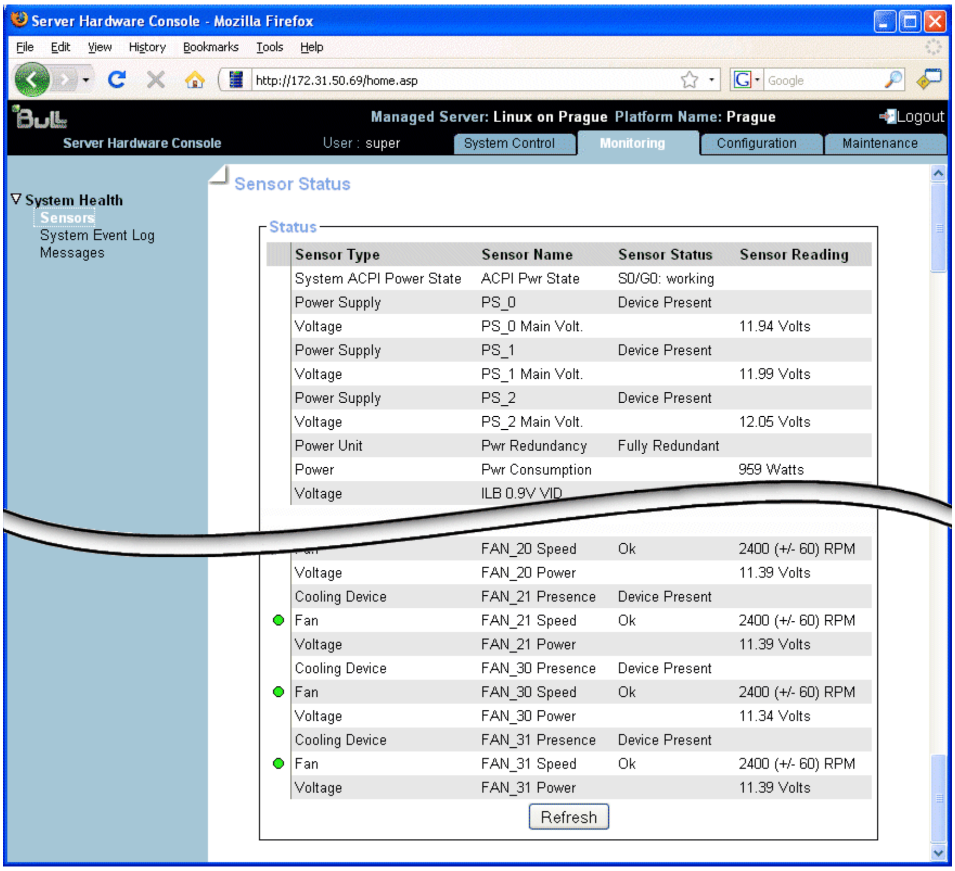
The server is equipped with various sensors that monitor:

- Power status
- Presence, absence, redundancy of components
- Voltage values
- Temperature values
- Fan speed

Procedure

1. From the **Monitoring** tab, click **System Health > Sensors** to display the **Sensor Status** page.
2. Click **Refresh** and check that all component icons are green.

Note Tables 4 and 5 explain sensor status page icons, values and readings.


Server Hardware Console - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.31.50.69/home.asp
Google
Bull
Managed Server: Linux on Prague Platform Name: Prague
Logout
Server Hardware Console
User : super
System Control
Monitoring
Configuration
Maintenance
System Health
Sensors
System Event Log
Messages

Sensor Status

Status

	Sensor Type	Sensor Name	Sensor Status	Sensor Reading
	System ACPI Power State	ACPI Pwr State	S0/G0: working	
	Power Supply	PS_0	Device Present	
	Voltage	PS_0 Main Volt.		11.94 Volts
	Power Supply	PS_1	Device Present	
	Voltage	PS_1 Main Volt.		11.99 Volts
	Power Supply	PS_2	Device Present	
	Voltage	PS_2 Main Volt.		12.05 Volts
	Power Unit	Pwr Redundancy	Fully Redundant	
	Power	Pwr Consumption		959 Watts
	Voltage	ILB 0.9V VID		
		FAN_20 Speed	Ok	2400 (+/- 60) RPM
	Voltage	FAN_20 Power		11.39 Volts
	Cooling Device	FAN_21 Presence	Device Present	
●	Fan	FAN_21 Speed	Ok	2400 (+/- 60) RPM
	Voltage	FAN_21 Power		11.39 Volts
	Cooling Device	FAN_30 Presence	Device Present	
●	Fan	FAN_30 Speed	Ok	2400 (+/- 60) RPM
	Voltage	FAN_30 Power		11.34 Volts
	Cooling Device	FAN_31 Presence	Device Present	
●	Fan	FAN_31 Speed	Ok	2400 (+/- 60) RPM
	Voltage	FAN_31 Power		11.39 Volts

Sensor Status Page	
Refresh button	The **Sensor Status** page is not automatically updated, therefore the display may not reflect current sensor status. Use this button, located at the bottom of the page, to update the display.

Figure 17. Sensor Status page

Sensor Status Page - Icons, Values and Readings				
Icon	Type	Name	Status	Reading
–	System ACPI Power State	ACPI Pwr State	• No reading • S0/G0: working • S4/S5: soft off	–
–	Power Supply	PS_X	• No reading • Device Present • Device Absent • Failure detected • Input lost or out of range	–
–	Power Unit	Pwr Redundancy	• No reading • Fully redundant • Redundancy Lost • Non redundant: insufficient resources	–
–	Power	Pwr Consumption	–	Value in Watts
–	Voltage	PS_X Main Volt. ILB XXX MTB XXX P0 XXX P1 XXX P2 XXX P3 XXX FAN_XX Power	• No reading • Ok • Limit exceeded	Value in Volts
–	Processor	PROC_X	• No reading • Device Present • Device Absent • Processor disabled • Thermal trip • Processor automatically throttled	–
Green Red	Temperature	MTB Temperature ILB Temperature PDB Temperature LCP Temperature	• No reading • Ok • Below/Above lower critical threshold	Value in °C
–	Cooling Device	FANBX_X Redund. FAN_X Presence	• No reading • Fully redundant • Redundancy lost • Non redundant: insufficient resources • Device Present • Device Absent	–
Green Red	Fan	FAN_X Speed	• No reading • Ok • Below/Above lower critical threshold	Value in RPM

Table 4. Sensor Status page description

Status Icons Description	
The status icons to the left of certain components indicate the status of this component with regard to nominal threshold values.	
Green	NORMAL This component is operating correctly. No problem has been detected.
Red	CRITICAL This component is not operating correctly. A problem has been detected. Immediate preventive or corrective action is required.

Table 5. Status Icons Description

3.3. Viewing and Clearing the System Event Log (SEL)

The System Event Log records events compliant with the IPMI standard, in particular those concerning:

- Power supplies
- FANs
- Temperature sensors

Notes

- Events recorded in this log can be transmitted via the event alerting system to an SNMP Manager or to offline personnel by email.
- You can access another log, which is called the Board and Security Messages log. This log records non-IPMI events.

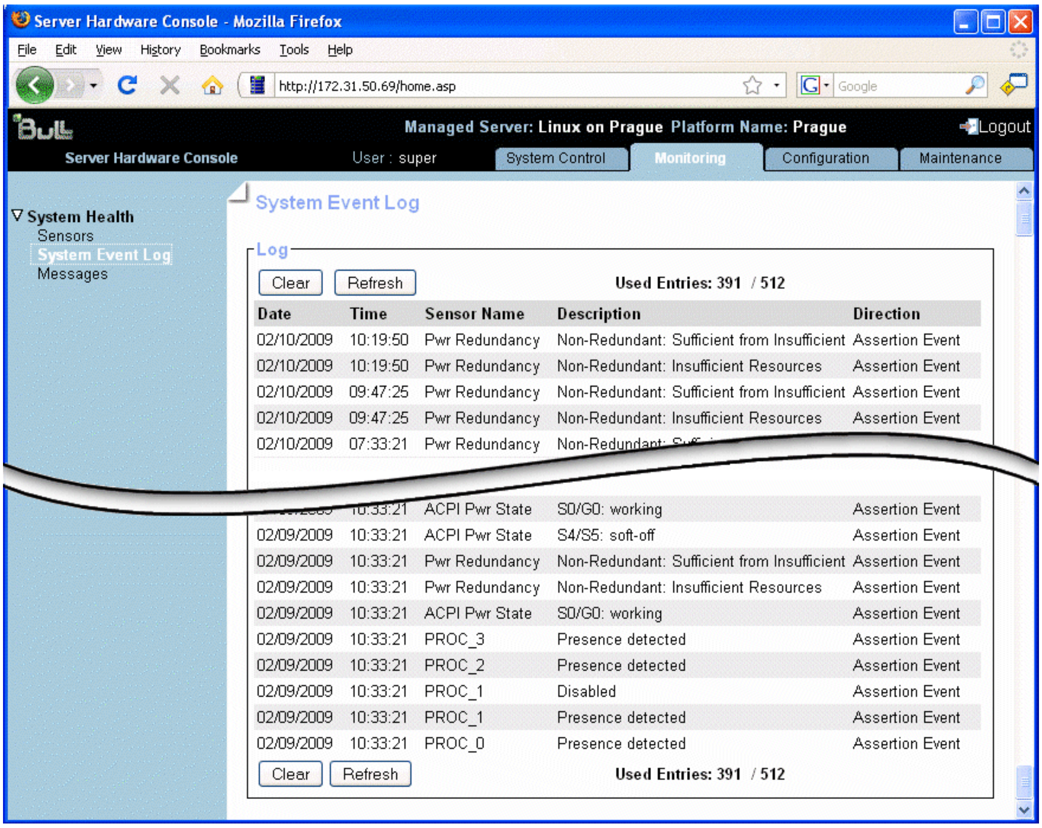
WARNING
The System Event Log can only store up to 512 entries at a time.
Once this limit is reached, the LOG IS NOT AUTOMATICALLY EMPTIED to allow for the arrival of new events. Beyond the 512-entry limit, NEW EVENTS ARE NOT RECORDED.
It is strongly recommended to empty this log regularly, using the Clear button, so that the latest events can be logged.
Note that cleared entries are deleted and cannot be retrieved.

Prerequisites

- Viewing: none.
- Clearing: you have Alert Settings & Clear SEL permission.

Procedure

- From the **Monitoring** tab, click **System Health > System Event Log** to open the **System Event Log** page:



Used Entries: 391 / 512

Date	Time	Sensor Name	Description	Direction
02/10/2009	10:19:50	Pwr Redundancy	Non-Redundant: Sufficient from Insufficient	Assertion Event
02/10/2009	10:19:50	Pwr Redundancy	Non-Redundant: Insufficient Resources	Assertion Event
02/10/2009	09:47:25	Pwr Redundancy	Non-Redundant: Sufficient from Insufficient	Assertion Event
02/10/2009	09:47:25	Pwr Redundancy	Non-Redundant: Insufficient Resources	Assertion Event
02/10/2009	07:33:21	Pwr Redundancy	Non-Redundant: Suf	
	10:33:21	ACPI Pwr State	S0/G0: working	Assertion Event
02/09/2009	10:33:21	ACPI Pwr State	S4/S5: soft-off	Assertion Event
02/09/2009	10:33:21	Pwr Redundancy	Non-Redundant: Sufficient from Insufficient	Assertion Event
02/09/2009	10:33:21	Pwr Redundancy	Non-Redundant: Insufficient Resources	Assertion Event
02/09/2009	10:33:21	ACPI Pwr State	S0/G0: working	Assertion Event
02/09/2009	10:33:21	PROC_3	Presence detected	Assertion Event
02/09/2009	10:33:21	PROC_2	Presence detected	Assertion Event
02/09/2009	10:33:21	PROC_1	Disabled	Assertion Event
02/09/2009	10:33:21	PROC_1	Presence detected	Assertion Event
02/09/2009	10:33:21	PROC_0	Presence detected	Assertion Event

Used Entries: 391 / 512

Figure 18. System Event Log page

- Use the **Refresh** button to update the display at any time.
- Use the **Clear** button to empty the log. Entries are deleted and cannot be retrieved.

Note SEL messages are explained in Appendix B - Troubleshooting the NovaScale 9006 Server Drawer, on page B-1.

Related Topics

- Viewing Board and Security Messages on page 3-6
- Configuring Alert Settings, on page 4-49
- Troubleshooting the NovaScale 9006 Server Drawer, on page B-1

3.4. Viewing Board and Security Messages

The Board and Security Messages log records non-IPMI events, such as power-on errors, user authentication, connection to the remote console, security violation, log deletion or firmware upgrade.

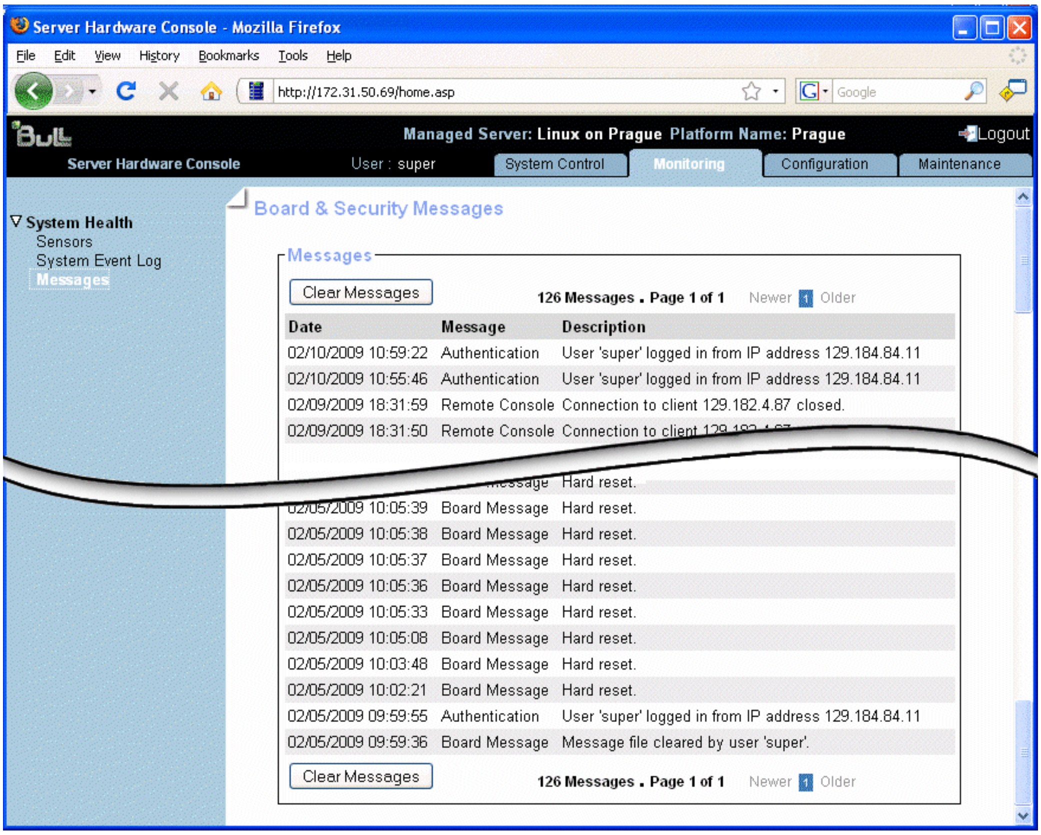
Note Events compliant with the IPMI standard are recorded in the System Event log.

Prerequisites

- You have **Security/Log/Authentication Settings** permission.

Procedure

1. From the **Monitoring** tab, click **System Health > Messages** to open the **Board & Security Messages** page:



126 Messages . Page 1 of 1

Date	Message	Description
02/10/2009 10:59:22	Authentication	User 'super' logged in from IP address 129.184.84.11
02/10/2009 10:55:46	Authentication	User 'super' logged in from IP address 129.184.84.11
02/09/2009 18:31:59	Remote Console	Connection to client 129.182.4.87 closed.
02/09/2009 18:31:50	Remote Console	Connection to client 129.182.4.87
	Message	Hard reset.
02/05/2009 10:05:39	Board Message	Hard reset.
02/05/2009 10:05:38	Board Message	Hard reset.
02/05/2009 10:05:37	Board Message	Hard reset.
02/05/2009 10:05:36	Board Message	Hard reset.
02/05/2009 10:05:33	Board Message	Hard reset.
02/05/2009 10:05:08	Board Message	Hard reset.
02/05/2009 10:03:48	Board Message	Hard reset.
02/05/2009 10:02:21	Board Message	Hard reset.
02/05/2009 09:59:55	Authentication	User 'super' logged in from IP address 129.184.84.11
02/05/2009 09:59:36	Board Message	Message file cleared by user 'super'.

126 Messages . Page 1 of 1

Figure 19. Board & Security Messages page

2. Browse messages, as required, using the **Newer** and **Older** buttons.

Important **This log can record up to 1.000 events. Once this limit is reached, the arrival of new messages will automatically delete the oldest messages in the log.**

Related Topics

- Viewing and Clearing the System Event Log (SEL), on page 3
- Setting Up Board and Security Messaging Policies, on page 4-11

Chapter 4. Configuring the Server Embedded Management Controller

This chapter explains how you can configure the server embedded management controller to suit your working environment. It includes the following topics:

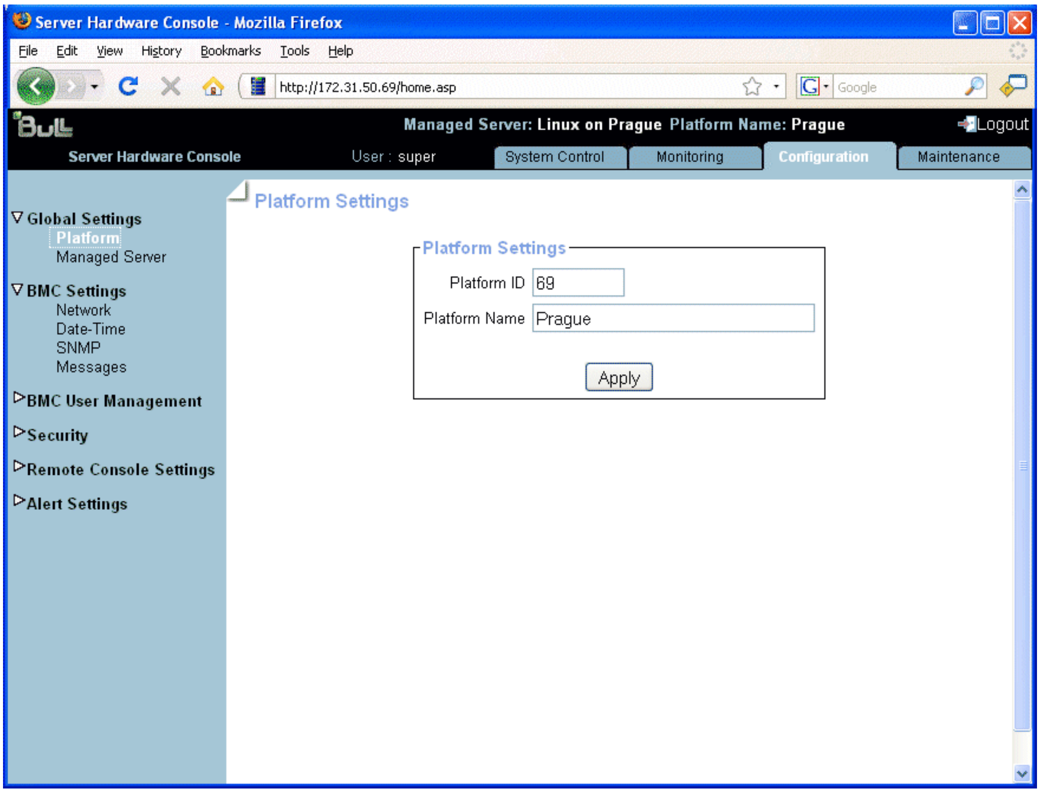
4.1. Configuring Platform Identification Settings

Prerequisites

- You have the **Network Settings** permission.

Procedure

1. From the **Configuration** tab, click **Global Settings > Platform** to open the **Platform Settings** page.



Managed Server: Linux on Prague Platform Name: Prague

User : super

Platform Settings

Platform ID 69

Platform Name Prague

Figure 20. Platform Settings page

2. Complete the fields and click **Apply**.

Related Topics

- Setting the Managed Server Name, on page 4-3

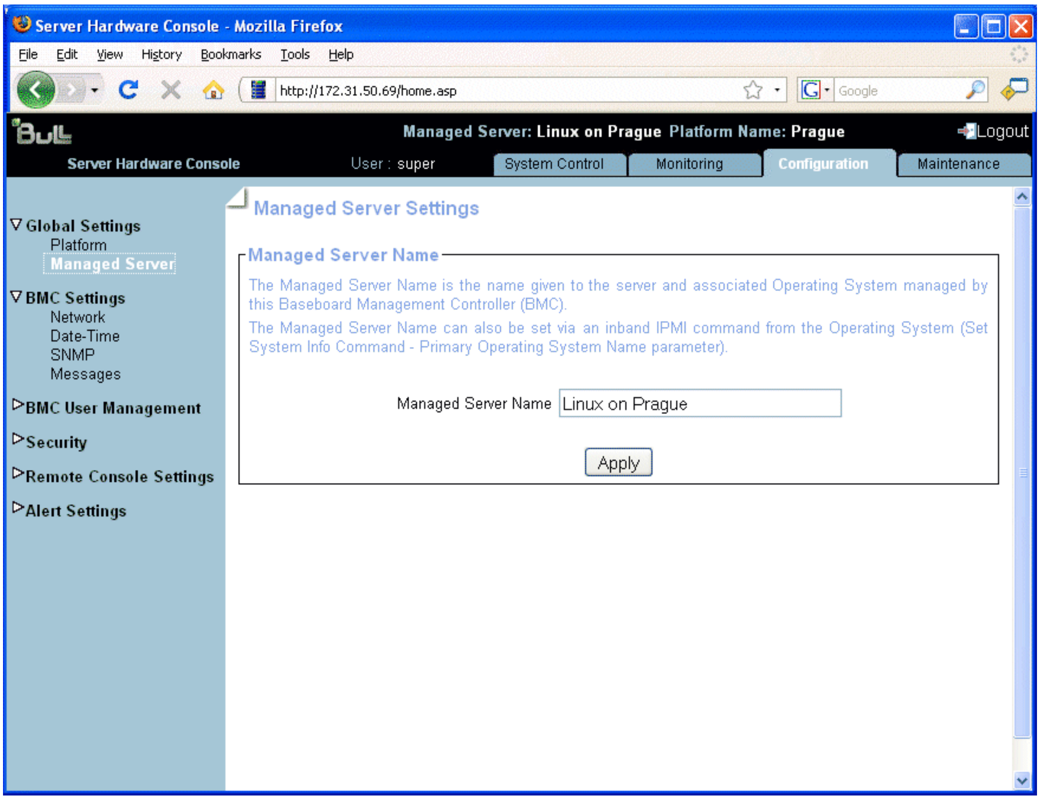
4.2. Setting the Managed Server Name

Prerequisites

- You have the **Network Settings** permission.

Procedure

1. From the **Configuration** tab, click **Global Settings** > **Managed Server** to open the **Managed Server Settings** page.



The Managed Server Name is the name given to the server and associated Operating System managed by this Baseboard Management Controller (BMC).

The Managed Server Name can also be set via an inband IPMI command from the Operating System (Set System Info Command - Primary Operating System Name parameter).

Managed Server Name: Linux on Prague

Figure 21. Managed Server Settings page

2. Complete the field and click **Apply**.

Related Topics

- Configuring Platform Identification Settings, on page 4-2

4.3. Configuring or Modifying Network Settings

The **Network Settings** page allows you to configure or modify the embedded management controller network settings for remote access to the Hardware Console from a computer or workstation with a Web browser.

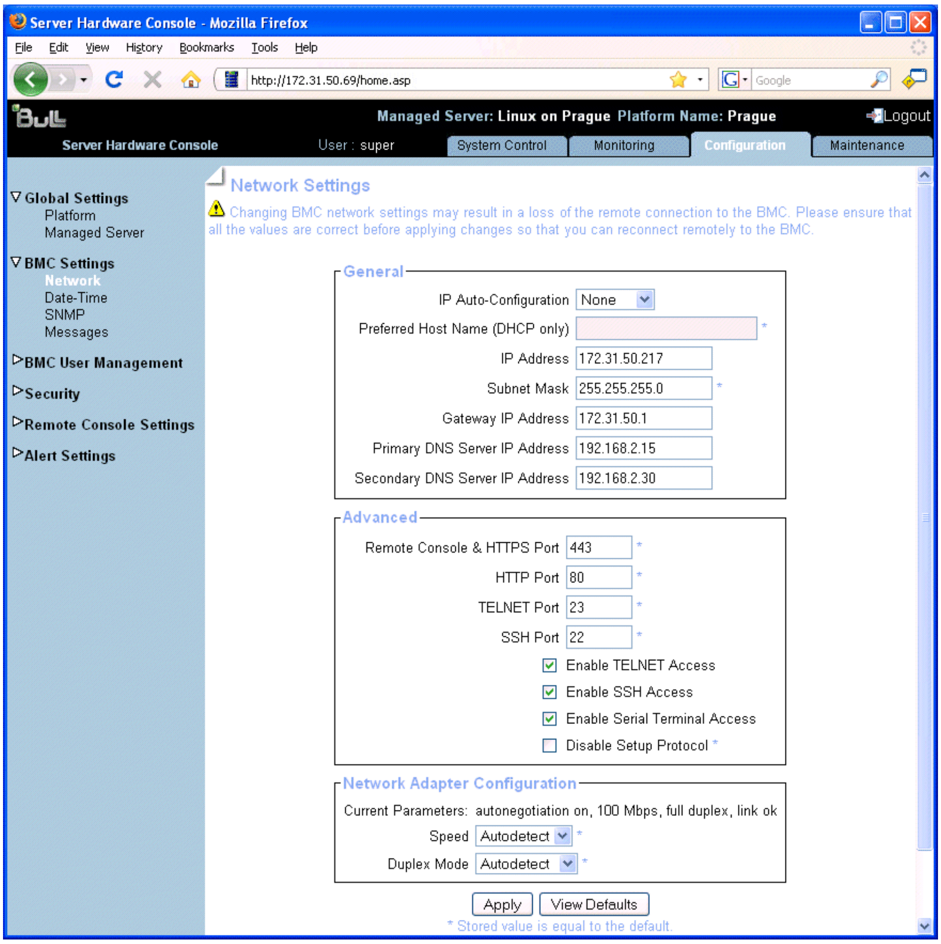
Prerequisites

- You have **Network Settings** permission.

WARNING
Good knowledge in network administration is required to complete this page.
If new network settings are incorrect, you may lose the connection to the console.
You are advised to note current settings before proceeding to enter new values so that you can restore the connection to the console if a problem arises.

Procedure

1. From the **Configuration** tab, click **BMC Settings > Network** to display the **Network Settings** page.



Network Settings

Changing BMC network settings may result in a loss of the remote connection to the BMC. Please ensure that all the values are correct before applying changes so that you can reconnect remotely to the BMC.

General

IP Auto-Configuration	None
Preferred Host Name (DHCP only)	*
IP Address	172.31.50.217
Subnet Mask	255.255.255.0 *
Gateway IP Address	172.31.50.1
Primary DNS Server IP Address	192.168.2.15
Secondary DNS Server IP Address	192.168.2.30

Advanced

Remote Console & HTTPS Port	443 *
HTTP Port	80 *
TELNET Port	23 *
SSH Port	22 *

☑ Enable TELNET Access
☑ Enable SSH Access
☑ Enable Serial Terminal Access
☐ Disable Setup Protocol *

Network Adapter Configuration

Current Parameters: autonegotiation on, 100 Mbps, full duplex, link ok

Speed	Autodetect *
Duplex Mode	Autodetect *

* Stored value is equal to the default.

Enterprise Network General Settings Box	
IP Auto-Configuration	This drop-down list allows you to enable or disable network auto-configuration via a DHCP or BOOTP server: • **None**: auto-configuration is disabled. • **DHCP**: network settings are retrieved from a DHCP server (Factory-default value). • **BOOTP**: network settings are retrieved from a BOOTP server.
Preferred host name (DHCP only)	Accessible only if **DHCP** is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if **None** is selected. The static IP address you want to use (Factory-default value: 192.x.x.x).
Subnet Mask	Accessible only if **None** is selected. The subnet mask you want to use (Factory-default value: 255.255.255.0).
Gateway IP Address	Accessible only if **None** is selected. Your default gateway IP address, if applicable.
Primary DNS Server IP Address	Accessible only if **None** is selected. Your primary DNS server IP address, if applicable.
Secondary DNS Server IP Address	Accessible only if **None** is selected. Your secondary DNS server IP address, if applicable.
Advanced Box	
Remote Console & HTTPS Port	The port number used for secure HTTPS connections and for the remote console (Factory-default: 443).
HTTP Port	The port number used for standard HTTP connections (Factory-default: 80).
TELNET Port	The Telnet port number (Factory-default: 23).
SSH Port	The Secure Shell (SSH) port number (Factory-default: 22).
Enable TELNET Access	Select this option to allow connection using a Telnet client. You must have **SSH/Telnet Access** permission.
Enable SSH Access	Select this option to allow connection using an SSH client. You must have **SSH/Telnet Access** permission.
Enable Serial Terminal Access	Select this option to open a Telnet connection to the server serial port in order to connect the server in terminal mode. You must have **SSH/Telnet Access** permission.
Disable Setup Protocol	Select this option to prevent the *psetup (Windows)* tool, used to discover the server on the LAN during initial setup, from re-detecting this server when installing other devices.

Network Adapter Configuration Box	
Current Parameters	Displays current network adapter settings.
Speed	LAN interface speed. • **Autodetect**: automatically adjusts the interface speed (Factory-default value). • **10Mbps**: fixed speed according to network. • **100Mbs**: fixed speed according to network. **Autodetect** is selected by default. If you encounter connection problems, select the fixed speed required by your network infrastructure.
Duplex Mode	LAN interface duplex mode. • **Autodetect**: automatically sets the duplex mode as required by your network infrastructure (Factory-default value). • **Half Duplex**: fixed duplex mode according to network. • **Full Duplex**: fixed duplex mode according to network. **Autodetect** is selected by default. If you encounter connection problems, select the fixed duplex mode required by your network infrastructure.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 22. Network Settings page - factory-default values

2. Complete the fields to comply with your network requirements and click **Apply**.
3. Log off the console.
4. Start the console with the new network settings from a remote computer or workstation to test the connection.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Enabling/Disabling Encryption, on page 4-33

What To Do if an Incident Occurs?

If you are unable to connect to the console from a remote computer or workstation, one of the following problems may be the cause:

- The LAN cable may be detached.
- Network settings are incorrect.
- Your network may be down.

4.4. Modifying Internal Clock Settings

The **Date/Time Settings** page allows you to set up the server internal clock. You can either set the clock manually or connect to a Network Time Protocol (NTP) server.

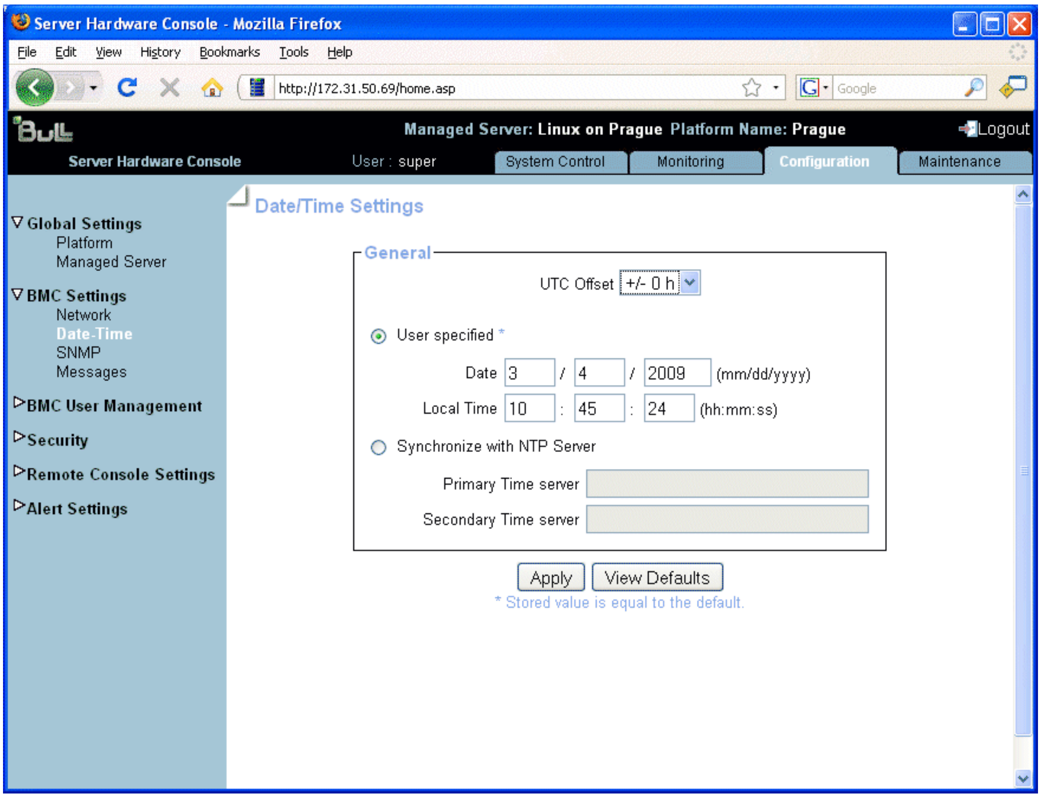
WARNING
If you do not use an NTP server, the date and time will not be persistent. In the event of a power cut, you will have to reset the date and time.

Prerequisites

- You have **Date/Time Settings** permission.
- If you want to use the NTP, you have the IP addresses of the NTP servers you want to use.

Procedure

1. From the **Configuration** tab, click **BMC Settings** > **Date-Time** to display the **Date/Time Settings** page:



Date/Time Settings

General

UTC Offset +/- 0 h

● User specified *

Date 3 / 4 / 2009 (mm/dd/yyyy)

Local Time 10 : 45 : 24 (hh:mm:ss)

○ Synchronize with NTP Server

Primary Time server

Secondary Time server

* Stored value is equal to the default.

General	
UTC Offset	UTC offset allows you to set the difference between local and universal time. You must use this drop-down list if you select **Synchronize with NTP Server**.
User Specified	This option allows you to manually set the server internal clock. You can either manually enter the date and use the **UTC Offset** drop-down list or manually enter both the date and local time.
Synchronize with NTP Server	This option allows you to enter the IP addresses of the NTP servers you want to use. You must use the **UTC Offset** drop-down list.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 23. Date/Time Settings page - factory-default values

2. If required, change the **UTC Offset** value.
3. Click either **User Specified** or **Synchronize with NTP Server**, complete the appropriate fields and click **Apply**.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

4.5. Enabling and Configuring the SNMP Agent

When enabled, the SNMP agent allows you to:

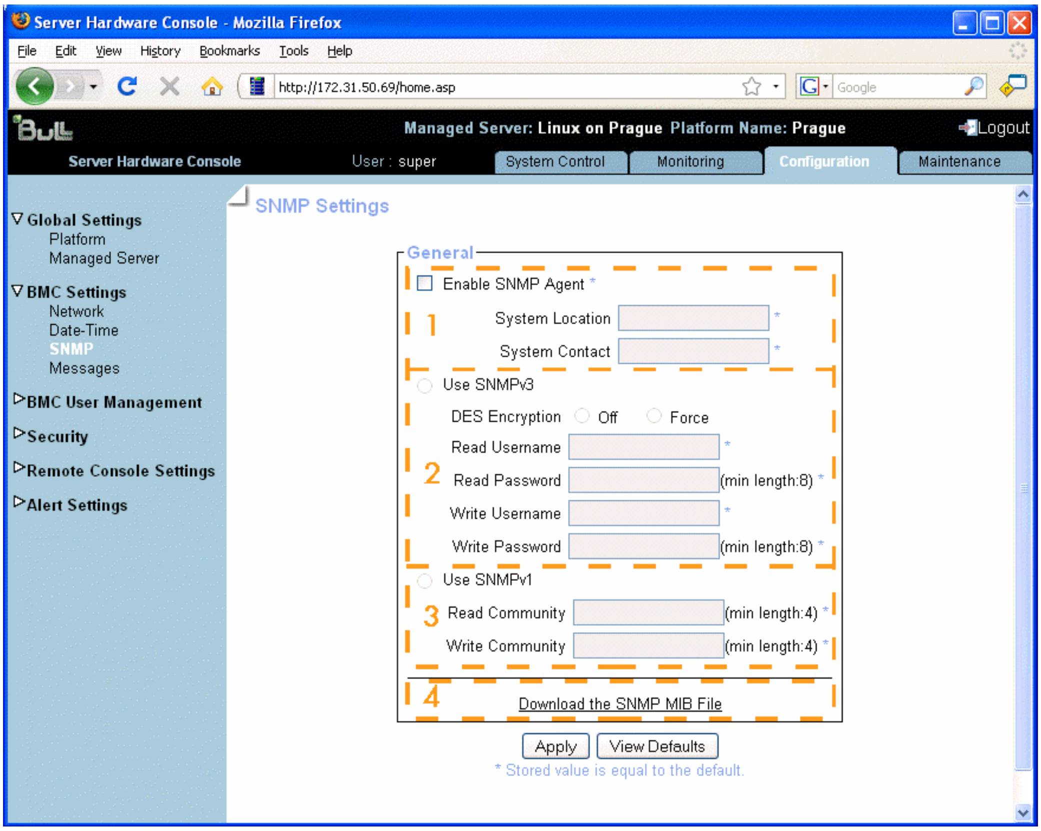
- Retrieve the following data from your SNMP manager:
  - Serial number.
  - Firmware version.
  - MAC address / IP address / Netmask / Gateway IP address.
  - Power status.
  - POST code.
- Perform the following actions through your SNMP manager:
  - Reset to factory settings.
  - Power on/off remotely.
- Report the following events to your SNMP manager:
  - User Logon (success and failure).
  - Access denied to a particular action.
  - Reset.
  - Power on/off.

Prerequisites

- You have **SNMP Settings** permission.
- Your SNMP manager software is correctly configured.

Procedure

1. From the **Configuration** tab, click **BMC Settings > SNMP** to display the **SNMP Settings** page:



General		
Area 1	Enable SNMP Agent	When selected, this option allows the SNMP agent to communicate with an SNMP manager (for example, **Bull System Manager**).
	• System Location	server name.
	• System Contact	server administrator's name or email address.
Area 2	Use SNMPv3	Select this option if required by your SNMP manager.
	• DES Encryption	Enables or disables the privacy provided by SNMPv3. Using privacy requires that both the SNMP manager and agent share a secret encryption key.
	• Read Username	Name of an SNMP user who has read-only access to the server.
	• Read Password	Read-only user authentication password.

General (continued)		
Area 2	• Write Username	Name of an SNMP user who has write access to the server.
	• Write Password	Write user authentication password.
Area 3	Use SNMPv1	Select this option if required by your SNMP manager. This option is to be selected for **Bull System Manager**.
	• Read Community	SNMP read-only community name for the server (example: **public**).
	• Write Community	SNMP write community name for the server.
Area 4	Download	This link allows you to save, as a .txt file, the server MIB file. This file is required by your SNMP manager to interpret trap messages.
View Defaults button		Allows you to display factory-default values (shown in this figure).

Figure 24. SNMP Settings page - factory-default values

2. If required, download the Management Information Base (MIB) file by clicking the **Download** button and install on the SNMP manager.

Note The **Bull System Manager** Add-on for the server supplies the MIB file.

3. Select **Enable SNMP Agent**.
4. Complete the **System Location** and **System Contact** fields.
5. Configure the SNMP agent depending on your SNMP manager:
   - If you select **Use SNMPv3**, complete the corresponding fields accordingly:
     - To allow data retrieval and event reporting only, complete the **Read User Name** and **Read Password** fields only.
     - To allow the performance of actions only, complete the **Write User Name** and **Write Password** fields only.
     - To allow data retrieval, event reporting AND the peformance of actions, complete the **Read User Name**, **Read Password**, **Write User Name** and **Write Password** fields
   - If you select **Use SNMPv1**, complete the corresponding fields accordingly:

     Important **It is NOT mandatory to complete all the fields.**
     To allow actions to be performed via an SNMP manager, complete the Write Community field.

     - To allow data retrieval and event reporting only, complete the **Read Community** field only.
     - To allow the performance of actions only, complete the **Write Community** field only.
6. Click **Apply**.
7. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

4.6. Setting Up Board, Security and Remote Console Messages

This section describes how to configure the Board and Security Messages log, which records non-IPMI events, such as power-on errors, user authentication, connection to the remote console, security violation, log deletion or firmware upgrade.

Note Events compliant with the IPMI standard are recorded in the System Event log. You can set up SEL messaging policies through **Alert Settings**.

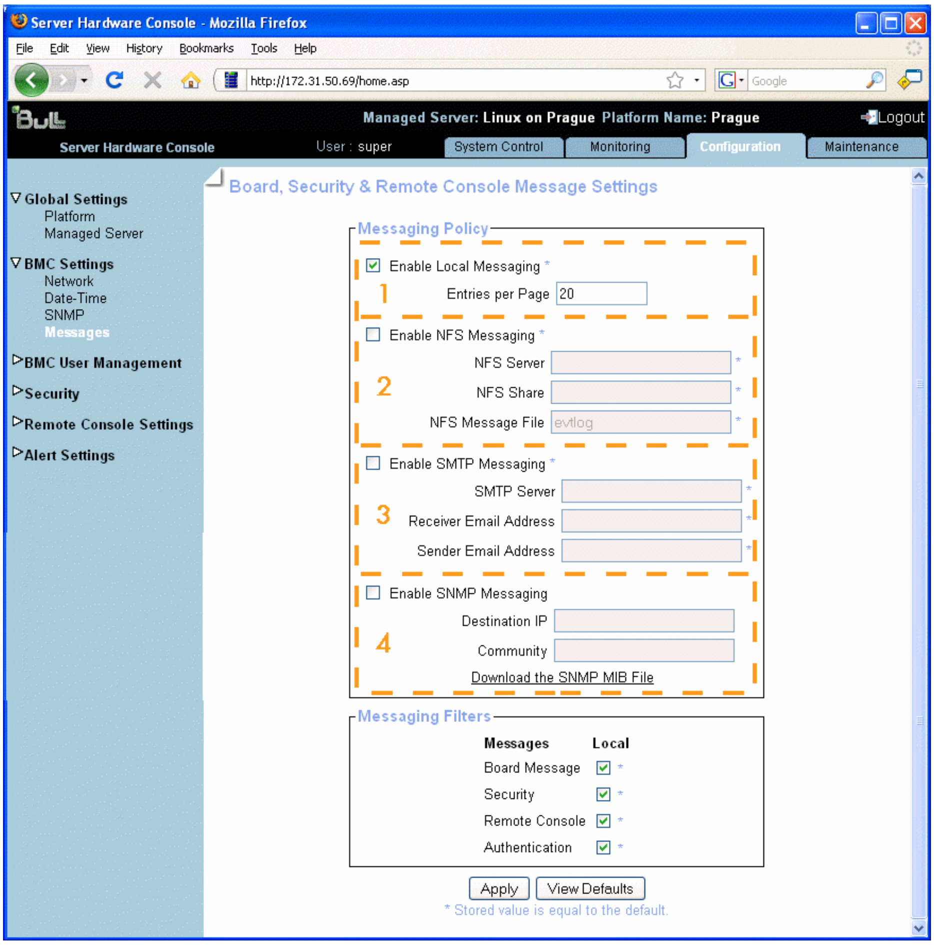
Important ***Alert and message transmission to the iCare Console must be set up directly from the iCare Console interface. Please refer to the** iCare Console User's Guide* ***for details.***

Prerequisites

- You have **Security/Log/Authentication Settings** permission.
- You have configured your NFS / SMTP / SNMP server for messaging.
- SNMP: You have enabled and configured the SNMP agent from **Configuration > General Settings > SNMP**.

Procedure

1. From the **Configuration** tab, click **BMC Settings > Messages** to display the **Board, Security & Remote Console Messages Settings** page:



Board, Security & Remote Console Message Settings

Messaging Policy

☑ Enable Local Messaging *

Entries per Page 20

□ Enable NFS Messaging *

NFS Server *

NFS Share *

NFS Message File evtlog *

□ Enable SMTP Messaging *

SMTP Server *

Receiver Email Address *

Sender Email Address *

□ Enable SNMP Messaging

Destination IP

Community

Download the SNMP MIB File

Messaging Filters

Messages	Local
Board Message	☑ *
Security	☑ *
Remote Console	☑ *
Authentication	☑ *

* Stored value is equal to the default.

Messaging Policy		
Area 1	**Enable Local Messaging**	This option is selected by default and allows message entries to be displayed in the **Board & Security Messages** page (**Monitoring** tab).
	• Entries per page	Maximum number of lines displayed in each **Board & Security Message** page. Enter a value between 1 and 100.
Area 2	**Enable NFS Messaging**	This option allows board and security messages to be written to a file located on a Network File System (NFS) server. **IMPORTANT:** • **The size of the NFS message file is not limited: each event is appended to the end of the file indefinitely. Depending on your hard disk space, you may have to empty or archive the file at regular intervals.** • **DO NOT use the same file name to write messages from more than one system using the same NFS shared directory.**
	• NFS Server	NFS server hostname or IP address.
	• NFS Share	Full pathname of the NFS shared directory. Note that the NFS shared directory is mounted immediately after you click the **Apply** button. To avoid error messages, use a valid NFS share value.
	• NFS Message File	Name of the file used to save the board and security messages.
Area 3	**Enable SMTP Messaging**	This option allows board and security messages to be sent by email to specified recipients. Emails contain the same description strings as the local messages and the mail subject is filled with the corresponding message group (Board Message, Security, Remote Console or Authentication).
	• SMTP Server	SMTP server IP address and port number. **The SMTP server MUST NOT require authentication**.
	• Receiver Email Address	Example: **administrator@mycompany.com**
	• Sender Email Address	Example: **system@mycompany.com**
Area 4	**Enable SNMP Messaging**	This option allows board and security messages to be sent by SNMP trap.
	• Destination IP	SNMP manager IP address and port number.
	• Community	(Optional) Example: **public**.
	• Download	Link allowing you to save, as a .txt file, the MIB file. This file is required by your SNMP manager to interpret trap messages.

Messaging Filter	
This box allows you to select message type and groups. Note: The columns displayed in this box depends on the messaging policies enabled.	
Board Message	This group consists of the following messages: • Device succesfully started. • Board Reset performed by user… • Firmware upload failed. • No firmware file uploaded. • Uploaded firmware file discarded. • Firmware validation failed. • Firmware file uploaded by user… • Firmware updated by user… • Internal log file cleared by user…
Security	This group consists of the following message: • Security Violation.
Remote Console	This group consists of the following messages: • Connection to Remote Console failed: <reason.> • Connection to client... established. • Connection to client ... closed.
Authentication	This group consists of the following messages: • Login failed. • Login succeed.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 25. Board, Security & Remote Console Messages Settings page - factory-default values

2. Complete the **Messaging Policy** box.
3. If necessary, modify the **Messaging Filter** box.
4. Click **Apply**.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Viewing Board and Security Messages, on page 5
- Enabling and Configuring the SNMP Agent, on page 4-8
- Configuring Alert Settings, on page 4-49

4.7. Managing Groups, Users and Permissions

Access to console features and data is based on users, groups and permissions. From the **Configuration** tab, use the **User Management** menu to implement a permission-based user management policy that enables users to only access the features and data they require.

4.7.1. Creating a User Account

The server is delivered with two predefined groups and one predefined user:

- **Admin** group with full permissions for full system access and one default **super** user .
- **User** group with no permissions and no predefined users.

You can create and manage users and associated permissions to suit your needs.

Note Predefined groups and users cannot be renamed or deleted, but the default **super** user password can be changed. Permissions for the default **Admin** group are not modifiable. Permissions for the default **User** group are modifiable.

Important **The server is equipped with a host-independent processor and memory unit which are limited in terms of processing instructions and memory space. To guarantee an acceptable response time, you are advised:**

- **Not to exceed 25 simultaneous user connections.**
- **Not to exceed 150 user accounts.**

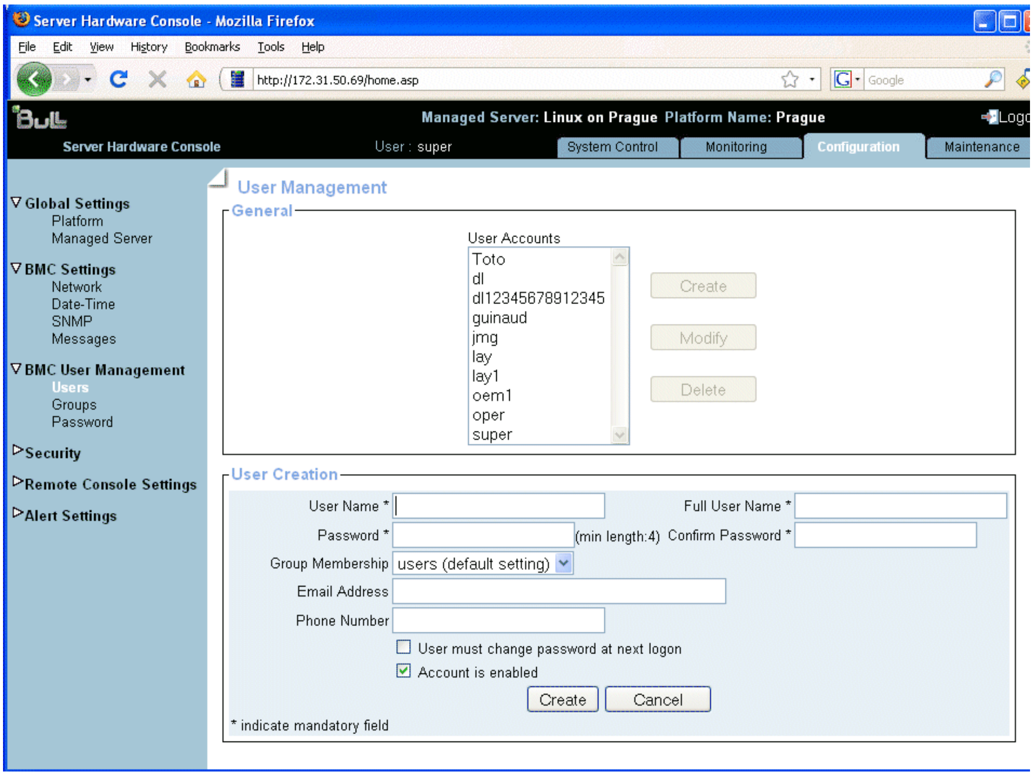
Prerequisites

- You have **User/Group Management** permission.
- You have created the group that the user is to be a member of.

Note If you have not created the group that the user is to be a member of, the newly created user will be attached to the predefined **users** group.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.
2. Click **Create** to display the **User Account Creation** dialog.



User Accounts: Toto, dl, dl12345678912345, guinaud, jmg, lay, lay1, oem1, oper, super

User Name *

Full User Name *

Password * (min length:4)

Confirm Password *

Group Membership: users (default setting)

Email Address

Phone Number

☐ User must change password at next logon

☑ Account is enabled

* indicate mandatory field

User Creation	
User Name	Name the user will use to log on (often a “short name”). • Name limited to 32 characters. • The following characters are not allowed: \"'`&*%|~?/ and space.
Full User Name	The user's full name. • Name limited to 32 characters. • The following characters are not allowed: \"'`&*%|~?/ and space.
Password	The password the user will use to log on. • Minimum password length: 4 characters. • Maximum password length: 32 characters. • The following character is not allowed: space.
Confirm Password	
Group Membership	Use this drop-down list to select the group that this user is to be a member of, according to the permissions you want the user to have. Note: If you do not select a group, the newly created user is automatically attached to the predefined **users** group. The **Change Password** permission is NOT enabled for the predefined **users** group.
Email Address	User's email address. Example: **john.smith@acme.com**.

User Creation (continued)	
Phone Number	User's phone number. Use only arabic numerals and optionally the characters .-+ with NO spaces. Examples: 0625252525, +33.1.25.25.25.25
User must change password at next logon	When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on.
Account is enabled	When cleared, this option makes the user account unavailable: the user's account information is maintained but it is no longer possible to log on using this account.

Figure 26. User Management page (User Creation box)

3. Complete the fields as required.
4. Click **Apply**. The user is created and appears in the **User Accounts** box.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Editing a User Account, on page 4-18
- Deleting a User Account, on page 4-22
- Creating a Group, on page 4-26
- Setting User and Group Permissions, on page 4-27
- Configuring Authentication Settings, on page 4-38
- Modifying your Password, on page 4-24

4.7.2. Viewing Existing User Account Details

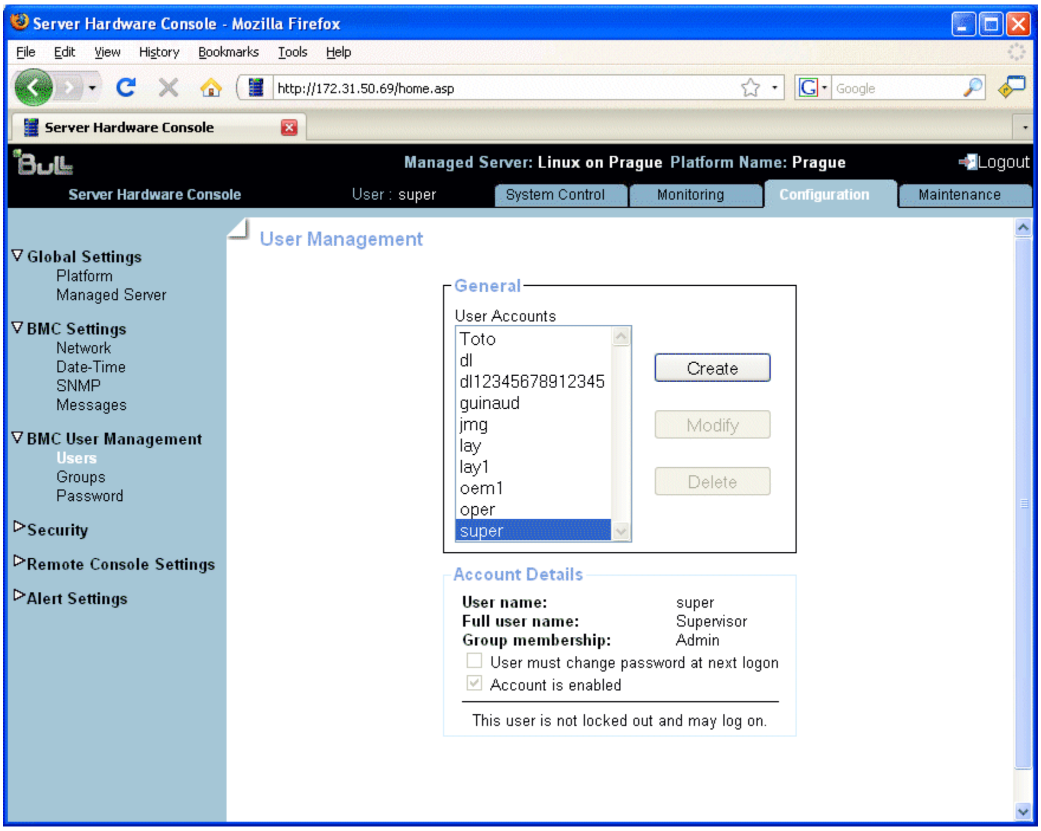
For easy user management, you can display the basic details of any user account at any time. You may want to use this feature, for example, to check user account details after the creation or modification of a user account or to check whether a user is locked out or not.

Prerequisites

You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users**. The **User Management** page appears.
2. In the **User Accounts** list, select a user to display the **Account Details** box.



User name: super
Full user name: Supervisor
Group membership: Admin

□ User must change password at next logon
☑ Account is enabled

This user is not locked out and may log on.

Account Details	
User Name	Name the user uses to log on (often a "short name").
Full User Name	The user's full name.
Group Membership	Group that this user is a member of (and consequently the permissions the user has).
Email Address	User's email address. This entry does not appear if the field is not completed when the user is created.
Phone Number	User's phone number. This entry does not appear if the field is not completed when the user is created.

Account Details (continued)	
User must change password at next logon	When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on.
Account is enabled	When selected, the user account is active and the user is able to log on.

Figure 27. User Management page (Account Details box)

Related Topics

- Editing a User Account, on page 4-18
- Creating a User Account, on page 4-14
- Deleting a User Account, on page 4-22

4.7.3. Editing a User Account

You can edit user account information at any time.

4.7.3.1. Changing User Account Details

You can change user account details (user name, full user name, password, email address and phone number) at any time. You might want to do this, for example, if a resource name is changed or if a resource changes roles in your organization.

Note You cannot change the account details of the predefined **super** user. However, the default **super** user password can be changed through the **Password Management** page, as detailed in Modifying your Password, on page 4-24.

Prerequisites

You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. Modify one (or more) of the following fields depending on your needs:
   - **User Name**,
   - **Full User Name**,
   - **Password** and **Confirm Password**,
   - **Email Address**,
   - **Phone Number**.

Note For details about these fields, see Figure 26, on page 4-16.

4. Click **Modify**. User account details are changed.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Changing Group Membership, on page 4-19
- Disabling/Enabling User Accounts, on page 4-20
- Forcing User Password Changes, on page 4-21

4.7.3.2. Changing Group Membership

A group is a collection of users who have the same permission requirements. Users automatically inherit the permissions of the group to which they belong. You can change permissions assigned to users by changing the group they are member of.

Prerequisites

- The group must be created.
- You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. Select in the **Group Membership** drop-down list the wanted group, according to the permissions you want the user to have.
4. Click **Modify**. The user's group membership is updated.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Creating a Group, on page 4-26
- Changing User Account Details, on page 4-18
- Disabling/Enabling User Accounts, on page 4-20
- Forcing User Password Changes, on page 4-21

4.7.3.3. Disabling/Enabling User Accounts

At times, you may need to make user accounts unavailable. You may want to use this feature, for example, when a maintenance intervention is scheduled. When you disable a user account, that user's account information is maintained but the user can no longer log on. The user account remains inactive until it is reenabled.

Prerequisites

You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management** > **Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. To disable the account, clear the **Account is enabled** check box; to enable the account, select it.
4. Click **Modify**. The account is updated.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Changing User Account Details, on page 4-18
- Changing User Account Details, on page 4-18
- Changing Group Membership, on page 4-19
- Forcing User Password Changes, on page 4-21
- Manually Unlocking a User Account, on page 4-23

4.7.3.4. Forcing User Password Changes

The following procedure describes how to force a user to change his/her password at the next logon.

Prerequisites

- You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management** > **Users** to display the **User Management** page.
2. Select the wanted user account in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. Check that **Change Password** permission is enabled for the group this user is a member of.

Important **This permission must be enabled for the group to which the user belongs otherwise he/she will not be able to log on.**

4. Select the **User must change password at next logon** check box.
5. Click **Modify**. The user will be requested to change his/her password the next time he/she tries to log on.

Note Once the user has changed his/her password, the **User must change password at next logon** check box of his/her account is automatically cleared.

Related Topics

- Changing Group Membership, on page 4-19
- Creating a Group, on page 4-26
- Changing User Account Details, on page 4-18
- Disabling/Enabling User Accounts, on page 4-20

4.7.4. Deleting a User Account

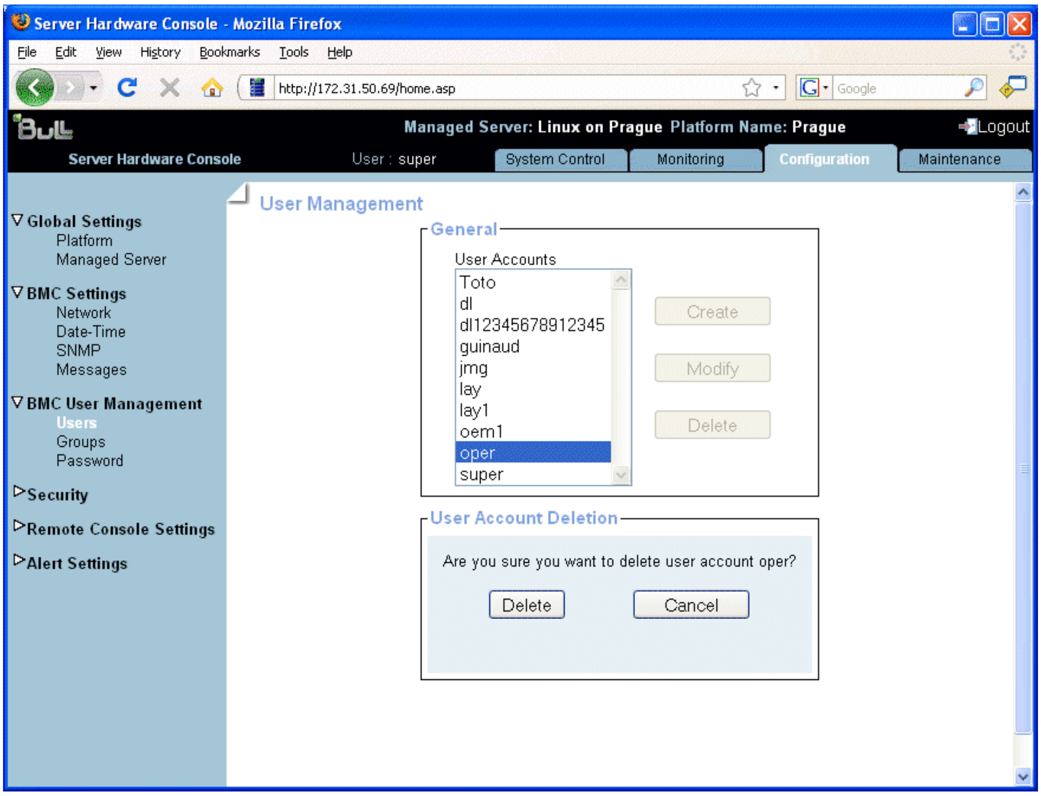
You can delete a user account when no longer needed. The deleted user account will be removed from the associated group.

Prerequisites

- You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.
2. Select a user in the **User Account** list box and click **Delete**. The **User Account Deletion** box appears.



User Accounts: Toto, dl, dl12345678912345, guinaud, jmg, lay, lay1, oem1, oper, super

Are you sure you want to delete user account oper?

Figure 28. User Account Deletion page

3. Click **Delete** to confirm. The user is removed from the list and from the associated group.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Creating a User Account, on page 4-14
- Creating a Group, on page 4-26
- Modifying your Password, on page 4-24

4.7.5. Manually Unlocking a User Account

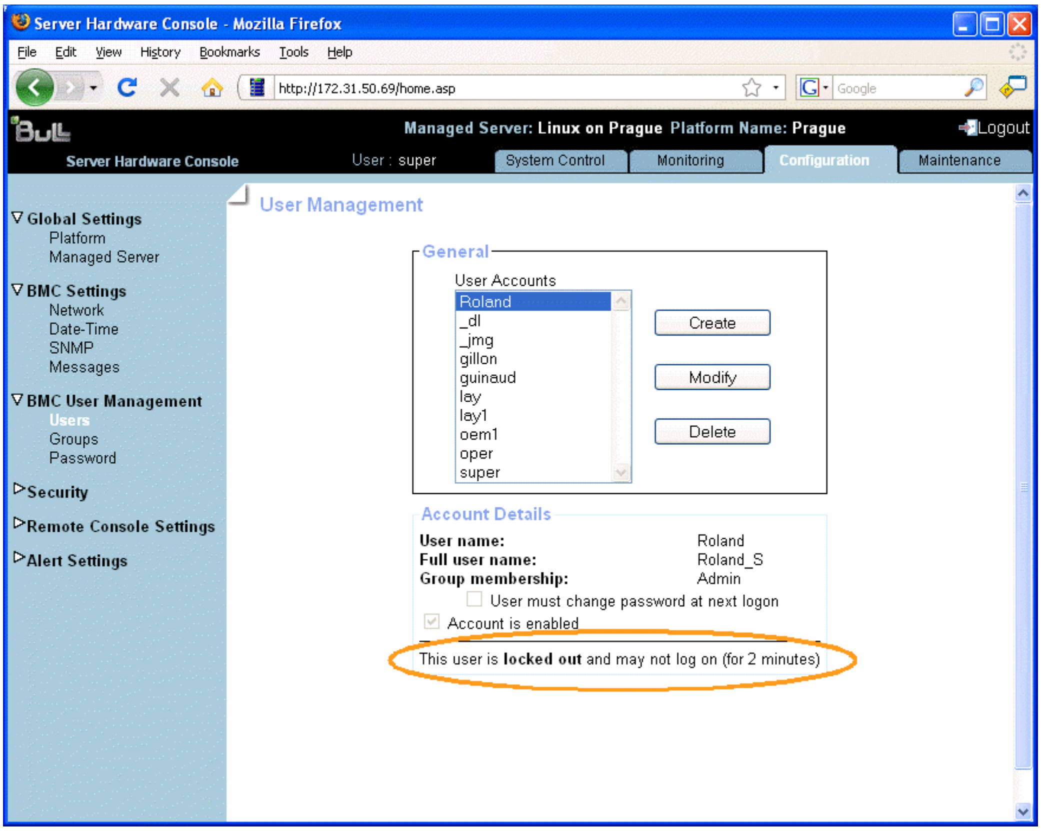
The user lockout feature disables a user account when a certain number of failed logons occur due to wrong passwords. When a user lockout duration is specified, the user account is automatically unlocked after the specified time. If a user lockout duration is not specified, the user account must be unlocked manually.

Prerequisites

- You have **Security/Log/Authentication Settings** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.
2. Select the locked-out user in the **User Account** list. The following message is displayed in the **Account Details** box:

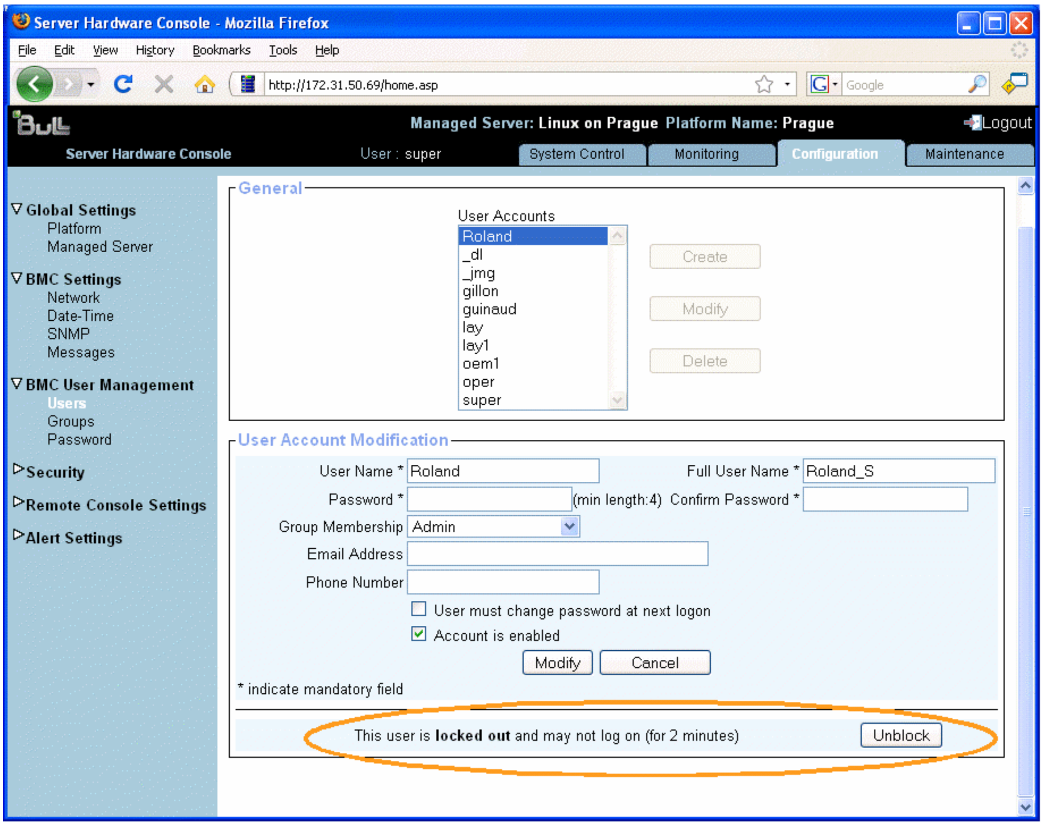


User name: Roland
Full user name: Roland_S
Group membership: Admin
☐ User must change password at next logon
☑ Account is enabled

This user is **locked out** and may not log on (for 2 minutes)

Figure 29. User Management page - Locked-out user

3. Click Modify to display the User Account Modification box.



User Accounts: Roland, _dl, _img, gillon, guinaud, lay, lay1, oem1, oper, super

User Name * Roland

Full User Name * Roland_S

Password * (min length:4) Confirm Password *

Group Membership Admin

Email Address

Phone Number

□ User must change password at next logon

☑ Account is enabled

* indicate mandatory field

This user is **locked out** and may not log on (for 2 minutes)

Figure 30. User Management page - Unblock button

4. Click Unblock. The user account is unlocked and the user can now log on again.

Related Topics

- Configuring User Account Lockout Parameters, on page 41
- Configuring Authentication Settings, on page 37

4.7.6. Modifying your Password

The following procedure explains how to change your current user account password.

Important **When you change the Super user password, you are advised to use the same password for all your managed resources. This will enable you to interface easily with the iCare Console.**

Prerequisites

- You have **Change Password** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Password**. The **Password Management** page appears.

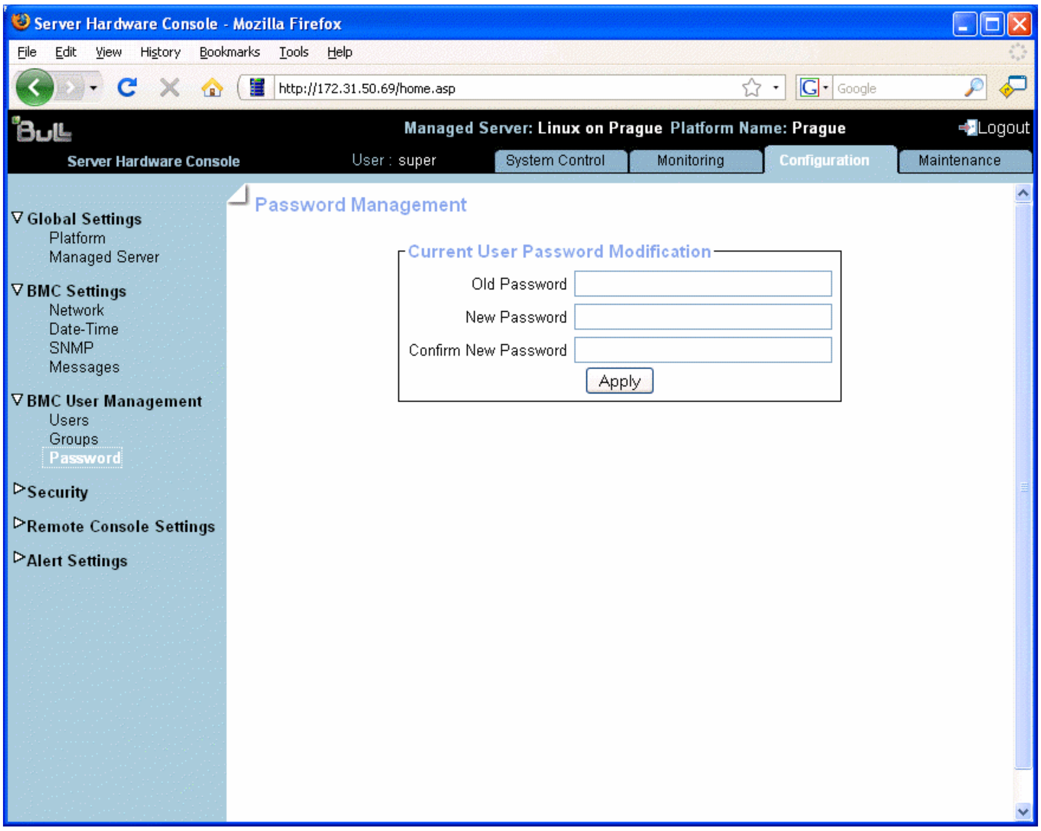


Figure 31. Password Management page

Important

- **Minimum password length: 4 characters.**
- **Maximum password length: 32 characters.**
- **The space character is forbidden.**

2. Complete the 3 fields.
3. Click **Apply**. Your new password is now valid and must be used when you next log on.

Related Topics

- Creating a User Account, on page 4-14
- Deleting a User Account, on page 4-22

4.7.7. Creating a Group

The Hardware Console is delivered with two predefined groups and one predefined user:

- **Admin** group with full permissions for full system access and one default **super** user.
- **User** group with no permissions and no predefined users.

You can create and manage new groups and associated permissions to suit your needs.

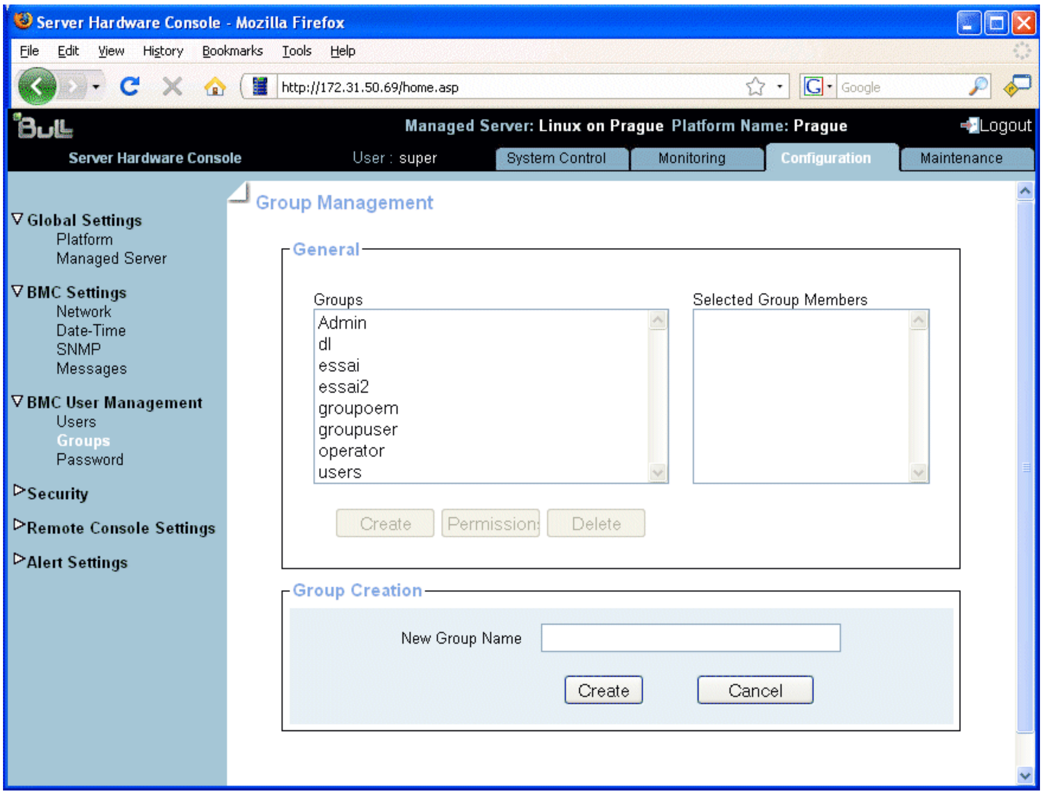
Important **Predefined groups and users cannot be renamed or deleted, but the default super user password can be changed.**
Permissions for the Admin group are not modifiable.
Permissions for the User group are modifiable.

Prerequisites

You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management** > **Groups**. The **Group Management** page appears.
2. Click **Create** to open the **Group Creation** box.



Groups: Admin, dl, essai, essai2, groupoem, groupuser, operator, users

New Group Name

Group Creation	
New Group Name	Name given to the group. Restrictions: • Name limited to 32 characters. • The following characters are not allowed: \"'`&*%|~?/ and space.

Figure 32. Group Management page description (Group Creation box)

3. Enter the group name in the **New Group Name** field and click **Create**. The group is created and appears in the **Groups** box. You can now proceed to define permissions and set up users for the group.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Setting User and Group Permissions, on page 4-27
- Creating a User Account, on page 4-14
- Editing a User Account, on page 4-18
- Deleting a Group, on page 4-32
- Deleting a User Account, on page 4-22

4.7.8. Setting User and Group Permissions

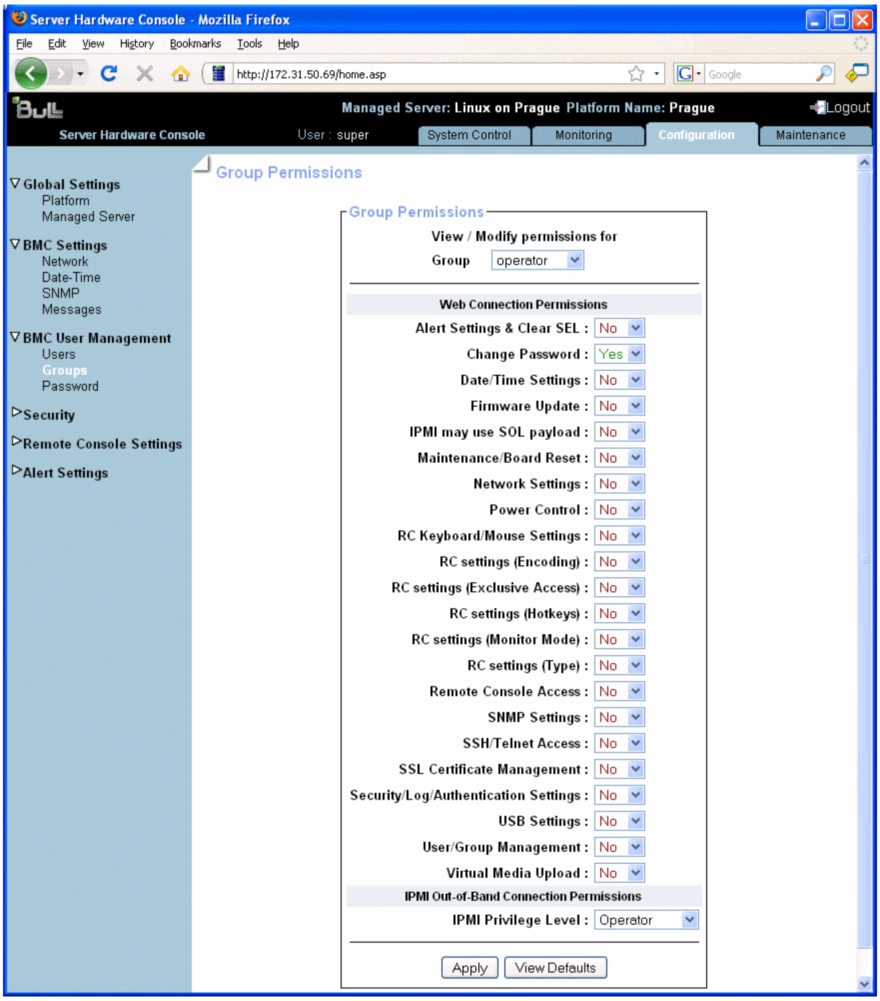
The features accessible to a user depend on the permissions defined for the group the user belongs to. This section describes how to specify and update the permissions that apply to users associated with a group.

Prerequisites

- You have **User/Group Management** permission.
- You have **Group Permissions** permission.
- You have created the group for which you want to set permissions.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Groups** to display the **Group Management** page.
2. Select the group and click **Permissions** to display the **Group Permissions** page:



Server Hardware Console - Mozilla Firefox

http://172.31.50.69/home.asp

Managed Server: Linux on Prague Platform Name: Prague

Server Hardware Console User : super

Group Permissions

Group Permissions

View / Modify permissions for

Group: operator

Web Connection Permissions	
Alert Settings & Clear SEL :	No
Change Password :	Yes
Date/Time Settings :	No
Firmware Update :	No
IPMI may use SOL payload :	No
Maintenance/Board Reset :	No
Network Settings :	No
Power Control :	No
RC Keyboard/Mouse Settings :	No
RC settings (Encoding) :	No
RC settings (Exclusive Access) :	No
RC settings (Hotkeys) :	No
RC settings (Monitor Mode) :	No
RC settings (Type) :	No
Remote Console Access :	No
SNMP Settings :	No
SSH/Telnet Access :	No
SSL Certificate Management :	No
Security/Log/Authentication Settings :	No
USB Settings :	No
User/Group Management :	No
Virtual Media Upload :	No
IPMI Out-of-Band Connection Permissions	
IPMI Privilege Level :	Operator

Group Permissions	
View / Modify Permissions for Group	This drop-down list allows you to select a group in order to view and/or modify the permissions set for the selected group.
Web Connection Permissions	This list allows you to enable or disable console features for the selected group. Select either **Yes** or **No** to enable or disable the feature(s) associated with each permission and click **Apply**. Use Tables 6 and 7 to help you select permissions. Note: Certain features are accessible to all users and the associated non-configurable permissions are not listed in this page.
IPMI Out-of-Band Connection Permissions	The **IPMI Privilege Level** drop-down list allows you to set a role for the selected group. See Table 8 and the IPMI specification for more details.

Figure 33. Group Permissions page description

3. Use Tables 6 and 7 below to help you select the permissions you want to assign to the selected group.

4. Click **Apply** to validate the selected permissions for the group.

5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

The following tables list permissions and associated features.

Console: Non-Configurable Permissions

Feature	Tab
Power Information: Viewing & Refreshing	System Control
Sensor Status	Monitoring
System Event Log: Viewing & Refreshing	Monitoring
Management Board	Maintenance
FRU	Maintenance
Firmware Version	Maintenance
Connected Users	Maintenance

Table 6. Console : Non-configurable permissions

Console: Configurable Permissions

Configurable Permission	Feature	Tab
Alert Settings & Clear SEL	System Event Log: Clearing	Monitoring
	Filters	Configuration
	Policies	Configuration
	LAN Destinations	Configuration
	General	Configuration
	Identification LED	Maintenance
Change Password	Password	Configuration
Date/Time Settings	Date-Time	Configuration
Firmware Update	*Listed Firmware Upgrades*	Maintenance
IPMI may use SOL payload	*Reserved*	-
Maintenance/Board Reset	Board Reset	Maintenance
	Hardware Exclusion	Maintenance
Network Settings	Platform	Configuration
	Managed Server	Configuration
	Network	Configuration
Power Control	Power Management	Power Control
RC Keyboard/Mouse Settings	Keyboard & Mouse	Configuration
RC settings (Encoding)	Transmission Encoding	Configuration
RC settings (Exclusive Access)	Miscellaneous Remote Console Settings	Configuration
RC settings (Hotkeys)	Mouse Hotkey	Configuration
RC settings (Monitor mode)	Remote Console Button Key	Configuration
RC settings (Type)	*Reserved*	-
Remote Console Access	Preview	System Control
	Launch	System Control
SNMP Settings	SNMP	Configuration

Configurable Permission (continued)	Feature (continued)	Tab (continued)
SSH/Telnet Access	SSH/Telnet connection	-
SSL Certificate Management	SSL Certificate	Configuration
Security/Log/Authentication Settings	Messages	Monitoring
	Encryption	Configuration
	User Logon Policy	Configuration
	Authentication	Configuration
	Power Button Lockout	Configuration
	User Lockout	Configuration
USB Settings	*Reserved*	-
User/Group Management	Users	Configuration
	Groups: Management	Configuration
	Groups: Permissions	Configuration
Virtual Media Upload	*Listed Virtual Media*	System Control

Table 7. Console: Configurable permissions

IPMI Out-of-Band Privileges	
IPMI Privilege Level	Possible values: • No Access • Callback • User • Operator • Administrator • OEM For more details about IPMI privilege levels, refer to the IPMI specification.

Table 8. IPMI: Out-of-Band privileges

Related Topics

- Creating a Group, on page 4-26
- Creating a User Account, on page 4-14
- Deleting a User Account, on page 4-22

4.7.9. Viewing Existing Groups and Members

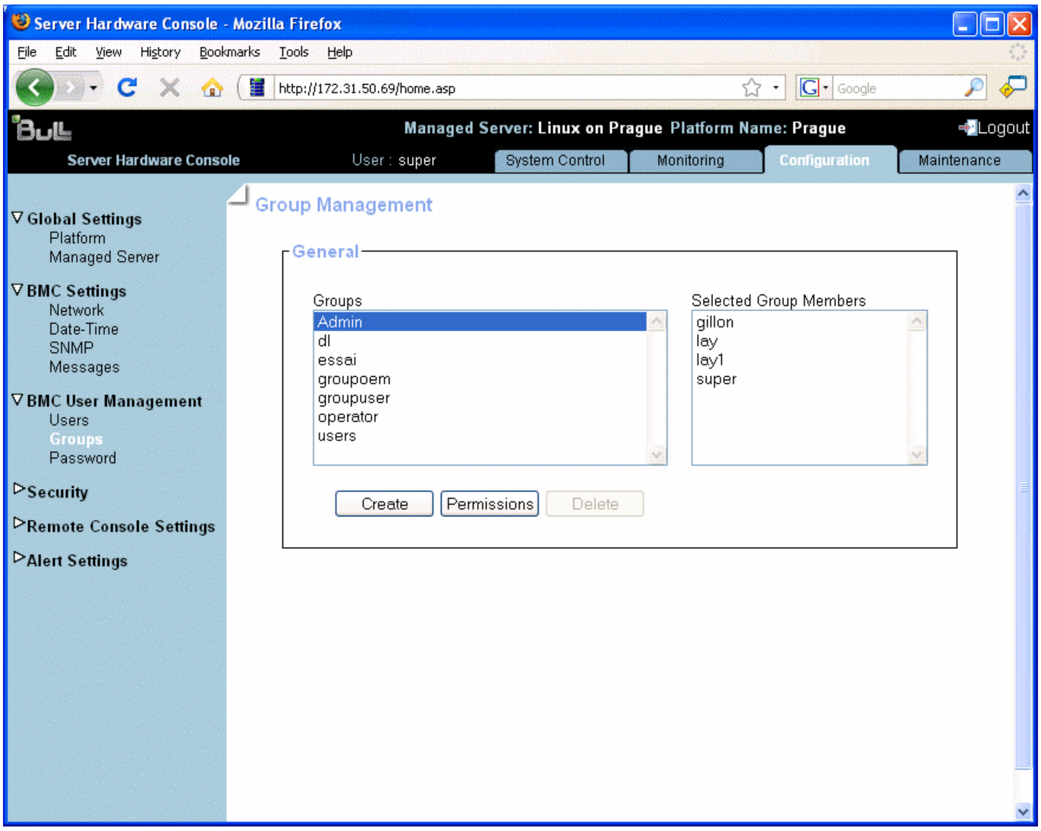
For easy group management, you can display the members of any group at any time. You may want to use this feature, for example, to check group membership after the creation or modification of a user account.

Prerequisites

You have **User/Group Management** permission.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Groups**. The **Group Management** page appears.
2. In the **Groups** list, select a group. The group members appear in the **Selected Group Members** list.



Groups: Admin, dl, essai, groupoem, groupuser, operator, users

Selected Group Members: gillon, lay, lay1, super

Figure 34. Group Management page

4.7.10. Deleting a Group

You can delete an empty group when no longer needed.

Important **Predefined groups and users cannot be deleted.**

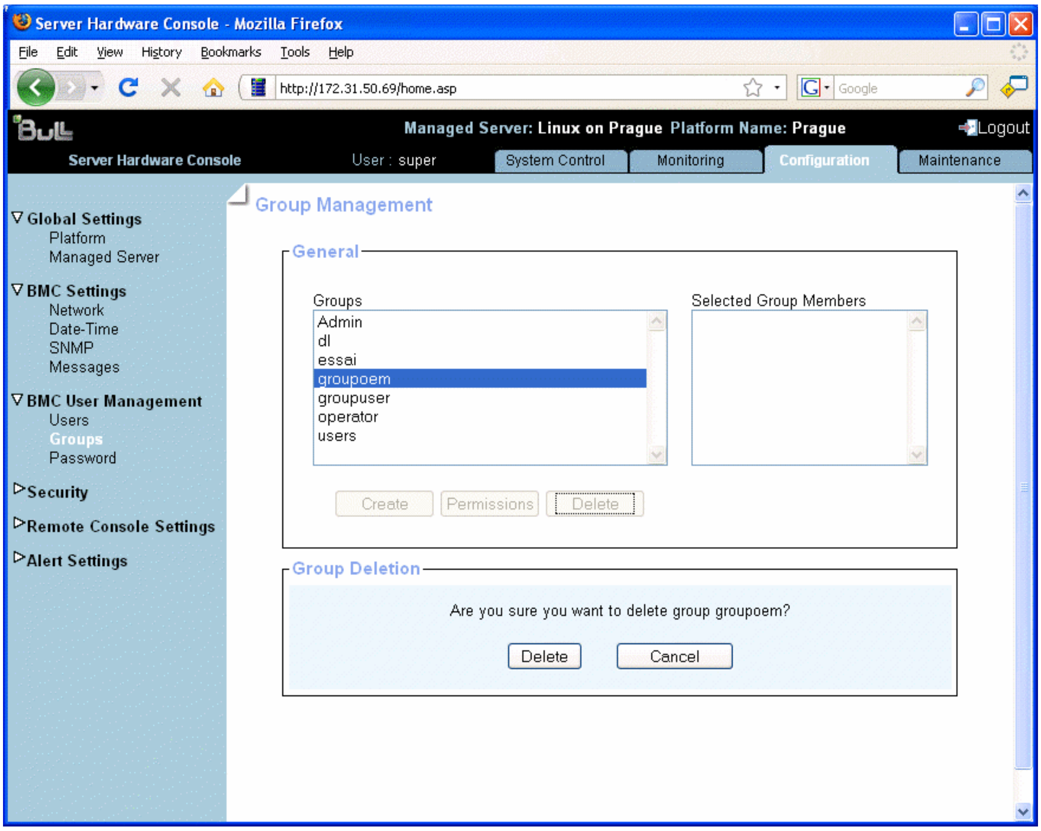
Prerequisites

- You have **User/Group Management** permission.
- No users are members of the group to be deleted, i.e. users have been deleted or moved to another group.

Procedure

1. From the **Configuration** tab, click **BMC User Management > Groups**. The **Group Management** page appears.
2. Select the group you want to delete in the **Groups** list box and click **Delete** to open the **Group Deletion** box.

Note If the selected group contains users, the **Delete** button is not available.



Group Management

General

Groups: Admin, dl, essai, groupoem, groupuser, operator, users

Selected Group Members

Group Deletion

Are you sure you want to delete group groupoem?

Figure 35. Group Management page description (Group Deletion box)

3. Click **Delete**. The group is deleted and disappears from the **Groups** box.

4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Creating a Group, on page 4-26
- Editing a User Account, on page 4-18
- Deleting a User Account, on page 4-22

4.8. Configuring Security Parameters

For optimum security, a comprehensive set of security features can be customized to suit your requirements. These features range from securing web connections to controlling the use of the physical power button.

4.8.1. Enabling/Disabling Encryption

This feature allows you to secure Web connections to the console and to control the encryption mode of the KVM protocol, which is activated when using the Remote System Console.

Important **By default, a temporary certificate is delivered to connect to the console with the HTTPS protocol. For optimum security, you are advised to generate and install your own certificate.**

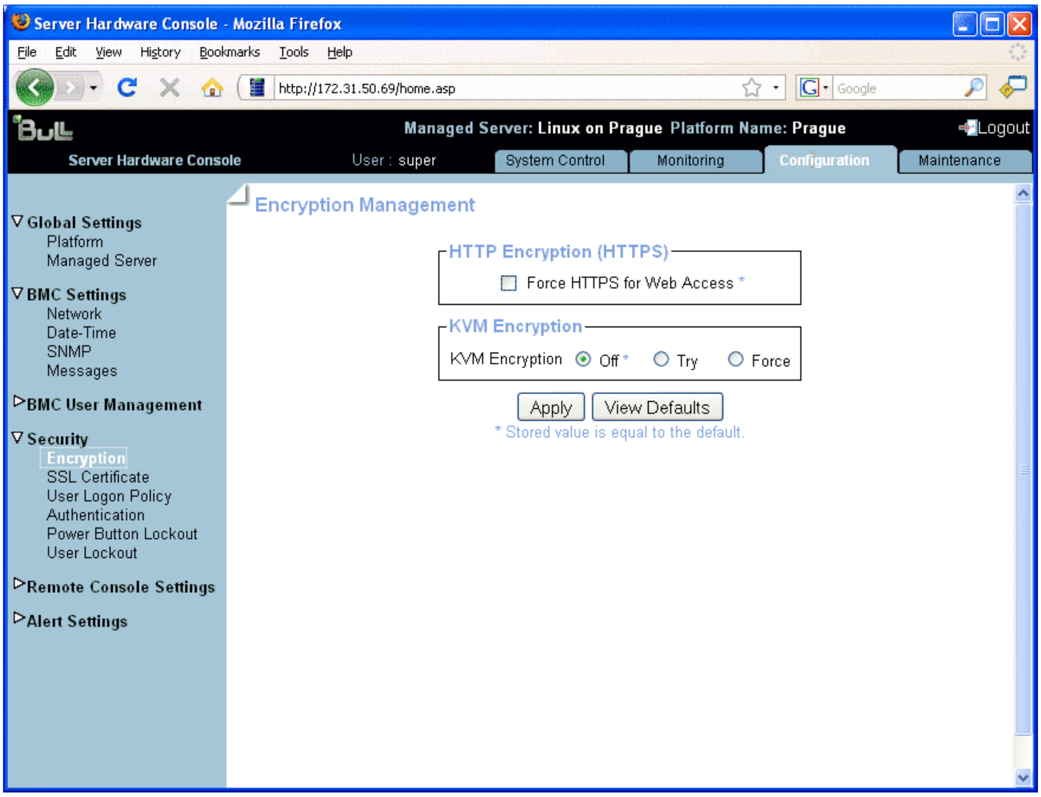
Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring or Modifying Network Settings, on page 4-4

Prerequisites

- You have **Security/Log/Authentication Settings** permission.

Procedure

1. From the **Configuration** tab, click **Security > Encryption**. The **Encryption Management** page appears.



Encryption Management

HTTP Encryption (HTTPS)

☐ Force HTTPS for Web Access *

KVM Encryption

KVM Encryption ● Off * ○ Try ○ Force

Apply | View Defaults

* Stored value is equal to the default.

HTTP Encryption (HTTPS)	
Force HTTPS for Web Access	The HTTPS protocol requires the use of an URL in one of the following formats: • https://<IP Address> • https://<Hostname> IMPORTANT: if this option is selected, the HTTP protocol (http://<IP address or hostname>) can no longer be used to connect to the Hardware Console.
KVM Encryption	
KVM Encryption	This option controls the encryption of the KVM protocol. This protocol is used by the Remote System Console to transmit the screen data to the administrator machine and the keyboard and mouse data back to the host. • If set to **Off**, encryption is disabled. • If set to **Try**, the Remote System Console tries to make an encrypted connection. If the encrypted connection cannot be established, an unencrypted connection is used instead. • If set to **Force**, the Remote System Console tries to make an encrypted connection. If the encrypted connection cannot be established, an error is reported.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 36. Encryption Management page - factory-default values

2. Select the wanted options and click **Apply**.

3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Getting and Installing a New SSL Certificate, on page 4-35
- Configuring or Modifying Network Settings, on page 4-4

4.8.2. Getting and Installing a New SSL Certificate

You can secure Web connections by configuring the console to use the HTTPS protocol.

A valid SSL certificate is required to use the HTTPS protocol. By default, a temporary certificate is delivered. For optimum security, you are advised to generate and install your own certificate.

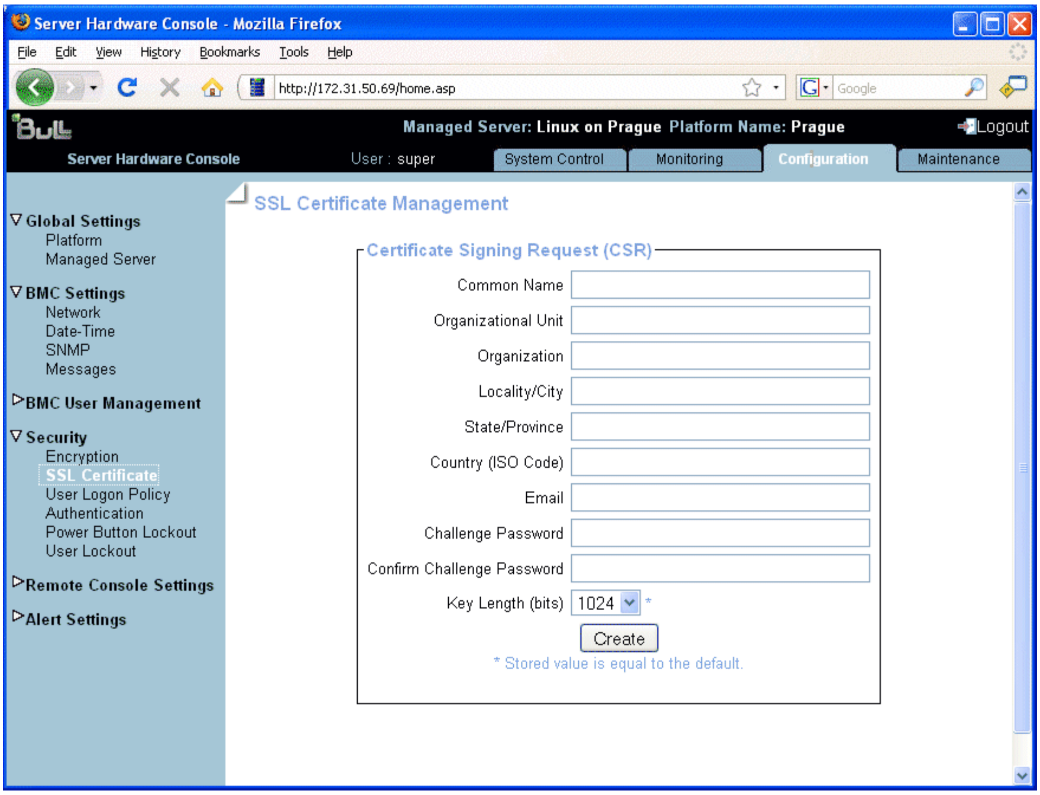
Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring or Modifying Network Settings, on page 4-4

Prerequisites

- You have **SSL Certificate Management** permission.

Procedure

1. From the **Configuration** tab, click **Security > SSL Certificate** to display the **SSL Certificate Management** page.



Common Name

Organizational Unit

Organization

Locality/City

State/Province

Country (ISO Code)

Email

Challenge Password

Confirm Challenge Password

Key Length (bits) 1024 *

* Stored value is equal to the default.

Certificate Signing Request (CSR)	
Common Name	“Fully Qualified Domain Name” (FQDN) (example : hostName.DomainName.Top-LevelDomain). If the Common Name differs from the network name, a security warning will pop up when the server is accessed using HTTPS.
Organizational Unit	Generally the name of the department (within your organization) using the server (example: **Research and Development**).
Organization	Name of your organization.
Locality/City	Name of your city.
State/Province	Name of your state, province or region.
Country (ISO Code)	ISO Code for your country (example: FR for France).
Email	Generally the administrator's email address.
Challenge Password	Depending on your certification authority, you may need to define a challenge password to authorize later changes to the certificate (example: revocation of the certificate). **The minimal length of this password is four characters.**
Confirm Challenge Password	
Key Length (bits)	Length of the generated key in bits. Generally 1024 bits. Longer keys may result in slower connection response time.

Figure 37. SSL Certificate Management page description

2. Complete the fields and click **Create** to generate your CSR.
3. Click **Download** to save the CSR to your computer and send it to the Certification Authority, which will check your information, generate a signed Certificate and send it back to you.
4. When you receive your signed certificate, use the **Certificate Upload** box to install the certificate.
5. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Enabling/Disabling Encryption, on page 4-33
- Configuring or Modifying Network Settings, on page 4-4

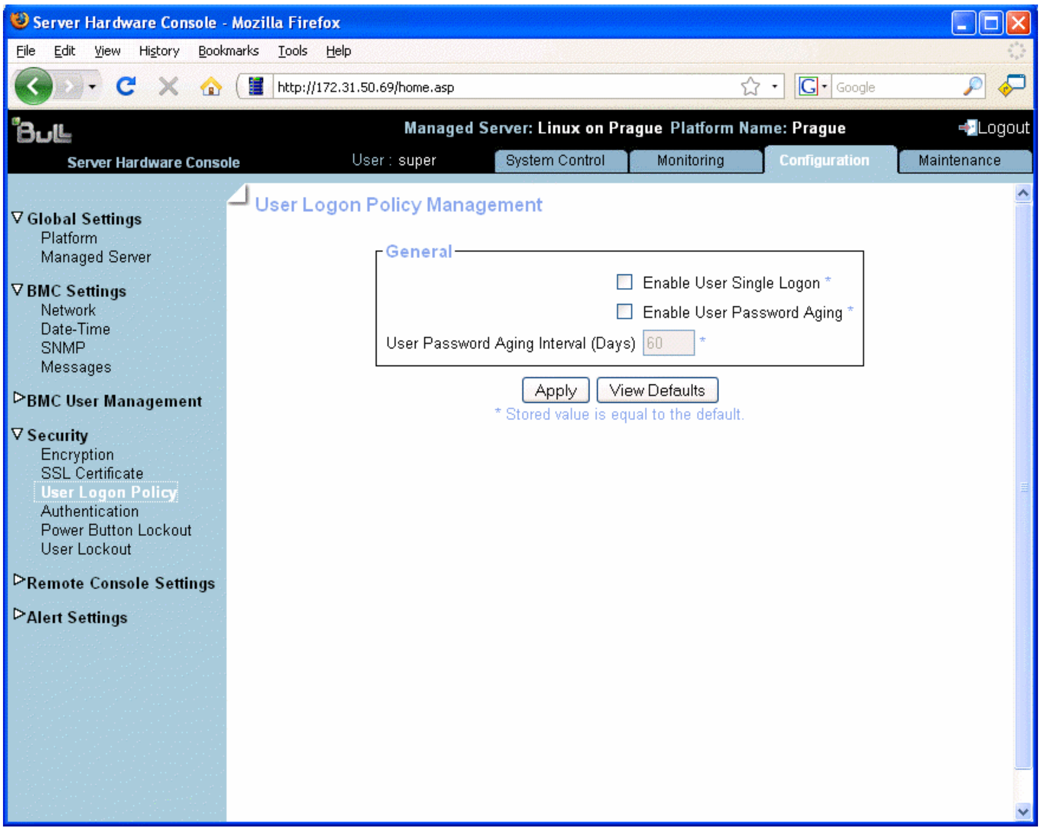
4.8.3. Configuring Logon Policy Settings

Prerequisites

- You have **Security/Log/Authentication Settings** permission.
- You log on with the user account you want to configure.

Procedure

1. From the **Configuration** tab, click **Security > User Logon Policy** to display the **User Logon Policy Management** page.



User Logon Policy Management

General

□ Enable User Single Logon *

□ Enable User Password Aging *

User Password Aging Interval (Days) 60 *

* Stored value is equal to the default.

General	
Enable User Single Logon	When this check box is selected, the current user account is limited to a single session logon: once connected, it is not possible to log on to the console again using the same user account.
Enable User Password Aging	When this check box is selected, the user has to change his/her password at the specified interval.
User Password Aging Interval (Days)	Password change interval, in days.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 38. User Logon Policy Management page - factory-default values

2. Select or clear the check boxes as required and click **Apply**.

3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring Authentication Settings, on page 4-38
- Configuring User Account Lockout Parameters, on page 4-42

4.8.4. Configuring Authentication Settings

By default, the console is configured to use its own **Local Authentication** mechanism to authenticate and connect users. You can either use this mechanism and manually create groups and user accounts or use your organization's LDAP or RADIUS server to use existing user accounts.

Important

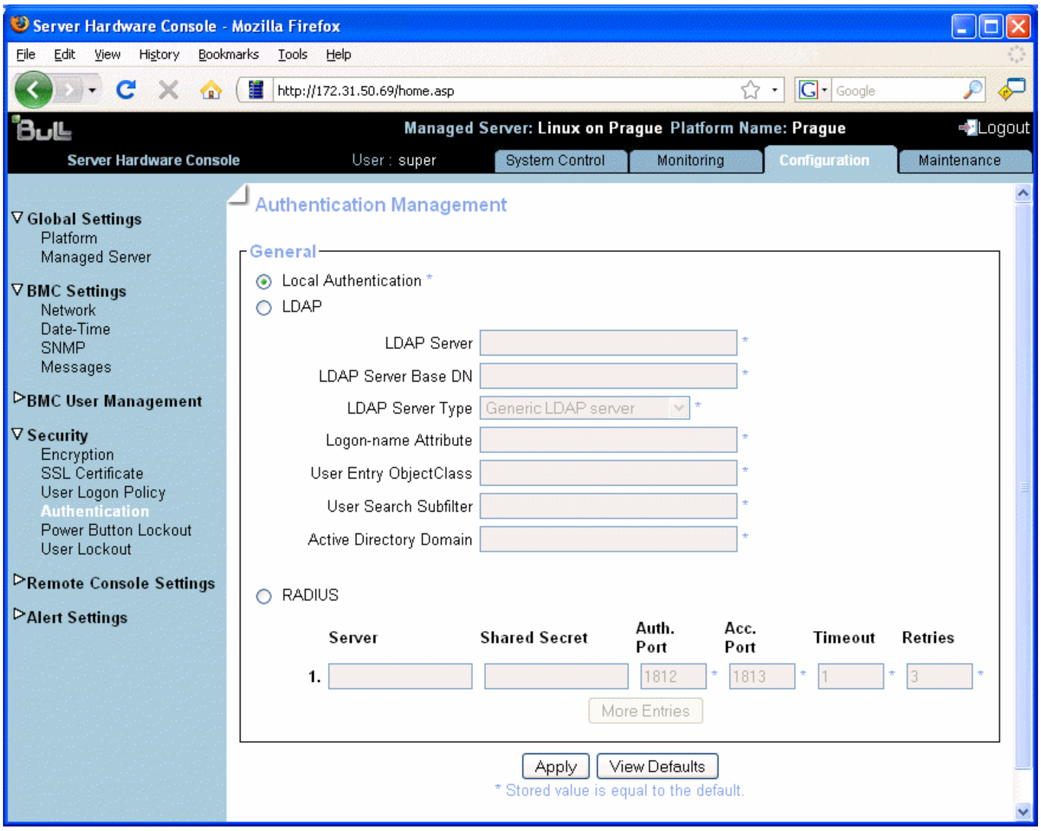
- **If you select LDAP authentication management, the LDAP database is only used for password verification. User permissions and private settings are still stored locally. You need to create user accounts via the console (User Management page) if you want users to log on using an LDAP server.**
- **The default "super" user account can always be used, whatever the authentication settings.**

Prerequisites

- You have **Security/Log/Authentication Settings** permission.
- For LDAP or RADIUS authentication management, you have configured the DNS server from the **Enterprise Network Settings** page.
- For RADIUS authentication management, you have declared the console as a RADIUS client (name and IP address) and have defined the shared secret.

Procedure

1. From the **Configuration** tab, click **Security > Authentication** to display the **Authentication Management** page.



Authentication Management

General

● Local Authentication *

○ LDAP

LDAP Server *

LDAP Server Base DN *

LDAP Server Type: Generic LDAP server *

Logon-name Attribute *

User Entry ObjectClass *

User Search Subfilter *

Active Directory Domain *

○ RADIUS

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.			1812 *	1813 *	1 *	3 *

* Stored value is equal to the default.

General	
Local Authentication	Enables the console's local authentication mechanism.
LDAP	Enables LDAP server authentication.
• LDAP Server	LDAP server's hostname or IP address.
• LDAP Server Base DN	Starting node to begin the search of user accounts. Example: **dc=users,dc=domain,dc=com**
• LDAP Server Type	• **Novell Directory Service** if you are using Novell eDirectory. • **Microsoft Active Directory**. • **Generic LDAP Server** if you are using any other LDAP directory.
• Logon Name Attribute	If you have selected **Novell Directory Service** or **Microsoft Active Directory**, leave these fields blank to use the directory's default value. • **Logon Name Attribute**: LDAP attribute used as user name to connect to the LDAP directory Example: **cn**. • **User Entry Object Class**: object class that identifies a user in the directory Example: **organizationalPerson**.
• User Entry Object Class	
• User Search Subfilter	Restricts the search to certain user accounts. (example: **(&(objectClass=person)(ou=System Validation))**)

General (continued)	
• Active Directory Domain	(**Microsoft Active Directory** only): Active Directory domain as it is configured in your Active Directory server. Example: **users.domain.com**
RADIUS	Enables RADIUS authentication
• Server Name	RADIUS server's hostname or IP address.
• Shared Secret	A shared secret is a text string used as a password between the RADIUS client and the RADIUS server. You can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z,a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation mark (!) or an asterisk (*).
• Auth. Port	RADIUS server port number used to listen to authentication requests (**#1812** by default).
• Acc. Port	RADIUS server port number used to listen to accounting requests (**#1813** by default).
• Timeout	Maximum amount of time in seconds to wait for the completion of the request. If the requested job is not completed within this interval of time it is cancelled.
• Retries	Number of retries if a request cannot be completed.
• More Entries	If you are using several RADIUS servers, click this button to add authentication configurations.
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 39. Authentication Settings page - factory-default values

2. Depending on your needs, click **Local Authentication**, **LDAP** or **RADIUS** and complete the appropriate fields and click **Apply**.
3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring or Modifying Network Settings, on page 4-4
- Creating a User Account, on page 4-14
- Setting User and Group Permissions, on page 4-27

4.8.5. Enabling/Disabling the Power Button

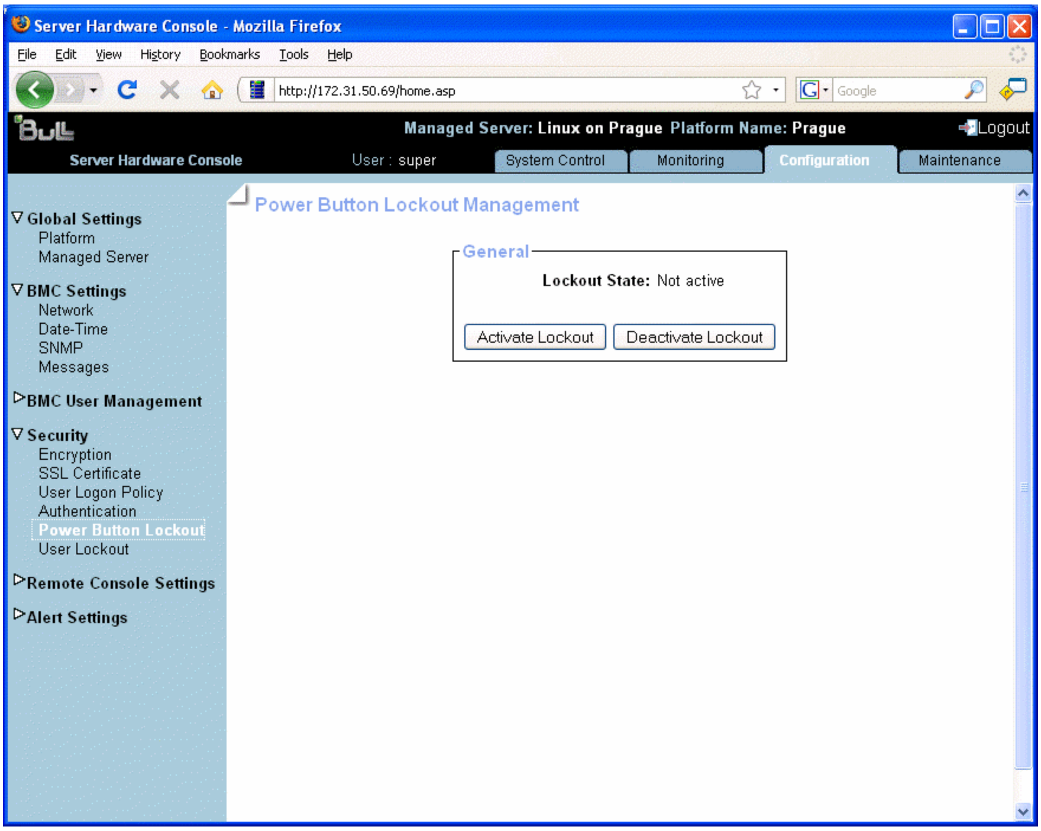
The server is equipped with a physical power button, located on the LCP. This power button can be locked to prevent tampering.

Prerequisites

You have **Security/Log/Authentication Settings** permission.

Procedure

1. From the **Configuration** tab, click **Security > Power Button Lockout** to open the **Power Button Lockout Management** page.



Lockout State: Not active

General	
Lockout State	2 possible values: • **Active:** the power button is locked. • **Not active:** the power button is unlocked.
Activate Lockout	Disables the LCP power button.
Deactivate Lockout	Enables the LCP power button.

Figure 40. Power Button Lockout Management page description

2. Click **Activate Lockout** or **Deactivate Lockout**, as required.

Related Topics

- Powering On the Server, on page 2-6
- Viewing Server Power Status, on page 2-4

4.8.6. Configuring User Account Lockout Parameters

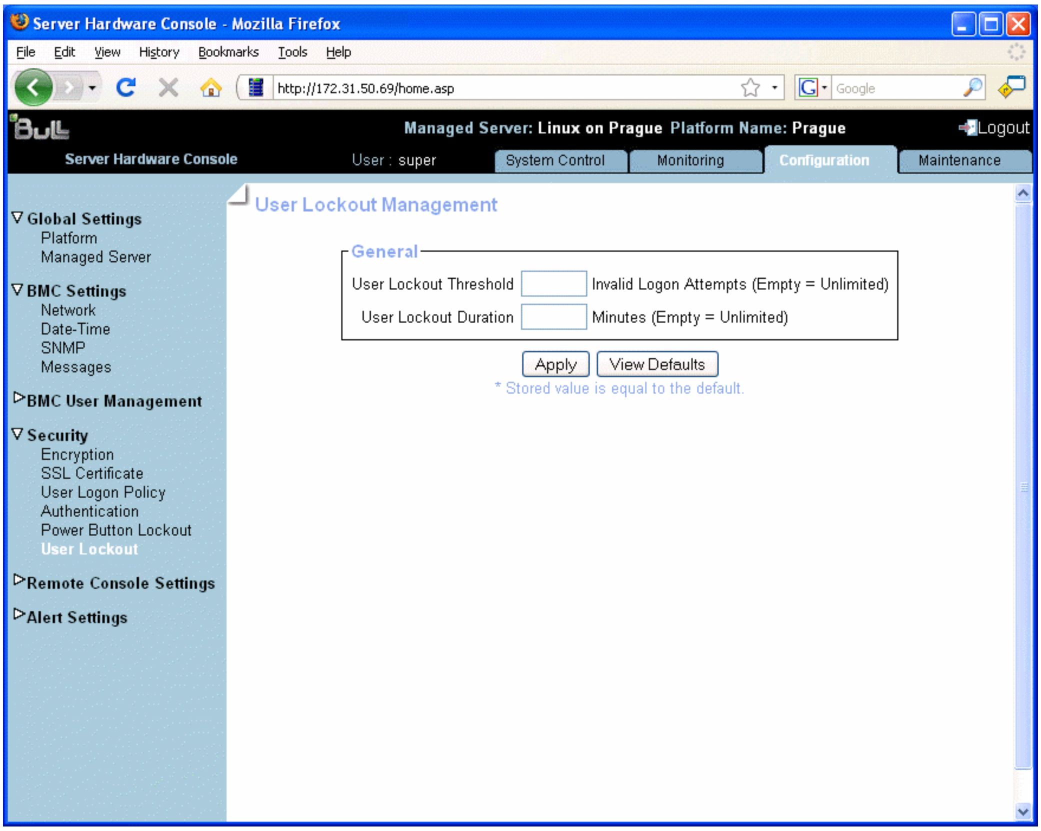
The user lockout feature disables a user account when a certain number of failed logons occur due to wrong passwords.

Prerequisites

- You have **Security/Log/Authentication Settings** permission.
- You have logged on with the user account to configure.

Procedure

1. From the **Configuration** tab, click **Security > User Lockout** to display the **User Lockout Management** page.



User Lockout Management

General

User Lockout Threshold ______ Invalid Logon Attempts (Empty = Unlimited)

User Lockout Duration ______ Minutes (Empty = Unlimited)

* Stored value is equal to the default.

General	
User Lockout Threshold	Maximum number of invalid logon attempts before locking the user account. Note: If you leave this field empty, the user account will never be locked.
User Lockout Duration	Enter a time in minutes during which the user account is to remain locked. Once this time is passed, the user account is automatically unlocked. Note: If you leave this field empty, a locked user account stays locked until you unlock it manually.
View **Defaults** button	Allows you to display factory-default values (shown in this figure).

Figure 41. User Lockout Management page - factory-default values

2. Complete the fields and click **Apply**.
3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring Authentication Settings, on page 4-38
- Configuring Logon Policy Settings, on page 4-37
- Manually Unlocking a User Account, on page 22

4.9. Setting Up the Remote System Console

The Remote System Console feature is used to connect directly to the server from the Hardware Console, allowing you to remotely view, use and control the server with the keyboard, video and mouse on your local computer.

The Remote System Console can be configured to suit your needs.

4.9.1. Configuring Remote System Console Settings

The **Remote Console Settings** page allows you to configure many parameters in order to:

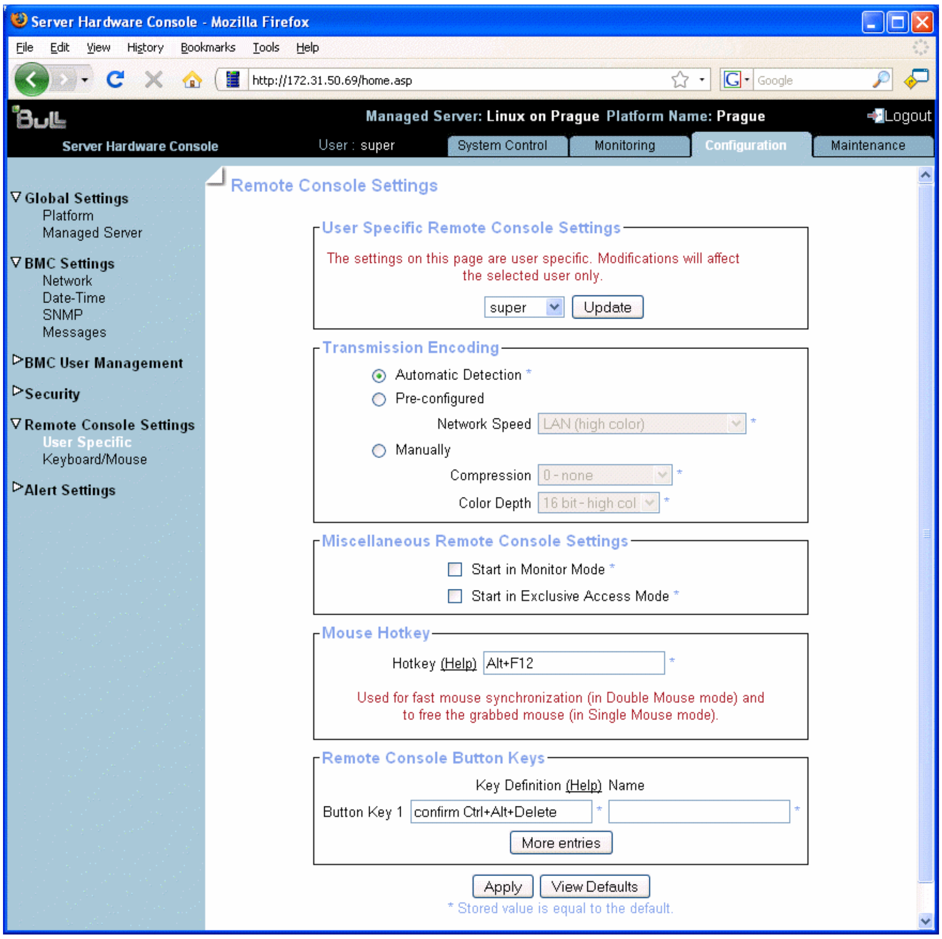
- Improve Remote System Console display performance.
- Set default start options.
- Specify a keystroke shortcut to launch the mouse synchronization process.
- Configure the keystroke combinations button displayed in the Remote System Console Control bar.

Prerequisites

- User specific settings: you are using the **super** user account.
- Transmission encoding settings: you have the **RC Settings (Encoding)** permission.
- Exclusive access settings: you have the **RC Settings (Exclusive Access)** permission.
- Monitor mode settings: you have the **RC Settings (Monitor Mode)** permission.
- Mouse Hotkey and Remote Console button keys settings: you have the **RC Settings (Hotkeys)** permission.

Procedure

1. From the **Configuration** tab, click **Remote Console Settings > User Specific**. The **Remote Console Settings** page appears.



Managed Server: Linux on Prague Platform Name: Prague

User : super

Remote Console Settings

User Specific Remote Console Settings

The settings on this page are user specific. Modifications will affect the selected user only.

super Update

Transmission Encoding

● Automatic Detection *

○ Pre-configured

Network Speed: LAN (high color) *

○ Manually

Compression: 0 - none *

Color Depth: 16 bit - high col *

Miscellaneous Remote Console Settings

□ Start in Monitor Mode *

□ Start in Exclusive Access Mode *

Mouse Hotkey

Hotkey (Help): Alt+F12 *

Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).

Remote Console Button Keys

Key Definition (Help) Name

Button Key 1: confirm Ctrl+Alt+Delete * *

More entries

Apply View Defaults

* Stored value is equal to the default.

User Specific Remote Console Settings
This box allows you to configure the Remote System Console settings available in this page for your own user account or for another user. Select in the drop-down list a user and click the **Update** button in order to view/modify the Remote System Console settings set for this user.
Transmission Encoding
This setting allows you to change the image-encoding algorithm used to transmit the video data to the Remote System Console in order to improve or optimize the display speed of the remote screen.

Transmission Encoding (continued)	
Automatic Detection	The video encoding and the compression level is computed automatically according to the available bandwidth and the current video data.
Pre-configured	Select in the **Network Speed** drop-down list the pre-configured setting that corresponds to your network specifications.
Manually	Use this option to adjust manually the compression rate and the color depth. Note that values displayed in the **Colcr Depth** drop-down list differ depending on the selected value in the **Compression** drop-down list. The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network speeds to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit or 8 Bit (256 colors) color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.
Miscellaneous Remote Console Settings	
Start in Monitor Mode	Select this option to start the Remote System Console with the **Monitor only** option enabled. For details, see The Options Menu, on page 2-16.
Start in Exclusive Access Mode	Select this option to start the Remote System Console with the **Exclusive Access** option enabled. For details, see The Options Menu, on page 2-16
Mouse Hotkey	
Hotkey	This field allows you to specify a hotkey combination which starts the mouse synchronization process if pressed in the Remote System Console. This hotkey works only if you have selected the **Linux Mouse Type**, as described in Setting Up Keyboard and Mouse Parameters, on page 4-47.

<table>
<tr><th colspan="2">Remote Console Button Keys</th></tr>
<tr><td colspan="2">This box allows you to configure keystroke combinations to send to the remote system that cannot be generated locally. This may be useful if you want to send <b>Control+Alt+Del</b> to the remote system, whereas your local computer runs on Windows.
Use the following syntax to create a keystroke combination or to modify an existing one: <b>[confirm] <keycode>[+|-|&gt;[*]<keycode&gt;]*</b>, where:
• Terms in brackets are optional.
• The star at the end means that you add further keys as often as required for your case.
• The term <b>confirm</b> adds a confirmation dialogue that appears before the keystrokes are sent to the remote system.
• <b><keycode></b> is the key to be sent.
Multiple key codes can be concatenated with either a plus (+), a minus (+), or a greater-than (>) symbol:
• The plus symbol (+) builds key combinations: the keys are pressed simultaneaously until a minus symbol (-) or the end of the combination is encountered.
• The minus symbol (-) builds single, separate keypress/keyrelease events.
• The ”greater-than” symbol (>) releases the last key only.
• The star (*) inserts a pause with a duration of 100 milliseconds.
Note: If you want to configure several keystroke combinations, click the <b>More entries</b> button to add <b>Button Key</b> fields.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td><b>View Defaults</b> button</td><td>Allows you to display factory-default values (shown in this figure).</td></tr>
</table>

Figure 42. Remote System Console Configuration - User Specific Settings

2. Complete the wanted fields and click **Apply**.
3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Setting Up Keyboard and Mouse Parameters, on page 4-47
- Using the Remote System Console, on page 2-12

4.9.2. Setting Up Keyboard and Mouse Parameters

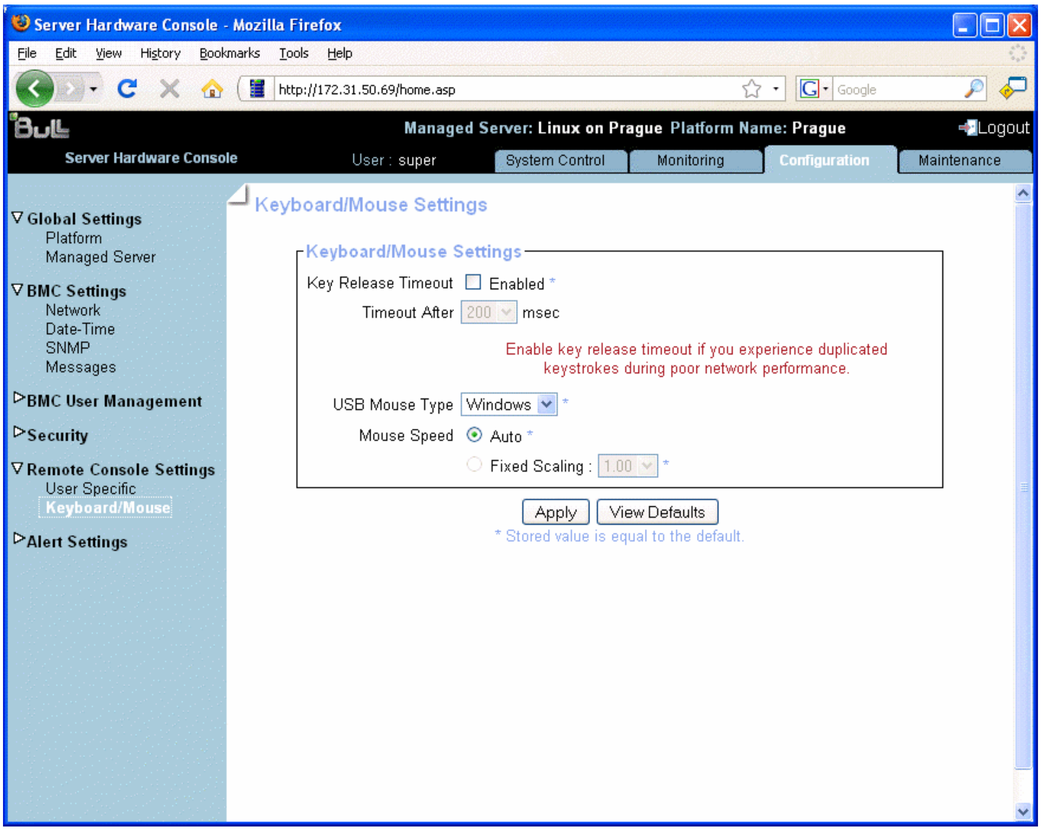
This page allows you to configure Keyboard and Mouse settings to use your local mouse and keyboard to control the remote server through the Remote System Console.

Prerequisites

- You have the **RC Keyboard/Mouse Settings** permission.

Procedure

1. From the **Configuration** tab, click **Remote Console Settings > Keyboard/Mouse**. The **Keyboard/Mouse Settings** page appears.



Keyboard/Mouse Settings

Keyboard/Mouse Settings

Key Release Timeout □ Enabled *

Timeout After 200 msec

Enable key release timeout if you experience duplicated keystrokes during poor network performance.

USB Mouse Type Windows *

Mouse Speed ● Auto *

○ Fixed Scaling : 1.00 *

* Stored value is equal to the default.

Keyboard/Mouse Settings	
Key Release Timeout	Enable this option if you experience unwanted repeated keystrokes when using your local keyboard to control the remote system. This issue usually occurs in a context of slow LAN performance. Note that when this option is enabled, the keystroke is automatically considered as released upon the Key Release Timeout, even if the key is maintained pressed.
Timeout After	Value of the Key Release Timeout in milliseconds.

Keyboard/Mouse Settings (continued)	
USB Mouse Type	Mice transmit their movement using absolute or relative values, depending on the operating system. • If your local workstation runs Windows 2000 or earlier, select **Windows** in the drop-down list. These OS use absolute coordinates to determine the position of the mouse pointer on the screen. In this mode, the remote mouse is always synchronized with the local mouse. • If your local workstation runs an older Windows version (like Windows 95 or 98) or a Linux operating system, select **Linux** in the drop-down list. These OS use relative coordinates to determine the position of the mouse pointer on the screen. In this mode, you may encounter synchronization issues between the remote mouse pointer and your local mouse.
Mouse Speed	By default, **Auto** is selected: this mode detects automatically the speed and acceleration settings of your mouse to determine the position of the mouse pointer on the remote screen. Select **Fixed Scaling** if you have synchronization issues between the remote remote mouse pointer and your local mouse. This mode translates the mouse movements as follows: one pixel move on your local workstation leads to “n” pixel moves on the remote system. Use the trial and error method to select the best “n” value in the drop-down list. **This option works only if mouse acceleration is turned off on the remote system.**
View Defaults button	Allows you to display factory-default values (shown in this figure).

Figure 43. Remote System Console Configuration - Keyboard and Mouse Settings

2. Change the keyboard and mouse parameters as wanted and click **Apply**.
3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring Remote System Console Settings, on page 4-43
- Using the Remote System Console, on page 2-12

4.10. Configuring Alert Settings

The alert transmission feature allows you to report selected events as alerts to one or more SNMP managers and/or email recipients.

When you set up alert transmission for the first time, you need to:

- Configure the event trap server community string and email server IP and sender addresses. For details, see Configuring the Event Trap and Email Server, on page 4-49.
- Configure the event trap server IP address(es) and/or email recipient address(es). For details, see Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51.
- Configure the alert transmission policy(ies). For details, see Setting up Alert Policies, on page 4-53.
- Select the events you want to report. For details, see Enabling/Disabling Predefined Event Filters, on page 4-56 and Setting up Configurable Event Filters, on page 4-58.

Note This section explains how to set up the alert transmission feature to suit standard needs. Advanced users may consult the official *IPMI Specification* for information about advanced alert transmission options.

Important **Alert transmission to the iCare Console must be set up directly from the iCare Console interface. Please refer to the *iCare Console User's Guide* for details.**

4.10.1. Configuring the Event Trap and Email Server

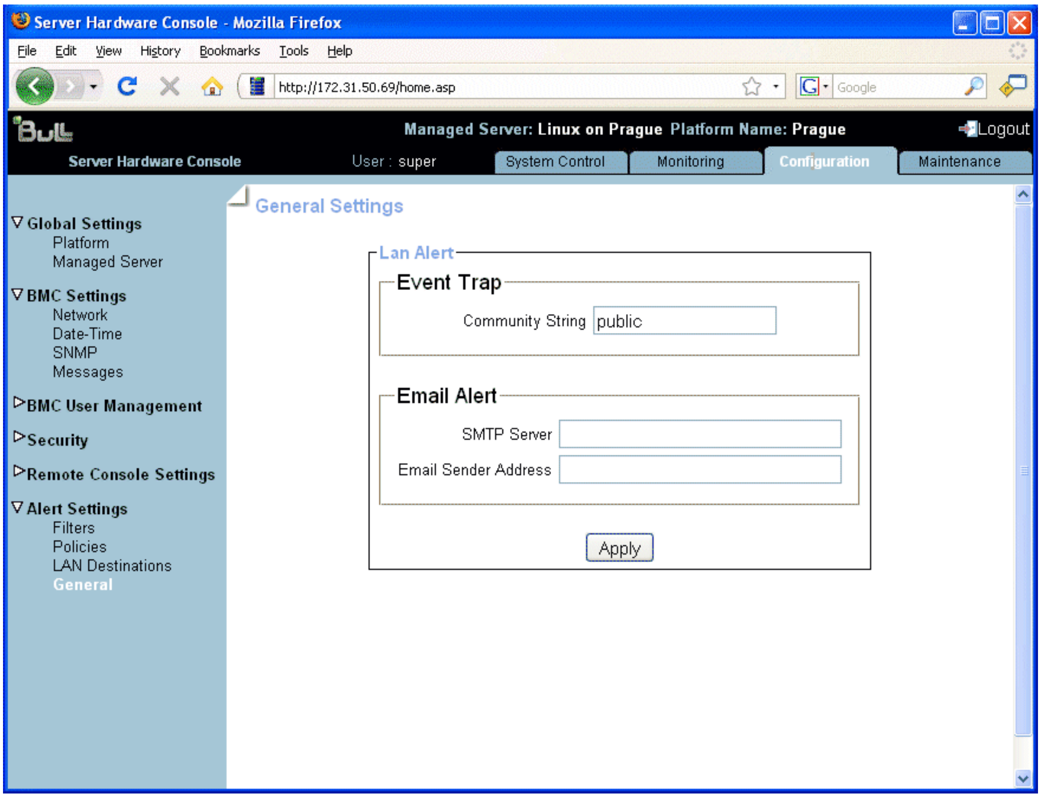
To be able to send events as alerts to SNMP managers and/or email recipients, you need to supply event trap server and email server details.

Prerequisites

- You have **Alert Settings & Clear SEL** permission.

Procedure

1. From the **Configuration** tab, click **Alert Settings** > **General** to display the **General Settings** page.



Community String: public

SMTP Server:

Email Sender Address:

LAN Alert	
Community String	If you want to use **PET alert** messaging, enter the same Community String value as the one used by the SNMP trap server. Default value: **public**.
SMTP Server and **Email Sender Address**	If you want to use **Email alert** messaging, enter: • **SMTP Server**: name or IP address of the outgoing SMTP email server used to send the email alert messages. • **Email Sender Address**: email server's sender address as it will appear in the header of the email.

Figure 44. General Settings page description

2. Complete the fields as required and click **Apply**.
3. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51
- Setting up Alert Policies, on page 4-53
- Enabling/Disabling Predefined Event Filters, on page 4-56
- Setting up Configurable Event Filters, on page 4-58

4.10.2. Configuring the Event Trap Server IP and Email Recipient Address(es)

To be able to send events as alerts to SNMP managers or email recipients, you need to configure the corresponding event trap server IP address(es) and/or email recipient address(es). These addresses are also called LAN destinations.

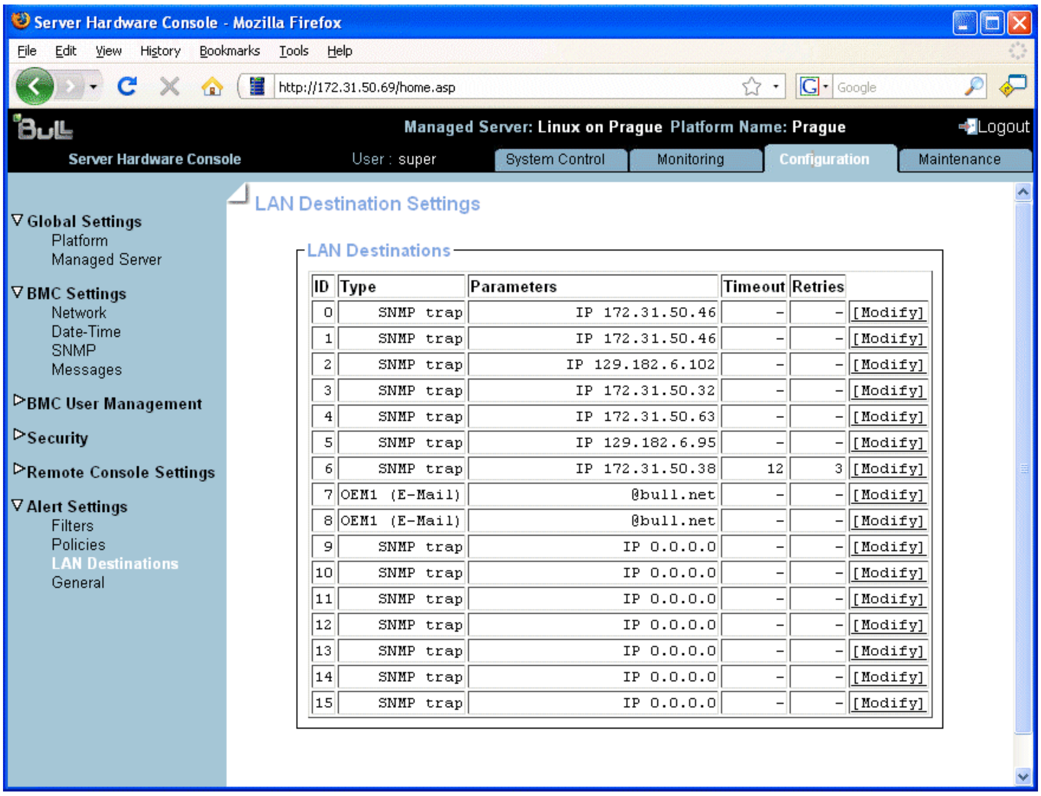
Important **Do not configure alert settings if you are using the iCare Console: alert and message transmission is automatically set up during the creation of the resources tree (resources discovery) through the iCare Console.**

Prerequisites

- You have Alert Settings & Clear SEL permission.

Procedure

1. From the Configuration tab, click Alert Settings > LAN Destinations to display the LAN Destination Settings page.



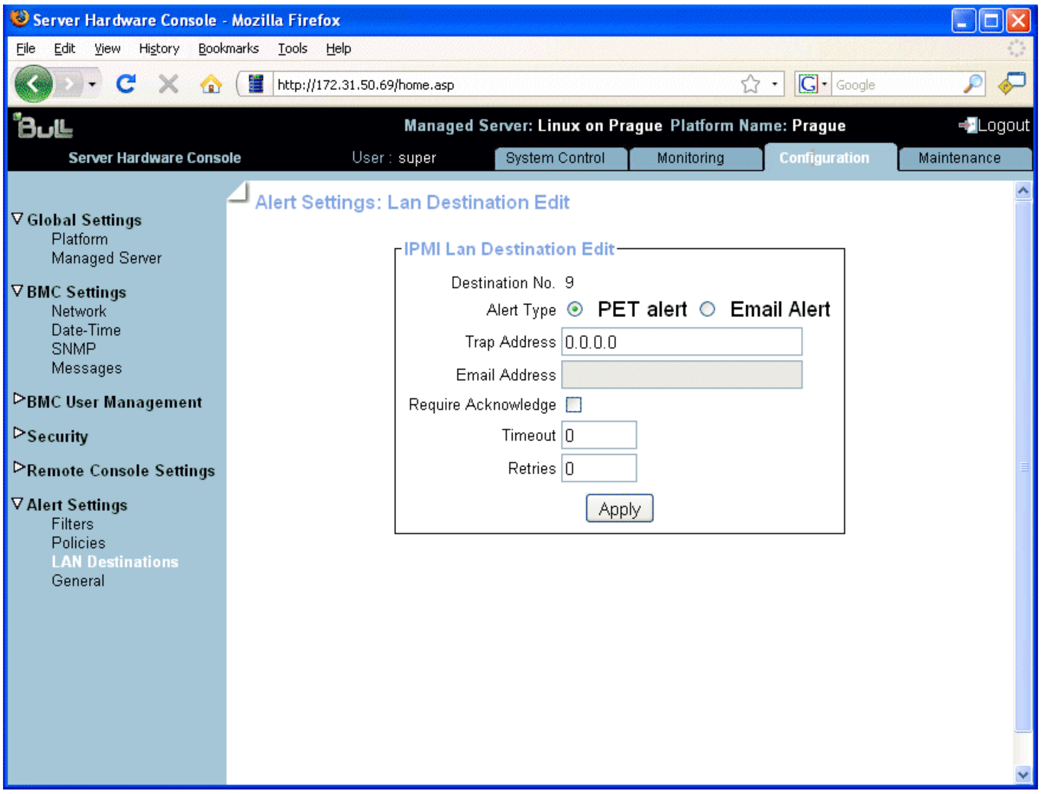
LAN Destination Settings

LAN Destinations

ID	Type	Parameters	Timeout	Retries	
0	SNMP trap	IP 172.31.50.46	-	-	[Modify]
1	SNMP trap	IP 172.31.50.46	-	-	[Modify]
2	SNMP trap	IP 129.182.6.102	-	-	[Modify]
3	SNMP trap	IP 172.31.50.32	-	-	[Modify]
4	SNMP trap	IP 172.31.50.63	-	-	[Modify]
5	SNMP trap	IP 129.182.6.95	-	-	[Modify]
6	SNMP trap	IP 172.31.50.38	12	3	[Modify]
7	OEM1 (E-Mail)	@bull.net	-	-	[Modify]
8	OEM1 (E-Mail)	@bull.net	-	-	[Modify]
9	SNMP trap	IP 0.0.0.0	-	-	[Modify]
10	SNMP trap	IP 0.0.0.0	-	-	[Modify]
11	SNMP trap	IP 0.0.0.0	-	-	[Modify]
12	SNMP trap	IP 0.0.0.0	-	-	[Modify]
13	SNMP trap	IP 0.0.0.0	-	-	[Modify]
14	SNMP trap	IP 0.0.0.0	-	-	[Modify]
15	SNMP trap	IP 0.0.0.0	-	-	[Modify]

Figure 45. LAN Destination Settings page

2. Select the first free LAN destination line (**IP 0.0.0.0**) and click **Modify** to display the **Alert Settings: LAN Destination Edit** page.



Destination No. 9

Alert Type ● PET alert ○ Email Alert

Trap Address 0.0.0.0

Email Address

Require Acknowledge □

Timeout 0

Retries 0

IPMI LAN Destination Edit	
Destination No.	Read-only. Predefined number used to identify the destination to which alert messages are to be sent.
Alert Type	Alert messaging format and method: • **PET alert** (Platform Event Trap): sends a PET alert to the specified trap address. • **Email alert**: generates an email alert to the specified email address.
Trap Address	**PET alerts** only. SNMP manager IP address. Example: 192.x.x.x.
Email Address	**Email alerts** only. Recipient's email address. Example: **john.smith@bull.net**
Require Acknowledge	**PET alerts** only. Select if you require alert message acknowledgement.
Timeout	**PET alerts** only. Time in seconds to wait for acknowledgement before retrying.
Retries	**PET alerts** only. Number of retries to make before aborting.

Figure 46. Alert Settings: LAN Destination Edit page description

3. Complete the fields as required and click **Apply**.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring the Event Trap and Email Server, on page 4-49
- Setting up Alert Policies, on page 4-53
- Enabling/Disabling Predefined Event Filters, on page 4-56
- Setting up Configurable Event Filters, on page 4-58

4.10.3. Setting up Alert Policies

Alert policies allow you to define alert messaging strategies.

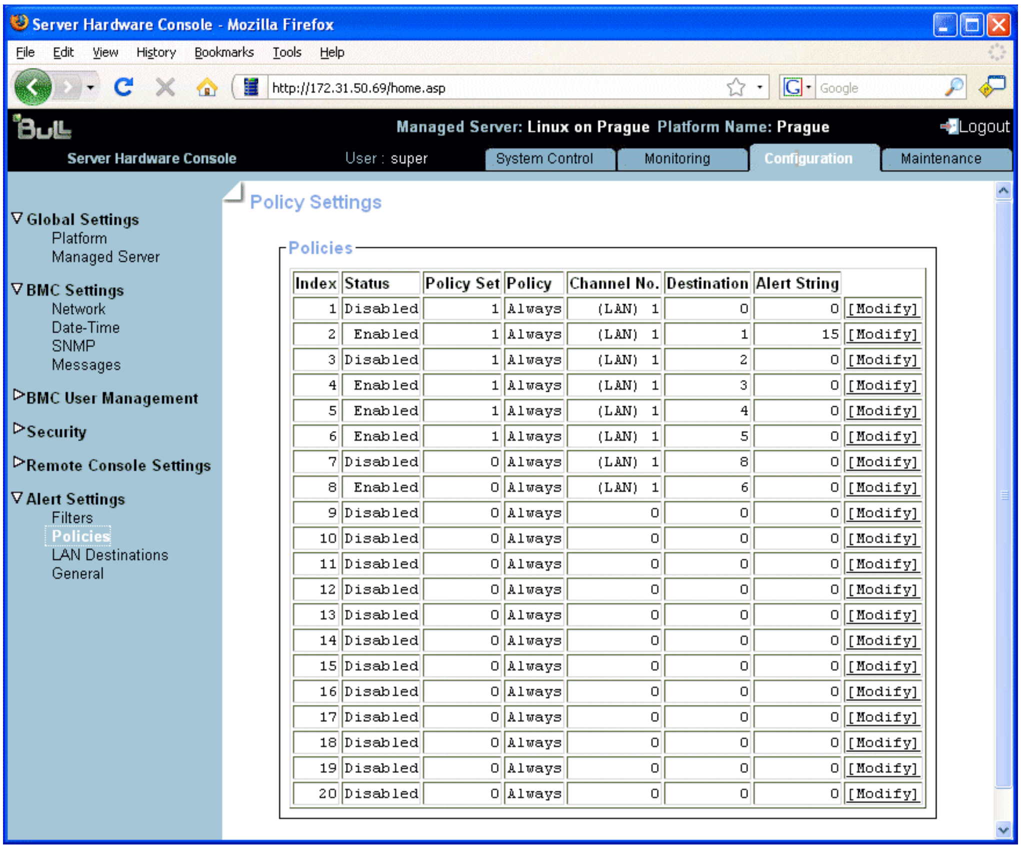
Note Some of the features described below are reserved for advanced users. For details about advanced alert transmission options, consult the official *IPMI Specification*.

Prerequisites

- You have **Alert Settings & Clear SEL** permission.

Procedure

1. From the **Configuration** tab, click **Alert Settings > Policies** to display the **Policy Settings** page.



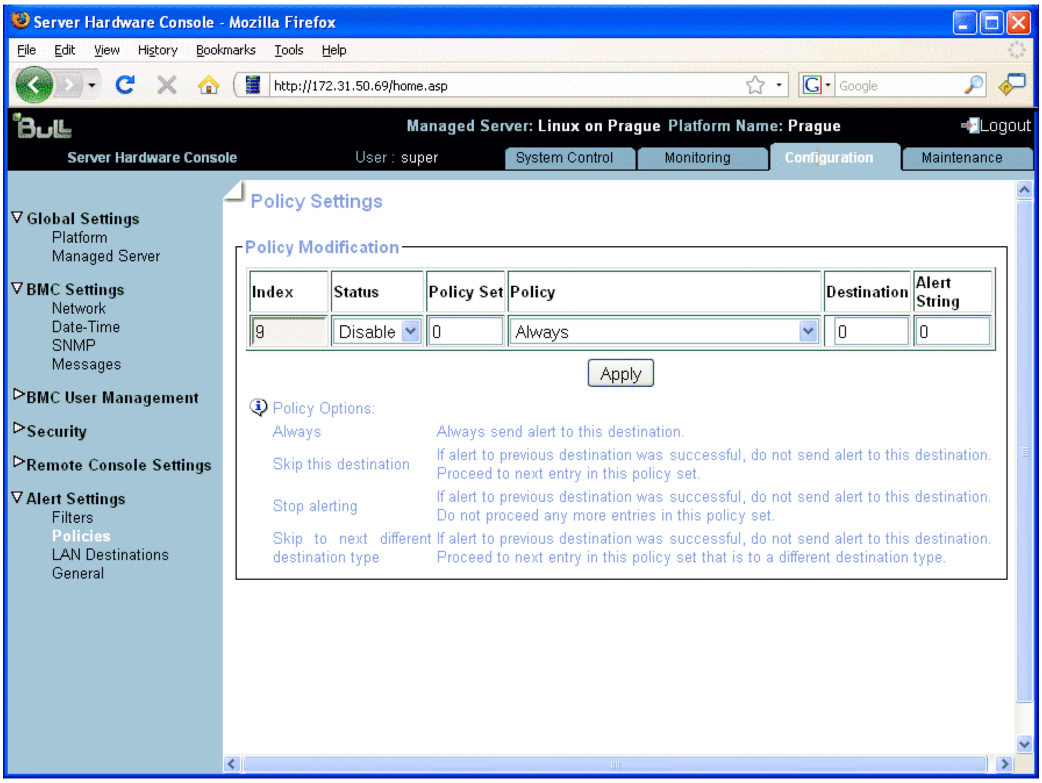
Policy Settings

Policies

Index	Status	Policy Set	Policy	Channel No.	Destination	Alert String	
1	Disabled	1	Always	(LAN) 1	0	0	[Modify]
2	Enabled	1	Always	(LAN) 1	1	15	[Modify]
3	Disabled	1	Always	(LAN) 1	2	0	[Modify]
4	Enabled	1	Always	(LAN) 1	3	0	[Modify]
5	Enabled	1	Always	(LAN) 1	4	0	[Modify]
6	Enabled	1	Always	(LAN) 1	5	0	[Modify]
7	Disabled	0	Always	(LAN) 1	8	0	[Modify]
8	Enabled	0	Always	(LAN) 1	6	0	[Modify]
9	Disabled	0	Always	0	0	0	[Modify]
10	Disabled	0	Always	0	0	0	[Modify]
11	Disabled	0	Always	0	0	0	[Modify]
12	Disabled	0	Always	0	0	0	[Modify]
13	Disabled	0	Always	0	0	0	[Modify]
14	Disabled	0	Always	0	0	0	[Modify]
15	Disabled	0	Always	0	0	0	[Modify]
16	Disabled	0	Always	0	0	0	[Modify]
17	Disabled	0	Always	0	0	0	[Modify]
18	Disabled	0	Always	0	0	0	[Modify]
19	Disabled	0	Always	0	0	0	[Modify]
20	Disabled	0	Always	0	0	0	[Modify]

Figure 47. Policy Settings page

2. Select the first free **disabled** alert policy and click **Modify** to display the **Policy Modification** page.



Index	Status	Policy Set	Policy	Destination	Alert String
9	Disable	0	Always	0	0

Policy Options:

Always	Always send alert to this destination.
Skip this destination	If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.
Stop alerting	If alert to previous destination was successful, do not send alert to this destination. Do not proceed any more entries in this policy set.
Skip to next different destination type	If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

Policy Modification	
Index	Read-only.
Status	Two possible values: • **Disable** (default value): the alert policy is not applied when an event occurs. • **Enable**: the alert policy is applied when an event occurs, according to the strategy selected from the **Policy** drop-down list and the destination number indicated in the **Destination** field.
Policy Set	Policies can be grouped into different policy sets, if required. This is a feature for advanced users. Only one policy set, **Policy Set 0**, is implemented for the predefined event filters. For details about advanced alert transmission options, you may consult the official *IPMI Specification*.

Policy Modification (continued)	
Policy	This drop-down list allows you to define an event messaging strategy for the current policy. This strategy is dependent on the strategies defined for preceding policies in the policy table belonging to the same policy set. According to the strategy you want to apply, select one of the following values: • **Always**: always send the alert to this destination. • **Skip this destination**: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination in the table. • **Stop alerting**: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and all subsequent destinations in the table. • **Skip to next different destination type**: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination using a different transmission method (**PET alert** vs **Email alert**).
Destination	Enter the predefined number used to identify the destination to which alert messages are to be sent. Note: This number corresponds to the number in the **ID** column on the **LAN Destination Settings** page.
Alert String	0 Read-only.

Figure 48. Policy Modification page description

3. Complete the required fields and click **Apply**.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Note Event Message Transmission Processing
When an event occurs, filter table entries are analyzed according to their index number: from 1 through to the last index number in the list.
When several enabled event filters match the event, the filter with the lowest policy set number is selected to transmit the alert.
When several enabled event filters match the event in the selected policy set, the filter with the highest severity is selected to transmit the alert.
When several enabled filters match the event in the selected policy set and they all have the same severity, the filter with the lowest index is selected to transmit the alert.

Related Topics

- Configuring the Event Trap and Email Server, on page 4-49
- Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51
- Enabling/Disabling Predefined Event Filters, on page 4-56
- Setting up Configurable Event Filters, on page 4-58

4.10.4. Enabling/Disabling Predefined Event Filters

Several event filters are factory-predefined and enabled by default. These predefined filters, listed in the Filter Table, cover all potential events. They cannot be modified, but can be enabled/disabled according to your needs. For details, refer to Predefined Alert Filters Description, on page A-1.

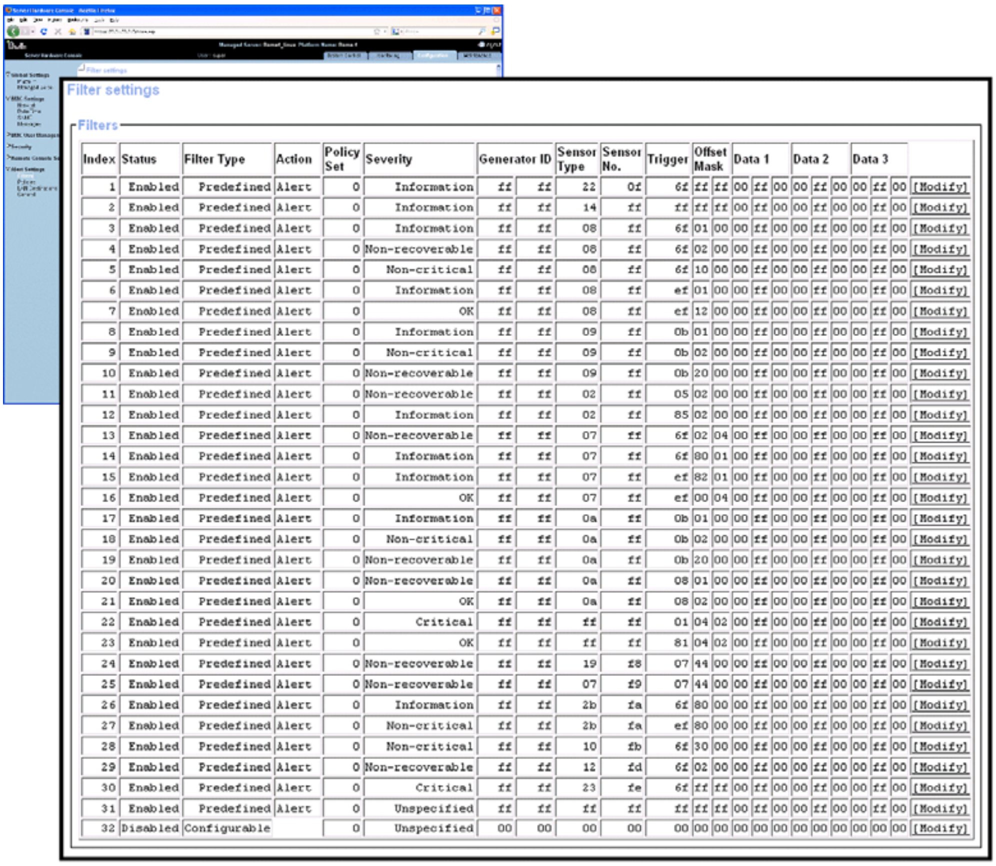
Note You can also define custom or "configurable" event filters. This is an advanced option. For details about advanced alert transmission options, you may consult the official *IPMI Specification* and Setting up Configurable Event Filters, on page 4-58.

Prerequisite

- You have **Alert Settings & Clear SEL** permission.

Procedure

1. From the **Configuration** tab, click **Alert Settings > Filters** to display the **Filter Settings** page.



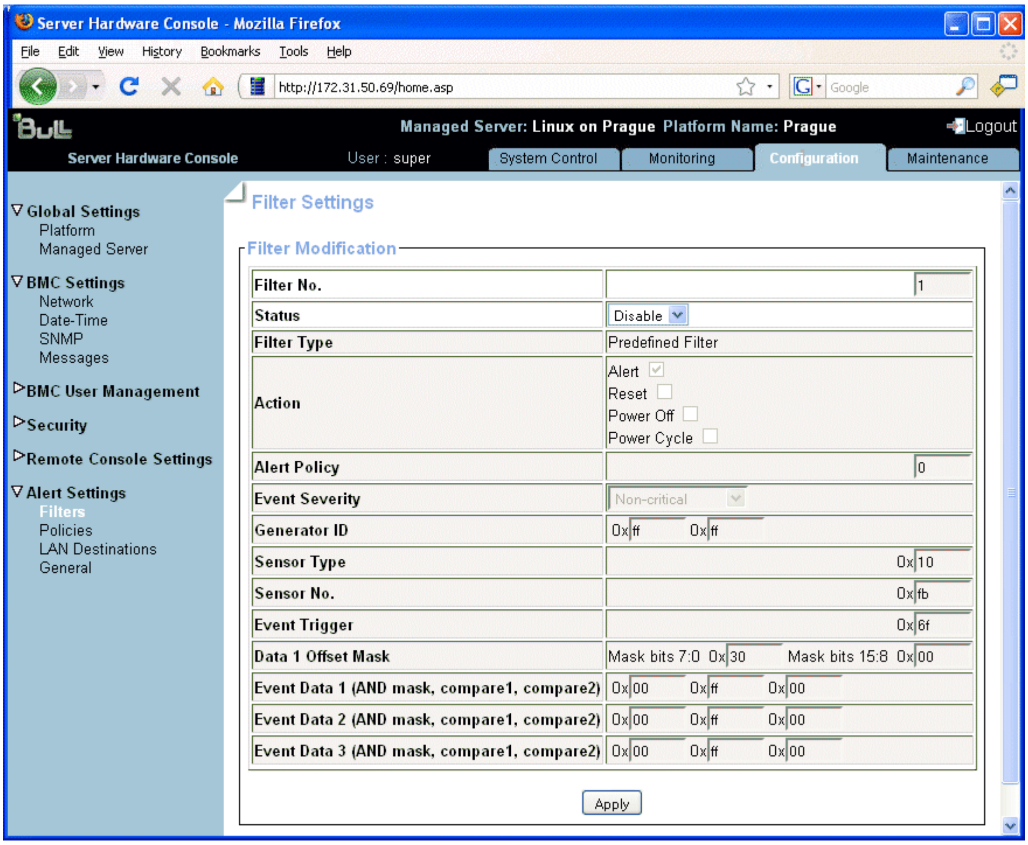
Filter settings

Filters

Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID		Sensor Type	Sensor No.	Trigger	Offset Mask		Data 1			Data 2			Data 3			
1	Enabled	Predefined	Alert	0	Information	ff	ff	22	0f	6f	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
2	Enabled	Predefined	Alert	0	Information	ff	ff	14	ff	ff	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
3	Enabled	Predefined	Alert	0	Information	ff	ff	08	ff	6f	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
4	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	08	ff	6f	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
5	Enabled	Predefined	Alert	0	Non-critical	ff	ff	08	ff	6f	10	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
6	Enabled	Predefined	Alert	0	Information	ff	ff	08	ff	ef	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
7	Enabled	Predefined	Alert	0	OK	ff	ff	08	ff	ef	12	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
8	Enabled	Predefined	Alert	0	Information	ff	ff	09	ff	0b	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
9	Enabled	Predefined	Alert	0	Non-critical	ff	ff	09	ff	0b	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
10	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	09	ff	0b	20	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
11	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	02	ff	05	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
12	Enabled	Predefined	Alert	0	Information	ff	ff	02	ff	85	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
13	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	07	ff	6f	02	04	00	ff	00	00	ff	00	00	ff	00	[Modify]
14	Enabled	Predefined	Alert	0	Information	ff	ff	07	ff	6f	80	01	00	ff	00	00	ff	00	00	ff	00	[Modify]
15	Enabled	Predefined	Alert	0	Information	ff	ff	07	ff	ef	82	01	00	ff	00	00	ff	00	00	ff	00	[Modify]
16	Enabled	Predefined	Alert	0	OK	ff	ff	07	ff	ef	00	04	00	ff	00	00	ff	00	00	ff	00	[Modify]
17	Enabled	Predefined	Alert	0	Information	ff	ff	0a	ff	0b	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
18	Enabled	Predefined	Alert	0	Non-critical	ff	ff	0a	ff	0b	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
19	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	0a	ff	0b	20	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
20	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	0a	ff	08	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
21	Enabled	Predefined	Alert	0	OK	ff	ff	0a	ff	08	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
22	Enabled	Predefined	Alert	0	Critical	ff	ff	ff	ff	01	04	02	00	ff	00	00	ff	00	00	ff	00	[Modify]
23	Enabled	Predefined	Alert	0	OK	ff	ff	ff	ff	81	04	02	00	ff	00	00	ff	00	00	ff	00	[Modify]
24	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	19	f8	07	44	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
25	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	07	f9	07	44	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
26	Enabled	Predefined	Alert	0	Information	ff	ff	2b	fa	6f	80	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
27	Enabled	Predefined	Alert	0	Non-critical	ff	ff	2b	fa	ef	80	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
28	Enabled	Predefined	Alert	0	Non-critical	ff	ff	10	fb	6f	30	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
29	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	12	fd	6f	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
30	Enabled	Predefined	Alert	0	Critical	ff	ff	23	fe	6f	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
31	Enabled	Predefined	Alert	0	Unspecified	ff	ff	ff	ff	ff	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
32	Disabled	Configurable		0	Unspecified	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	[Modify]

Figure 49. Filter Settings page (Predefined Filters)

2. Select the required predefined filter, using the table in Predefined Alert Filters Description, on page A-1, and click **Modify** to display the **Filter Modification** box.



Filter Settings

Filter Modification

Filter No.	1
Status	Disable
Filter Type	Predefined Filter
Action	Alert ☑ Reset □ Power Off □ Power Cycle □
Alert Policy	0
Event Severity	Non-critical
Generator ID	0x ff 0x ff
Sensor Type	0x 10
Sensor No.	0x fb
Event Trigger	0x 6f
Data 1 Offset Mask	Mask bits 7:0 0x 30 Mask bits 15:8 0x 00
Event Data 1 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00
Event Data 2 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00
Event Data 3 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00

Filter Modification	
Filter No.	Read-only, according to order in the Filter List.
Status	Two possible values: • **Disable** (default value): the filter is not taken into account when an event occurs. • **Enable**: the action specified in the **Action** field is executed if an event matches filter parameters.
Filter Type	Read-only: **Predefined Filter**
Action	Read-only: **Alert**. • **Alert**: the event is sent to the specified destination(s) (for details, see Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51) • **Reset**: the server is reset. • **Power Off**: the server is powered down. • **Power Cycle**: the server is restarted
Policy Set	Read-only: **0**.
Event Severity	Read-only, according to predefined severity.

Filter Modification (continued)	
Generator ID	Read-only. For further details, you may consult the official *IPMI Specification.*
Sensor Type	
Sensor No.	
Event Trigger	
Data 1 Offset Mask	
Event Data 1 (AND mask, compare1, compare2)	
Event Data 2 (AND mask, compare1, compare2)	
Event Data 3 (AND mask, compare1, compare2)	

Figure 50. Predefined Filters - Modification page

3. In the **Status** drop-down list, select either **Enable** or **Disable** depending on your needs and click **Apply**.
4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring the Event Trap and Email Server, on page 4-49.
- Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51
- Setting up Alert Policies, on page 4-53.
- Setting up Configurable Event Filters, on page 4-58
- Predefined Alert Filters Description, on page A-1

4.10.5. Setting up Configurable Event Filters

You may use the configurable event filters to create a custom event filter, for example if you want to define a different severity for the filter or if you want to associate the filter with a different policy set.

When you set up a configurable event filter, you must disable the corresponding predefined event filter to ensure that the configurable event filter is applied.

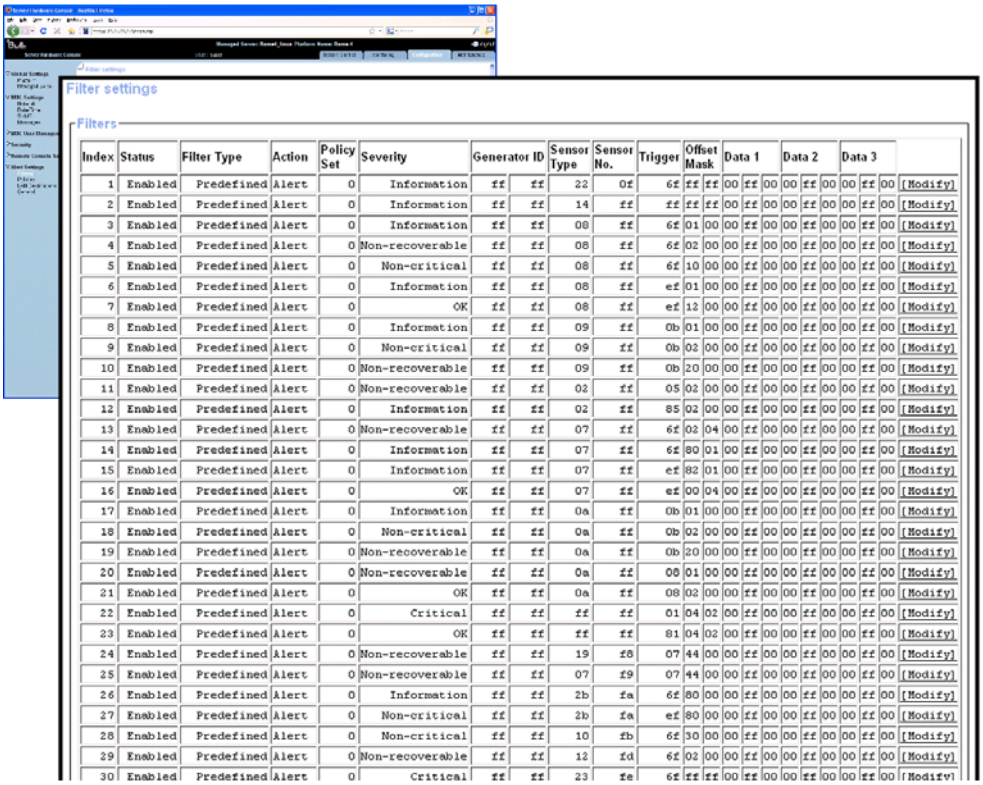
Note You are advised to consult the official *IPMI Specification* for information about advanced alert transmission options.

Prerequisite

- You have **Alert Settings & Clear SEL** permission.

Procedure

1. From the **Configuration** tab, click **Alert Settings > Filters** to display the **Filter Settings** page.



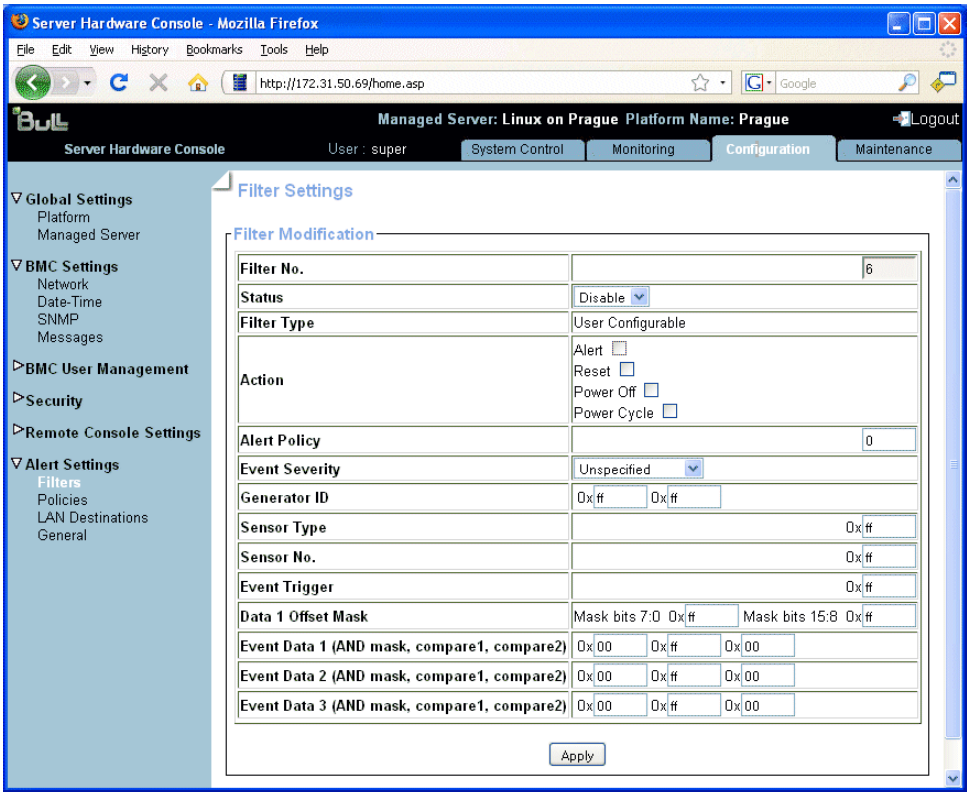
Filter settings

Filters

Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID		Sensor Type	Sensor No.	Trigger	Offset Mask		Data 1			Data 2			Data 3			
1	Enabled	Predefined	Alert	0	Information	ff	ff	22	0f	6f	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
2	Enabled	Predefined	Alert	0	Information	ff	ff	14	ff	ff	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]
3	Enabled	Predefined	Alert	0	Information	ff	ff	08	ff	6f	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
4	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	08	ff	6f	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
5	Enabled	Predefined	Alert	0	Non-critical	ff	ff	08	ff	6f	10	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
6	Enabled	Predefined	Alert	0	Information	ff	ff	08	ff	ef	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
7	Enabled	Predefined	Alert	0	OK	ff	ff	08	ff	ef	12	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
8	Enabled	Predefined	Alert	0	Information	ff	ff	09	ff	0b	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
9	Enabled	Predefined	Alert	0	Non-critical	ff	ff	09	ff	0b	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
10	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	09	ff	0b	20	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
11	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	02	ff	05	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
12	Enabled	Predefined	Alert	0	Information	ff	ff	02	ff	85	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
13	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	07	ff	6f	02	04	00	ff	00	00	ff	00	00	ff	00	[Modify]
14	Enabled	Predefined	Alert	0	Information	ff	ff	07	ff	6f	80	01	00	ff	00	00	ff	00	00	ff	00	[Modify]
15	Enabled	Predefined	Alert	0	Information	ff	ff	07	ff	ef	82	01	00	ff	00	00	ff	00	00	ff	00	[Modify]
16	Enabled	Predefined	Alert	0	OK	ff	ff	07	ff	ef	00	04	00	ff	00	00	ff	00	00	ff	00	[Modify]
17	Enabled	Predefined	Alert	0	Information	ff	ff	0a	ff	0b	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
18	Enabled	Predefined	Alert	0	Non-critical	ff	ff	0a	ff	0b	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
19	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	0a	ff	0b	20	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
20	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	0a	ff	08	01	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
21	Enabled	Predefined	Alert	0	OK	ff	ff	0a	ff	08	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
22	Enabled	Predefined	Alert	0	Critical	ff	ff	ff	ff	01	04	02	00	ff	00	00	ff	00	00	ff	00	[Modify]
23	Enabled	Predefined	Alert	0	OK	ff	ff	ff	ff	81	04	02	00	ff	00	00	ff	00	00	ff	00	[Modify]
24	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	19	f8	07	44	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
25	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	07	f9	07	44	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
26	Enabled	Predefined	Alert	0	Information	ff	ff	2b	fa	6f	80	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
27	Enabled	Predefined	Alert	0	Non-critical	ff	ff	2b	fa	ef	80	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
28	Enabled	Predefined	Alert	0	Non-critical	ff	ff	10	fb	6f	30	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
29	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	12	fd	6f	02	00	00	ff	00	00	ff	00	00	ff	00	[Modify]
30	Enabled	Predefined	Alert	0	Critical	ff	ff	23	fe	6f	ff	ff	00	ff	00	00	ff	00	00	ff	00	[Modify]

Figure 51. Filter Settings page (Configuration Filters)

2. Select the first free configurable filter in the list and click **Modify** to display the **Filter Modification** box.



Filter Settings

Filter Modification

Filter No.	6
Status	Disable
Filter Type	User Configurable
Action	Alert □ Reset □ Power Off □ Power Cycle □
Alert Policy	0
Event Severity	Unspecified
Generator ID	0x ff 0x ff
Sensor Type	0x ff
Sensor No.	0x ff
Event Trigger	0x ff
Data 1 Offset Mask	Mask bits 7:0 0x ff Mask bits 15:8 0x ff
Event Data 1 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00
Event Data 2 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00
Event Data 3 (AND mask, compare1, compare2)	0x 00 0x ff 0x 00

Filter Modification	
Filter No.	Filter number (read-only field).
Status	Two possible values: • **Disable** (default value): the filter is not taken into account when an event occurs. • **Enable**: the action specified in the **Action** field is executed if an event matches filter parameters.
Filter Type	This read-only field displays **User Configurable** to specify that you are editing a configurable event filter.
Action	Possible values: • **Alert**: the event is sent to the specified destination(s) (for details, see Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51) • **Reset**: the server is reset. • **Power Off**: the server is powered off. • **Power Cycle**: the server is powered off then powered on.
Policy Set	Default value: 0. Policies can be grouped into different policy sets, if required. This is a feature for advanced users. Only one policy set, **Policy Set 0**, is implemented for the predefined event filters. For details about advanced alert transmission options, you may consult the official *IPMI Specification*.
Event Severity	Select the severity value that you want to send when the event matches the filter parameters.
Generator ID	These bit fields allow you to specify the event that you want to filter. You are advised to copy the values entered for the corresponding predefined event filter that you are customizing. For further details, you may consult the official *IPMI Specification* or your Customer Representative.
Sensor Type	
Sensor No.	
Event Trigger	
Data 1 Offset Mask	
Event Data 1 (AND mask, compare1, compare2)	
Event Data 2 (AND mask, compare1, compare2)	
Event Data 3 (AND mask, compare1, compare2)	

Figure 52. Configurable Filters - Modification page description

3. Complete the required fields and click **Apply**.

4. If required, to back up configuration data, use the **KiraTool Environment** utility provided on the *Resource and Documentation CD*. Refer to *Backup Configuration Data* in Appendix C.

Related Topics

- Configuring the Event Trap and Email Server, on page 4-49
- Configuring the Event Trap Server IP and Email Recipient Address(es), on page 4-51
- Setting up Alert Policies, on page 4-53
- Enabling/Disabling Predefined Event Filters, on page 4-56
- Predefined Alert Filters Description, on page A-1

Chapter 5. Using Maintenance Features

This chapter explains the maintenance operations you can perform from the console. It includes the following topics:

- Viewing and/or Saving Board, FRU, Firmware and User Information, on page 5-2
- Updating Firmware, on page 5-4
- Resetting Devices, on page 5-9
- Enabling/Disabling Identification LED, on page 5-11
- Excluding/Including Processor Sockets, on page 5-12
- Viewing Connected Users, on page 5-13

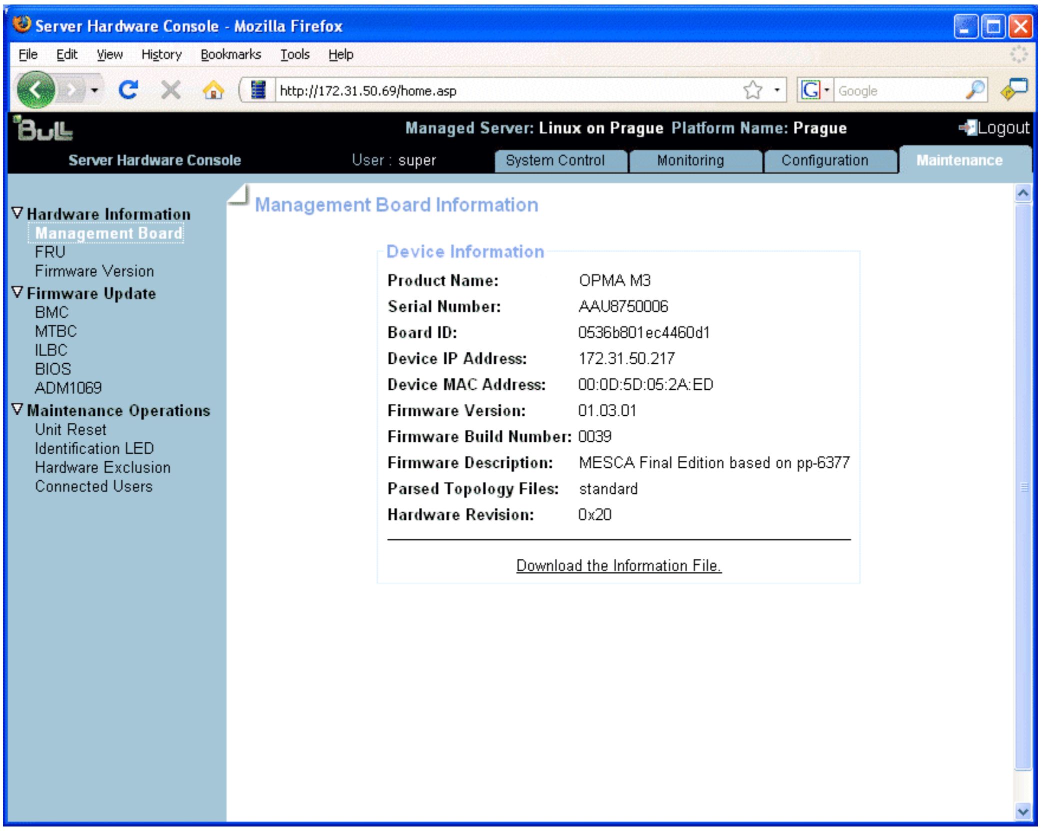
5.1. Viewing and/or Saving Board, FRU, Firmware and User Information

5.1.1. Viewing and Saving Embedded Management Board Information

You can display and/or save to an XML file embedded management board device and firmware information. This feature is particularly useful for maintenance and troubleshooting (checking current firmware version prior to an upgrade or sending the XML file to the support team, for example).

Procedure

1. From the **Maintenance** tab, click **Hardware Information > Management Board** to display the **Management Board Information** page.



Product Name:	OPMA M3
Serial Number:	AAU8750006
Board ID:	0536b801ec4460d1
Device IP Address:	172.31.50.217
Device MAC Address:	00:0D:5D:05:2A:ED
Firmware Version:	01.03.01
Firmware Build Number:	0039
Firmware Description:	MESCA Final Edition based on pp-6377
Parsed Topology Files:	standard
Hardware Revision:	0x20

Note The **Firmware Version** and **Firmware Build Number** values identify the **current** firmware version and build number.

Figure 53. Management Board Information page description

2. To view or save management board information to an XML file, click **Download the Information File**.

Related Topics

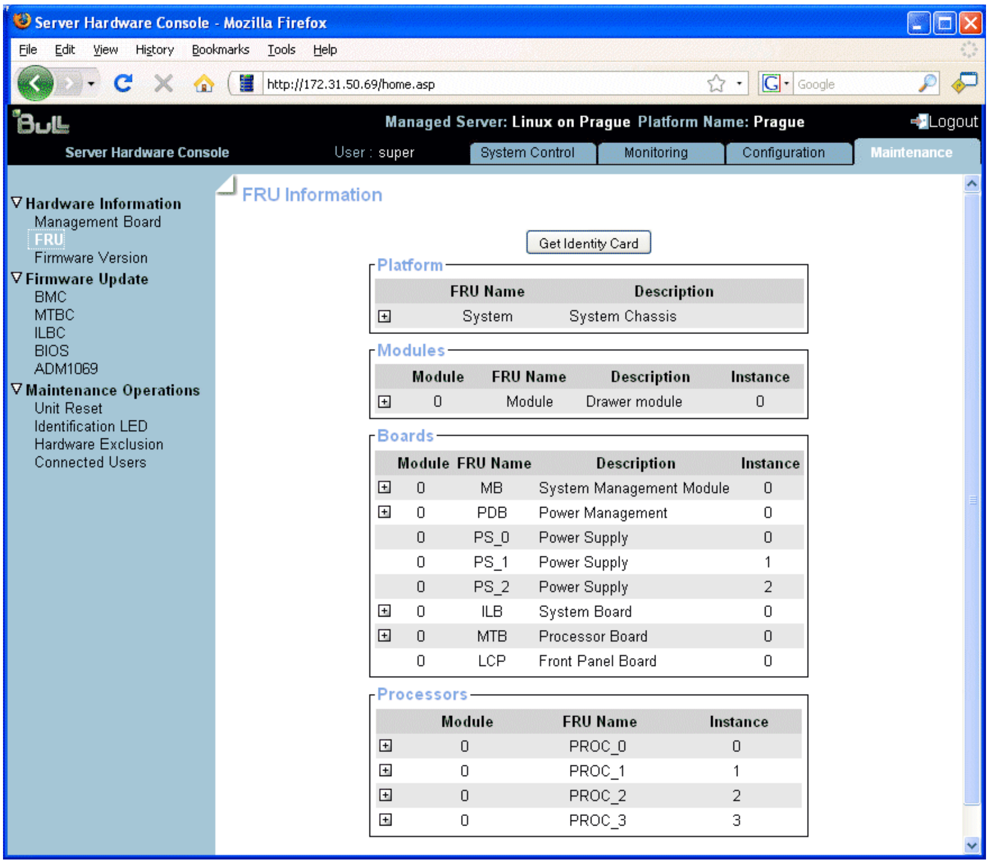
- Viewing and Saving FRU Information, on page 5-3
- Updating the Embedded Management Board (BMC) Firmware, on page 5-4

5.1.2. Viewing and Saving FRU Information

The IPMI-compliant information engraved on the FRU (Field Replaceable Unit) can be viewed online and/or saved to an XML file and downloaded for offline analysis and archiving. This feature is particularly useful to the support team.

Procedure

1. From the **Maintenance** tab, click **Hardware Information** > **FRU** to display the **FRU Information** page. As FRU information for all system components must be collected, the page may take several minutes to load.



Platform

	FRU Name	Description
⊞	System	System Chassis

Modules

	Module	FRU Name	Description	Instance
⊞	0	Module	Drawer module	0

Boards

	Module	FRU Name	Description	Instance
⊞	0	MB	System Management Module	0
⊞	0	PDB	Power Management	0
	0	PS_0	Power Supply	0
	0	PS_1	Power Supply	1
	0	PS_2	Power Supply	2
⊞	0	ILB	System Board	0
⊞	0	MTB	Processor Board	0
	0	LCP	Front Panel Board	0

Processors

	Module	FRU Name	Instance
⊞	0	PROC_0	0
⊞	0	PROC_1	1
⊞	0	PROC_2	2
⊞	0	PROC_3	3

Figure 54. FRU Information page

Note The plus button next to a FRU name indicates that the line can be expanded to show more information on the FRU. Note that the plus buttons next to the processor names are displayed only when the server is powered on.

2. To save and download the displayed FRU information in XML format, click **Get Identity Card** and follow the instructions on the screen.

Related Topics

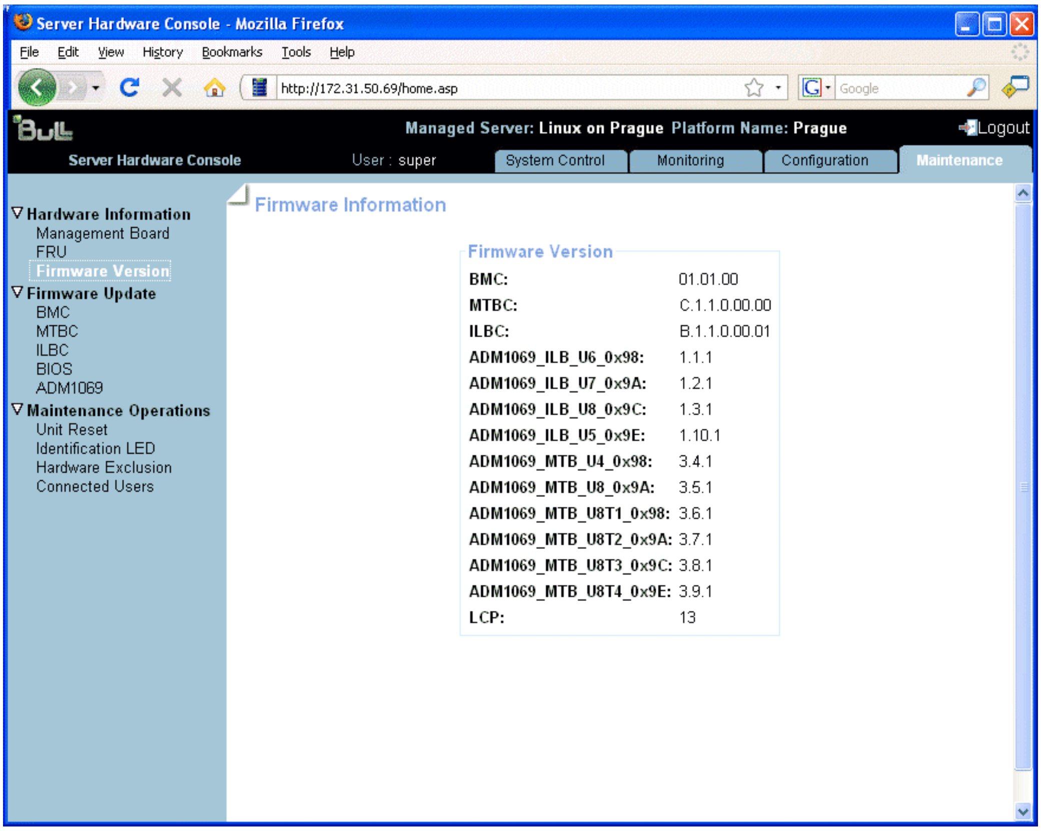
- Viewing and Saving Embedded Management Board Information, on page 5-2
- Updating the Embedded Management Board (BMC) Firmware, on page 5-4

5.1.3. Viewing Firmware Information

This feature is particularly useful for maintenance and troubleshooting (checking current firmware version prior to an upgrade or sending information to the support team, for example).

Procedure

- From the **Maintenance** tab, click **Hardware Information** > **Firmware Version** to display the **Firmware Information** page.



Firmware Information

Firmware Version

BMC:	01.01.00
MTBC:	C.1.1.0.00.00
ILBC:	B.1.1.0.00.01
ADM1069_ILB_U6_0x98:	1.1.1
ADM1069_ILB_U7_0x9A:	1.2.1
ADM1069_ILB_U8_0x9C:	1.3.1
ADM1069_ILB_U5_0x9E:	1.10.1
ADM1069_MTB_U4_0x98:	3.4.1
ADM1069_MTB_U8_0x9A:	3.5.1
ADM1069_MTB_U8T1_0x98:	3.6.1
ADM1069_MTB_U8T2_0x9A:	3.7.1
ADM1069_MTB_U8T3_0x9C:	3.8.1
ADM1069_MTB_U8T4_0x9E:	3.9.1
LCP:	13

Figure 55. Firmware Information page

Related Topics

- Updating Firmware, on page 5-4

5.2. Updating Firmware

5.2.1. Updating the Embedded Management Board (BMC) Firmware

The embedded management board firmware can be updated to install new features.

WARNING
The update process checks the validity and the consistency of the firmware file before starting the update. If the firmware file contains an error, the update does not start and the current firmware file is kept as is.

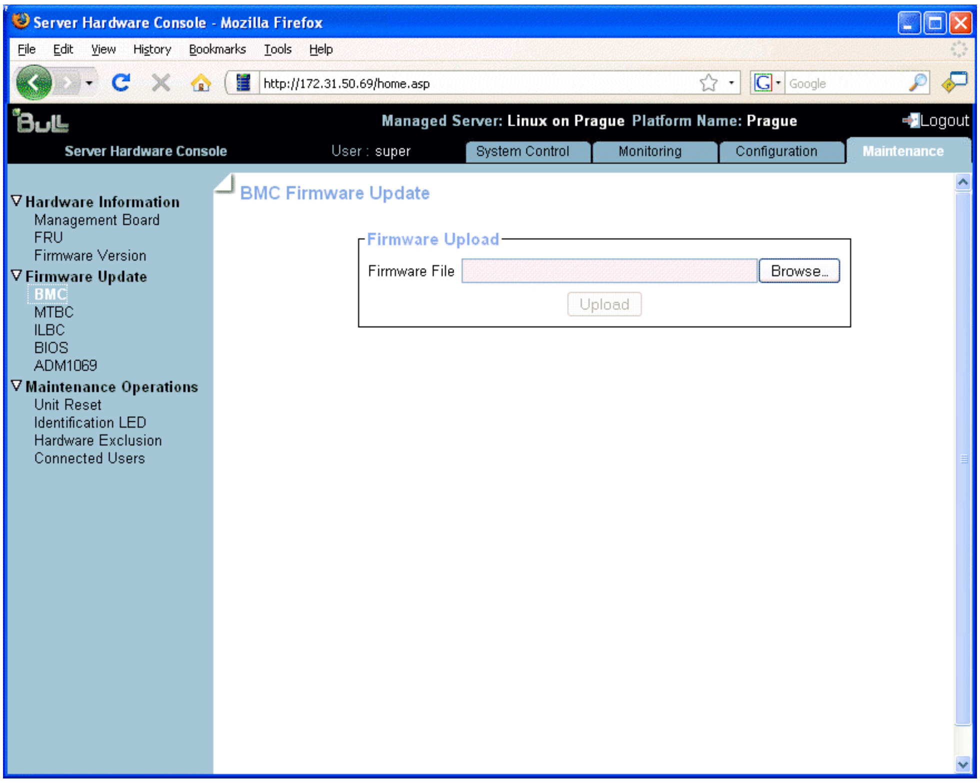
Prerequisites

- No other users are connected to the console or are likely to connect to the console.
- The new uncompressed firmware file is accessible on the computer used to launch the console.
- You have **Firmware Update** permission.

Procedure

WARNING
The update process may take some time and MUST NOT be interrupted. No other actions may be performed during the process.

1. From the **Maintenance** tab, click **Firmware Update** > BMC to display the **BMC Firmware Update** page.



http://172.31.50.69/home.asp

Managed Server: Linux on Prague Platform Name: Prague

User : super

Figure 56. BMC Firmware Update page

2. From the **Firmware Upload** box, click **Browse** to get the new version of the firmware file (or type the full file pathname in the **Firmware File** field) and click **Upload**. The content of the firmware file is copied to the management board RAM and a summary page appears.
3. Check that the new firmware version is correct and click **Update** to launch the update process.

Once the update is completed, the server embedded management controller software is automatically reset and you are redirected to the authentication page.

Note If the authentication page does not appear automatically, enter the Hardware Console IP address in your Web browser.

4. Log in and check that the new firmware version and build number appear in the **Management Board Information** page.

Related Topics

- Viewing Connected Users, on page 5-13

5.2.2. Updating MTBC, ILBC and BIOS Firmware

Important **The update process checks the validity and the consistency of the firmware file before starting the update. If the firmware file contains an error, the update does not start and the current firmware file is kept as is.**

Prerequisites

- The server must be powered down.
- No other users are connected to the console or are likely to connect to the console.
- The new uncompressed firmware file is accessible on the computer used to launch the console.
- You have **Firmware Update** permission.

Procedure

1. From the **Power Control** tab, check that the server is powered down to the standby mode by clicking the **Refresh** button in the **Power Information** box. If the displayed power state is **Off**, proceed to Step 2, otherwise power down the system.
2. Depending on the device to update, from the **Maintenance** tab click one of the following item in the navigation tree:
   a. **Firmware Update** > **MTBC** to display the **MTBC Firmware Update** page.
   b. **Firmware Update** > **ILBC** to display the **ILBC Firmware Update** page.
   c. **Firmware Update** > **BIOS** to display the **BIOS Firmware Update** page.
3. From the **Firmware Upload** box, click **Browse** to get the new version of the firmware file (or type the full file pathname in the **Firmware File** field) and click **Upload**. The content of the firmware file is copied to the management board RAM.
4. Check that the new firmware version is correct and click **Update** to launch the update process.

   ⚠ **WARNING**
   The update process may take some time and MUST NOT be interrupted. For example, the BIOS update may take up to 40 minutes per processor (i.e 2 hours and 40 minutes for a 4 processors rack server). No other actions may be performed during the process.

5. Check that the new firmware version and build number appear in the **Management Board Information** page.
6. Power on the system.

Related Topics

- Viewing Connected Users, on page 5-13

5.2.3. Updating ADM1069 Firmware

Important **The update process checks the validity and the consistency of the firmware file before starting the update. If the firmware file contains an error, the update does not start and the current firmware file is kept as is.**

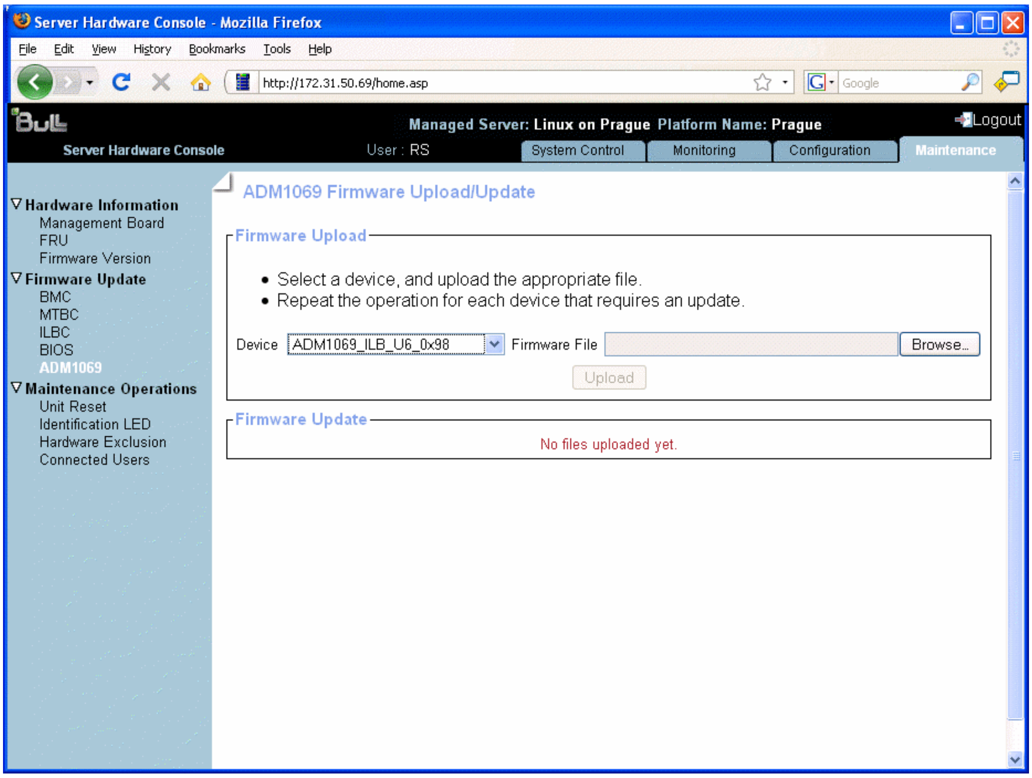
Prerequisites

- The server must be powered down.
- No other users are connected to the console or are likely to connect to the console.
- The new uncompressed firmware file is accessible on the computer used to launch the console.
- You have **Firmware Update** permission.

Procedure

WARNING
The update process may take some time and MUST NOT be interrupted. No other actions may be performed during the process.

1. From the **Power Control** tab, check that the server is powered down to the standby mode by clicking the **Refresh** button in the **Power Information** box. If the displayed power state is **Off**, proceed to Step 2, otherwise power down the system.
2. From the **Maintenance** tab, click **Firmware Update > ADM1069** to display the **ADM1069 Firmware Upload/Update** page.



ADM1069 Firmware Upload/Update

Firmware Upload

- Select a device, and upload the appropriate file.
- Repeat the operation for each device that requires an update.

Device ADM1069_ILB_U6_0x98 Firmware File

Firmware Update

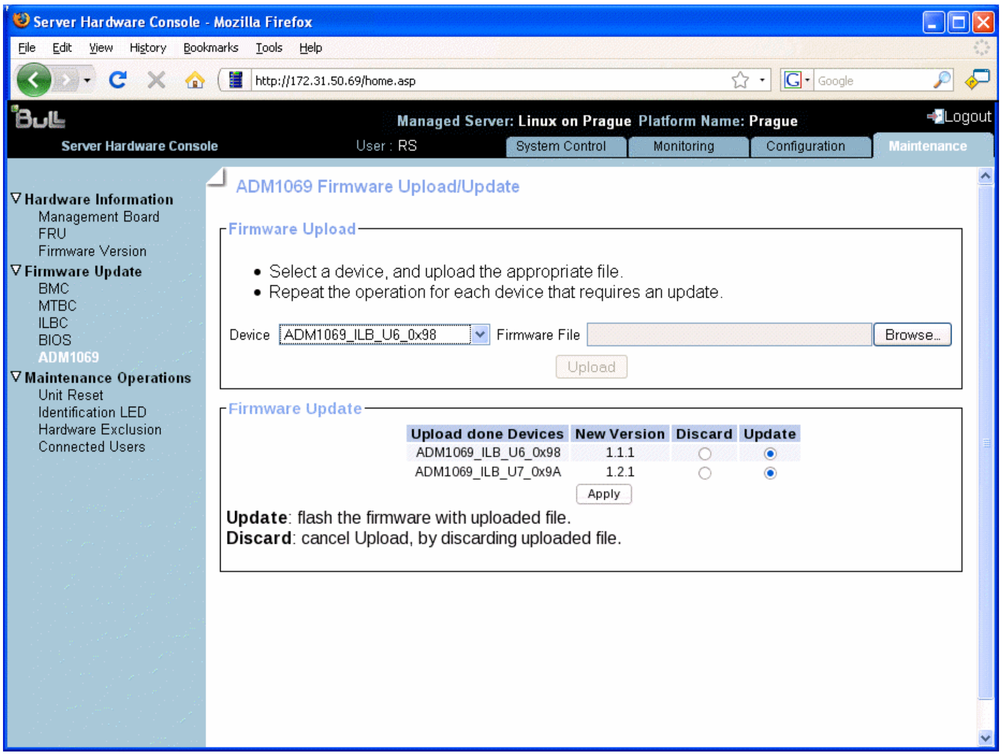
No files uploaded yet.

Figure 57. ADM1069 Firmware Upload/Update page - Step 1

3. Select in the **Device** drop-down list the ADM1069 device to update.

4. From the **Firmware File** field, click **Browse** to get the new version of the firmware file (or type the full file pathname) and click **Upload**. The new firmware version appears in the **Firmware Update** box.

5. If required, repeat Steps 3 and 4 for other ADM1069 devices to update, as illustrated in the following figure:



Managed Server: Linux on Prague **Platform Name:** Prague

User : RS

ADM1069 Firmware Upload/Update

Firmware Upload

- Select a device, and upload the appropriate file.
- Repeat the operation for each device that requires an update.

Device: ADM1069_ILB_U6_0x98 Firmware File:

Firmware Update

Upload done Devices	New Version	Discard	Update
ADM1069_ILB_U6_0x98	1.1.1	○	●
ADM1069_ILB_U7_0x9A	1.2.1	○	●

Update: flash the firmware with uploaded file.
Discard: cancel Upload, by discarding uploaded file.

Figure 58.   ADM1069 Firmware Upload/Update page - Step 2

6. If necessary, modify the values displayed in the **Discard** and **Update** columns and click **Apply**.

Related Topics

- Viewing Connected Users, on page 5-13

5.3. Resetting Devices

You can reset the entire embedded management software without altering configuration data, in the event of a feature abnormal freeze or a program hang for example. You can also reset specific software subdevices associated with the Remote System Console.

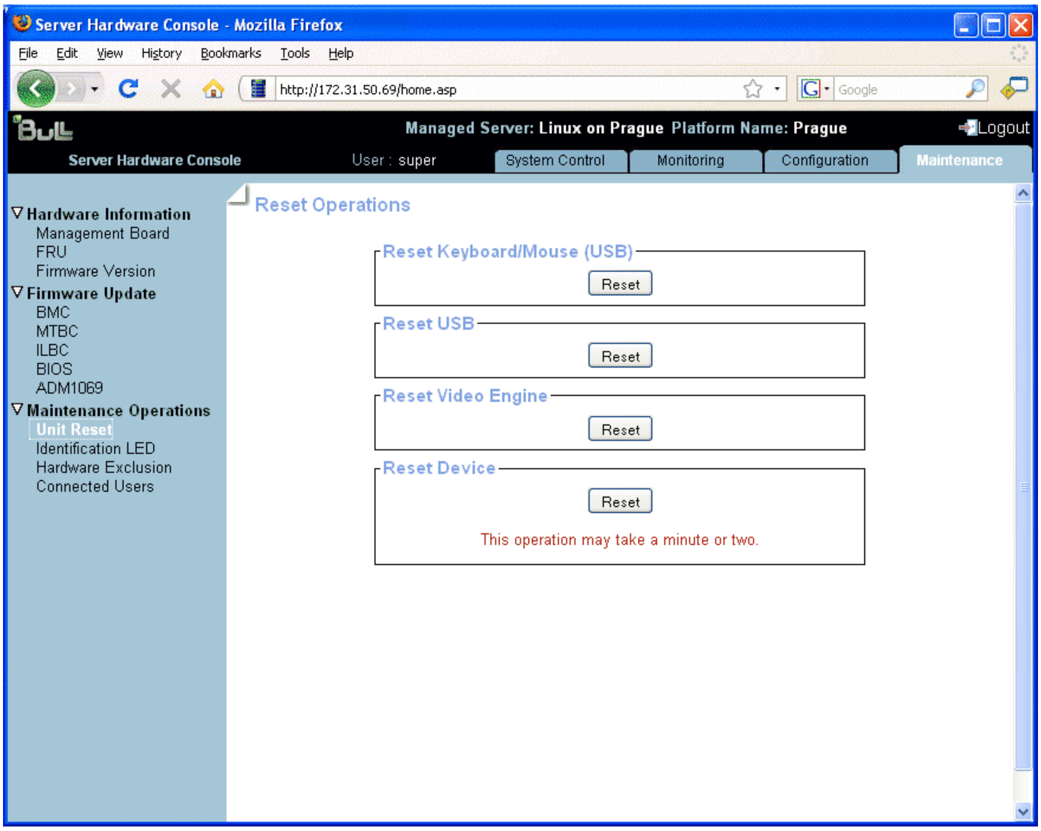
Important
- **The reset device command disconnects any connected users.**
- **The reset subdevices commands do not disconnect users.**

Prerequisites

- Reset Device: you have the **Maintenance/Board Reset** permission.
- Reset Keyboard/Mouse (USB), USB, video engine: you have the **Remote Console Access** permission.

Procedure

1. From the **Maintenance** tab, click **Maintenance Operations > Unit Reset** to open the **Reset Operations** page.



This operation may take a minute or two.

Reset Keyboard/Mouse (USB)	
Reset button	Resets the keyboard/Mouse subdevice, which manages the keyboard and mouse devices used to control the remote system through the Remote System Console.
Reset USB	
Reset button	Resets the USB engine subdevice.
Reset Video Engine	
Reset button	Resets the video engine subdevice, which manages the Remote System Console display.
Reset Device	
Reset button	Closes down and restarts the embedded software.

Figure 59. Reset Operations page

2. Click the wanted **Reset** button.

Related Topics

- Enabling/Disabling Identification LED, on page 5-11
- Excluding/Including Processor Sockets, on page 5-12

5.4. Enabling/Disabling Identification LED

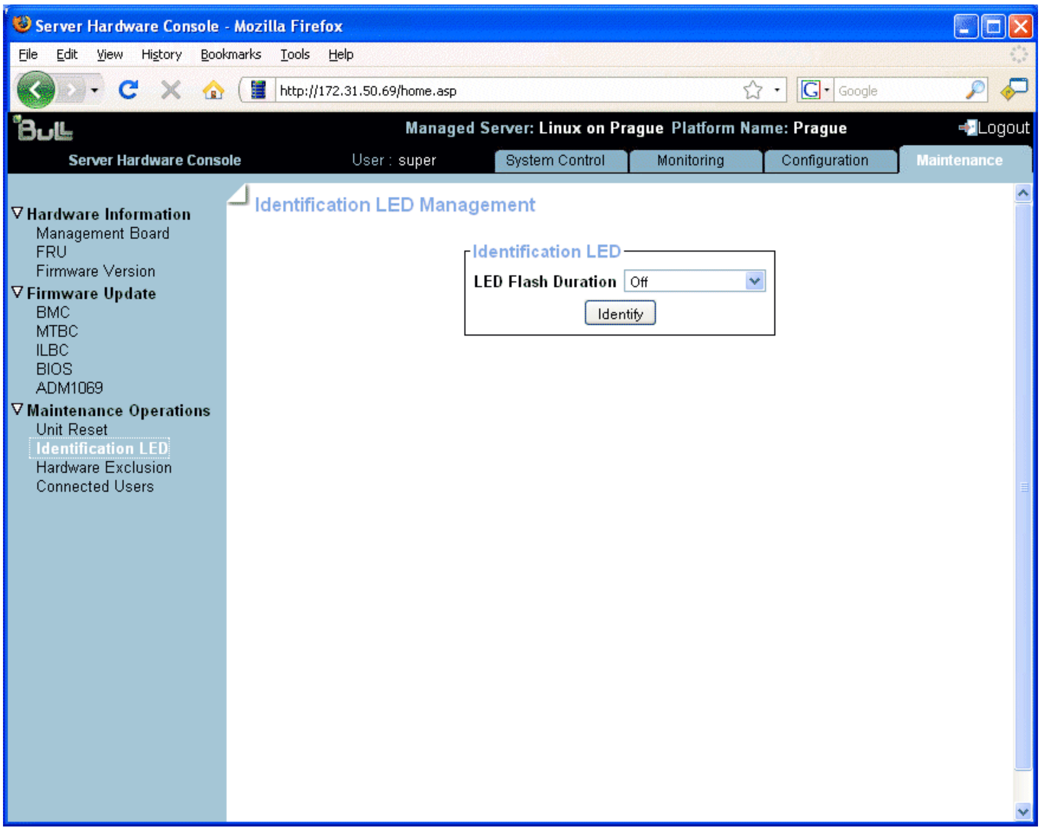
The server drawer has two identification LEDs, located at the front and at the rear of the drawer. These two blue ID LEDs provide a visual indication of a drawer being serviced.

Prerequisites

- You have **Alert Settings & Clear SEL** permission.

Procedure

1. From the **Maintenance** tab, click **Maintenance Operations** > **Identification LED** to open the **Identification LED Management** page.



Managed Server: Linux on Prague Platform Name: Prague

User : super

LED Flash Duration Off

Figure 60. Identification LED Management page

2. Select in the **LED Flash Duration** drop-down list the wanted value and click **Identify**.

Related Topics

- Resetting Devices in the *NovaScale 9006 Server Hardware Console User's Guide*
- Excluding/Including Processor Sockets, on page 5-12

5.5. Excluding/Including Processor Sockets

The console allows you to exclude and include processor sockets in a static way: the system must be powered off to select the components to exclude/include and the modification is taken into account at next power on.

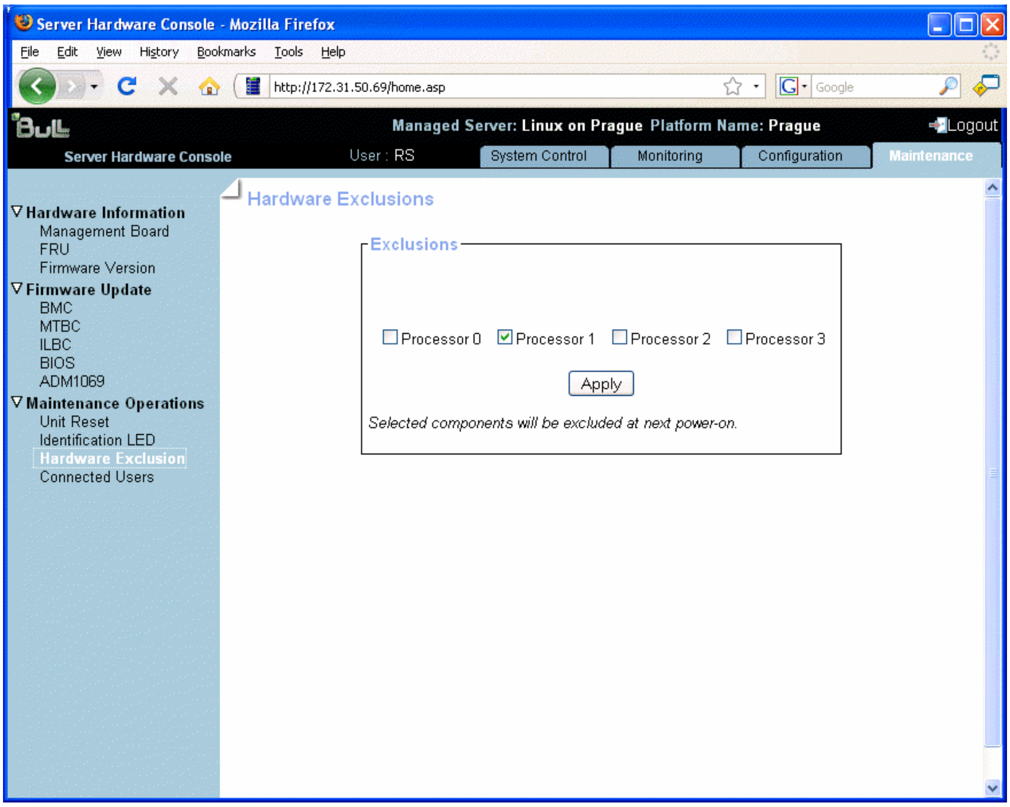
Important Excluding processor sockets is a special task that you must perform only in case of failure.

Prerequisites

- You have Maintenance/Board Reset permission
- The server must be powered off.

Procedure

1. From the Maintenance tab, click Maintenance Operations > Hardware Exclusion to open the Hardware Exclusions page.



□ Processor 0 ☑ Processor 1 □ Processor 2 □ Processor 3

Selected components will be excluded at next power-on.

Figure 61. Hardware Exclusions page

2. Either select the check box(es) corresponding to the processor socket(s) to exclude or clear the check box(es) corresponding to the processor socket(s) to include and click Apply.
3. Power on the system to apply the modification.

Related Topics

- Resetting Devices, on page 5-9
- Enabling/Disabling Identification LED in the *NovaScale 9006 Server Hardware Console User's Guide*

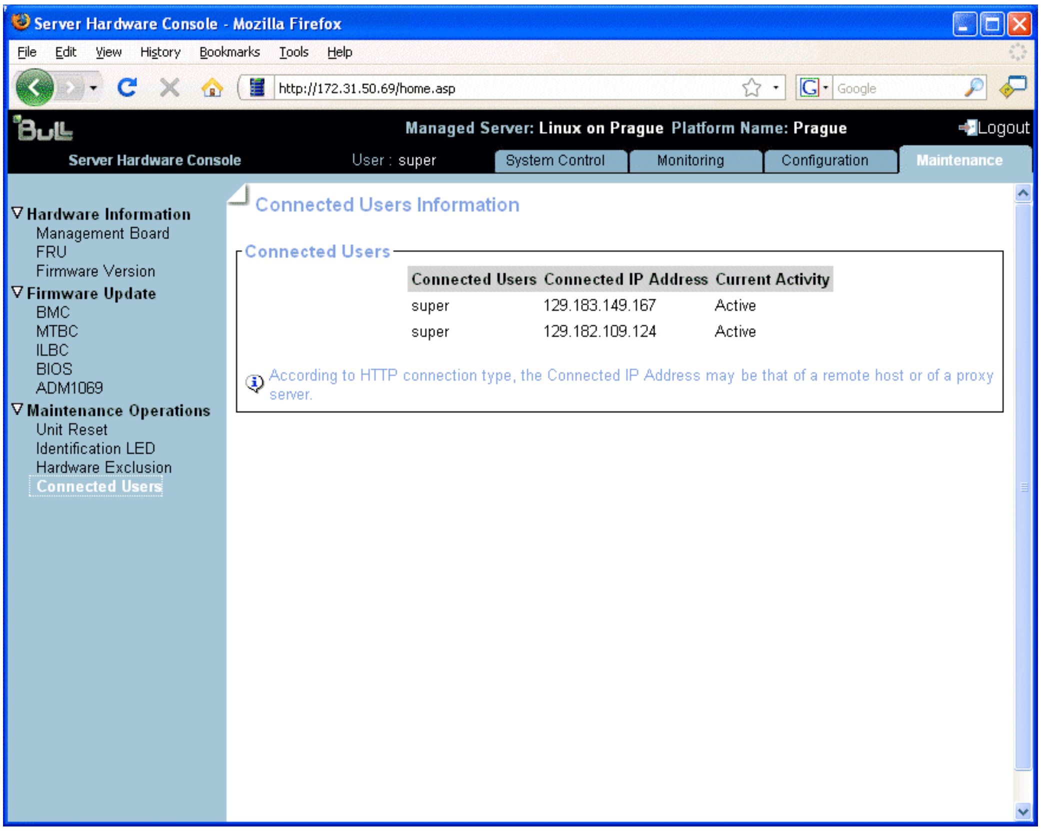
5.6. Viewing Connected Users

You may see if other users are connected to the console before performing configuration tasks or prior to a maintenance intervention.

Important **According to the connection type, the displayed IP address may correspond to a proxy server.**

Procedure

- From the **Maintenance** tab, click **Maintenance Operations** > **Connected Users** to display the **Connected Users Information** page.



Connected Users Information

Connected Users

Connected Users	Connected IP Address	Current Activity
super	129.183.149.167	Active
super	129.182.109.124	Active

According to HTTP connection type, the Connected IP Address may be that of a remote host or of a proxy server.

Figure 62. Connected Users Information page

Related Topics

- Viewing Board and Security Messages, on page 3-6

Appendix A.Predefined Alert Filters Description

This appendix lists predefined event filters. A set of predefined filters, covering all the hardware events likely to occur during system operation, are available for the transmission of alerts to an SNMP Trap Manager, such as Bull System Manager (BSM) or to an email recipient.

For guidance, the following sets of filters are available, according to event type:

Event Type	Filter Index
Power system Board	1
Sub-Chassis	2
Power Supply	3, 4, 5, 6, 7
Power Unit	8, 9, 10
System board (ILB)	11, 12, 22, 23
Processor board (MTB)	11, 12, 22, 23
Power distribution board (PDB)	22, 23
Control panel (LCP)	22, 23
Processor	11, 12, 13, 14, 15, 16
Fan box	17, 18, 19
Fan device	20, 21, 22, 23
BMC	24, 25, 26, 27, 28, 29, 30

Notes

- Pre-defined filters are not modifiable, they can only be enabled or disabled. On system delivery, all predefined filters are enabled.
- If a pre-defined filter does not suit your needs, you can create a custom filter. In this case, you must disable the corresponding predefined filter to ensure that your custom filter is processed.

The use and configuration of event filters is explained in Configuring Alert Settings, on page 4-49.

The following table details the events associated with each predefined filter.

N°	Component	Source	Event/Description	Severity	Meaning
1	Power system Board	ACPI Pwr State	S0/G0: working S0/G0: soft off	Information	The system is powered on. The system is powered off.
2	Sub-chassis	Power button	Power button pressed	Information	The power button has been pressed.
3	Power supply	PS_X	Presence detected.	Information	The PS_X power supply is present.
4	Power supply	PS_X	Power supply failure detected	Non-recoverable	A failure has been detected on the PS_X power supply.
5	Power supply	PS_X	Power supply input lost or out of range	Non-critical	An AC failure has been detected by the PS_X power supply.
6	Power supply	PS_X	Presence detected	Information	The PS_X power supply is not or no more present.
7	Power supply	PS_X	Power supply failure detected	Return to OK	The previous failure on the PS_0 power supply disappeared.
7	Power supply	PS_X	Power supply input lost	Return to OK	The PS_0 power supply AC input is now correct.
8	Power Unit	Pwr Redundancy	Fully redundant	Information	The three power supplies are up and running.
9	Power Unit	Pwr Redundancy	Redundancy lost	Non-critical	Two power supplies are up and running.
10	Power Unit	Pwr Redundancy	Non redundant: Insufficient resources	Non-recoverable	Only one power supply is up and running.
11	System board (ILB)	ILB 0.9V VID	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 0.9V VID	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.0V S GBE	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.0V S GBE	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.05V ICH	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.05V ICH	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.1V IOH0	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.1V IOH0	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.1V IOH1	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.1V IOH1	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.1V SL	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.1V SL	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.2V VID	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.2V VID	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.5V LEG	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.5V LEG	Limit exceeded	Information	This voltage is now OK.

N°	Component	Source	Event/Description	Severity	Meaning
11	System board (ILB)	ILB 1.8V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.8V	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 1.8V S	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 1.8V S	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 3.3V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 3.3V	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 3.3V S	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 3.3V S	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 3.3V SL	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 3.3V SL	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 5V LEG	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 5V LEG	Limit exceeded	Information	This voltage is now OK.
11	System board (ILB)	ILB 12V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB 12V	Limit exceeded	Information	This voltage is now OK.
22	System board (ILB)	ILB temperature	At or below lower critical threshold (going low)	Critical	The ILB temperature is lower than the minimum.
22	System board (ILB)	ILB temperature	At or above upper critical threshold (going high)	Critical	The ILB temperature is upper than the maximum.
23	System board (ILB)	ILB temperature	At or below lower critical threshold (going low)	Return to OK	The ILB temperature is now OK.
23	System board (ILB)	ILB temperature	At or above upper critical threshold (going high)	Return to OK	The ILB temperature is now OK.
11	Processor board (MTB)	MTB 1.2V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor board (MTB)	MTB 1.2V	Limit exceeded	Information	This voltage is now OK.
11	Processor board (MTB)	MTB 3.3V SD	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor board (MTB)	MTB 3.3V SD	Limit exceeded	Information	This voltage is now OK.
11	Processor board (MTB)	MTB 3.3V SL	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor board (MTB)	MTB 3.3V SL	Limit exceeded	Information	This voltage is now OK.
11	Processor board (MTB)	MTB 5V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.

N°	Component	Source	Event/Description	Severity	Meaning
12	Processor board (MTB)	MTB 5V	Limit exceeded	Information	This voltage is now OK.
22	Processor board (MTB)	MTB Temperature	At or below lower critical threshold (going low)	Critical	The MTB temperature is lower than the minimum.
22	Processor board (MTB)	MTB Temperature	At or above upper critical threshold (going high)	Critical	The MTB temperature is upper than the maximum.
23	Processor board (MTB)	MTB Temperature	At or below lower critical threshold (going low)	Return to OK	The MTB temperature is now OK.
23	Processor board (MTB)	MTB Temperature	At or above upper critical threshold (going high)	Return to OK	The MTB temperature is now OK.
22	Power distribution board (PDB)	PDB Temperature	At or below lower critical threshold (going low)	Critical	The PDB temperature is lower than the minimum.
22	Power distribution board (PDB)	PDB Temperature	At or above upper critical threshold (going high)	Critical	The PDB temperature is upper than the maximum.
23	Power distribution board (PDB)	PDB Temperature	At or below lower critical threshold (going low)	Return to OK	The PDB temperature is now OK.
23	Power distribution board (PDB)	PDB Temperature	At or above upper critical threshold (going high)	Return to OK	The PDB temperature is now OK.
22	Control panel (LCP)	LCP Temperature	At or below lower critical threshold (going low)	Critical	The LCP temperature is lower than the minimum.
22	Control panel (LCP)	LCP Temperature	At or above upper critical threshold (going high)	Critical	The LCP temperature is upper than the maximum.
23	Control panel (LCP)	LCP Temperature	At or below lower critical threshold (going low)	Return to OK	The LCP temperature is now OK.
23	Control panel (LCP)	LCP Temperature	At or above upper critical threshold (going high)	Return to OK	The LCP temperature is now OK.
13	Processor	PROC_X	Thermal trip	Non-recoverable	PROC_X reached the highest temperature limit and stopped.
14	Processor	PROC_X	Processor presence detected	Information	PROC_X is present.
14	Processor	PROC_X	Processor disabled	Information	PROC_X is disabled.
13	Processor	PROC_X	Processor automatically throttled	Non-recoverable	PROC_X runs slowly to limit temperature or power consumption.
15	Processor	PROC_X	Thermal trip	Information	PROC_X runs normally.
15	Processor	PROC_X	Processor presence detected	Information	PROC_X is absent.
15	Processor	PROC_X	Processor disabled	Information	PROC_X is enabled.
16	Processor	PROC_X	Processor automatically throttled	Return to OK	PROC_X runs normally.
11	Processor	PX 1.1V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX 1.1V	Limit exceeded	Information	This voltage is now OK.

N°	Component	Source	Event/Description	Severity	Meaning
11	Processor	PX 1.8V	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX 1.8V	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX 3.3V CHCD	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX 3.3V CHCD	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX 3.3V TKW	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX 3.3V TKW	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX 12V ARARAT	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX 12V ARARAT	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VCC 0	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VCC 0	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VCC 1	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VCC 1	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VTT 0	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VTT 0	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VTT 1	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VTT 1	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VDD 0	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VDD 0	Limit exceeded	Information	This voltage is now OK.
11	Processor	PX VDD 1	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	Processor	PX VDD 1	Limit exceeded	Information	This voltage is now OK.
17	Fan box	FANBX_X Redund.	Fully redundant	Information	Both of the fans in the fanbox are up and running.
18	Fan box	FANBX_X Redund.	Redundancy lost	Non-critical	Only one fan in the fanbox is up and running.
19	Fan box	FANBX_X Redund.	Non redundant: Insufficient resources	Non-recoverable	No fan are working in the fanbox.
20	Fan device	FAN_XY Presence	Device removed / Device absent	Non-recoverable	In the fan box #X the fan#Y is not or no more present.
21	Fan device	FAN_XY Presence	Device inserted / Device present	Return to OK	In the fan box #X the fan#Y is (now) present.
22	Fan device	FAN_XY Speed	At or below lower critical threshold (going low)	Critical	In the fan box # X the fan #Y speed is lesser than the minimum required.
23	Fan device	FAN_XY Speed	At or below lower critical threshold (going low)	Return to OK	In the fan box # X the fan #Y is now at normal speed.
24	BMC	Chipset Error	Transition to Critical from less severe	Non-recoverable	A chipset uncorrectable error has occurred.
24	BMC	Chipset Error	Transition to Non-Recoverable	Non-recoverable	A chipset uncorrectable error has occurred

N°	Component	Source	Event/Description	Severity	Meaning
25	BMC	Processor Error	Transition to Critical from less severe	Non-recoverable	A processor uncorrectable error has occurred.
25	BMC	Processor Error	Transition to Non-Recoverable	Non-recoverable	A processor uncorrectable error has occurred.
26	BMC	Version Change	Management controller firmware change was successful	Information	Management controller firmware change was successful.
27	BMC	Version Change	Management controller firmware change was unsuccessful	Non-critical	Management controller firmware change was unsuccessful.
26	BMC	Version Change	System firmware change was successful	Information	System firmware change was successful.
27	BMC	Version Change	System firmware change was unsuccessful	Non-critical	System firmware change was unsuccessful.
26	BMC	Version Change	Programmable hardware change was successful	Information	Programmable hardware change was successful.
27	BMC	Version Change	Programmable hardware change was unsuccessful	Non-critical	Programmable hardware change was unsuccessful.
28	BMC	Sel	Sel log full	Non-critical	No more room for a new event in the System Event Log.
28	BMC	Sel	Sel almost full	Non-critical	The System Event Log is 75% full.
29	BMC	System Event	A system boot event has occurred	Non-recoverable	[7:5] Message class 0 Processor 0 error 1 Processor 1 error 2 Processor 2 error 3 Processor 3 error 4 ILB power error 5 FPGA error 6 System / Environment error 7 Software error [4:0] BMC/SMC step nb : 0-31 see BMC/SMC power steps worksheets [7:6] Sequence nb 0 Power ON sequence 1 Power OFF sequence 2 Reset sequence 3 rfu [5:0] Error nb : 0-63 see error messages worksheet
30	BMC	watchdog	Offset 0:Timeout – no specific action Offset 1:Timeout followed by hard reset Offset 2:Timeout followed by Power Down Offset 3:Timeout followed by power Cycle	Critical	Timeout during BIOS init step which causes the configured action.

Table 9. Predefined Event Filters

Appendix B. Troubleshooting the NovaScale 9006 Server Drawer

This appendix describes the System Event Log (SEL) messages; it includes the following topics:

B.1. ILB SEL Messages

ILB 0.9V VID: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 0.9V VID: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.0V S GBE: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.0V S GBE: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.05V ICH: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.05V ICH: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1V IOH0: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1V IOH0: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1V IOH1: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1V IOH1: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1V SL: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.1VSL: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.2V VID: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.2V VID: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.5V LEG: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.5V LEG: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Actions	None.
Filter Number	12.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.8V: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.8V: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.8V S: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 1.8V S: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V S: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V S: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V SL: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 3.3V SL: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 5V LEG: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 5V LEG: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 12V: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB 12V: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB Temperature: At or below lower critical threshold (going low)

Description	The ILB temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB Temperature: At or above upper critical threshold (going high)

Description	The ILB temperature is upper than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB Temperature: At or below lower critical threshold (going low)

Description	The ILB temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

ILB Temperature: At or above upper critical threshold (going high)

Description	The ILB temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.2. MTB SEL Messages

MTB 1.2V: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 1.2V: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 3.3V SD: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 3.3V SD: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 3.3V SL: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 3.3V SL: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 5V: Limit Exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB 5V: Limit Exceeded

Description	This voltage is now OK.
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB Temperature: At or below lower critical threshold (going low)

Description	The MTB temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB Temperature: At or above upper critical threshold (going high)

Description	The MTB temperature is upper than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB Temperature: At or below lower critical threshold (going low)

Description	The MTB temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

MTB Temperature: At or above upper critical threshold (going high)

Description	The MTB temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.3. Processor SEL Messages

Proc_X: Thermal trip

Description	PROC_X reached the highest temperature limit and stopped.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	13.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Thermal trip

Description	PROC_X runs normally.
Severity	Information.
Direction	Deassertion.
Filter Number	15.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor presence detected

Description	PROC_X is present.
Severity	Information.
Direction	Assertion.
Filter Number	14.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor presence detected

Description	PROC_X is absent.
Severity	Information.
Direction	Deassertion.
Filter Number	15.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor disabled

Description	PROC_X is disabled.
Severity	Information.
Direction	Assertion.
Filter Number	14.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor disabled

Description	PROC_X is enabled.
Severity	Information.
Direction	Deassertion.
Filter Number	15.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor automatically throttled

Description	PROC_X runs slowly to limit temperature or power consumption.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	13.
Actions	check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

Proc_X: Processor automatically throttled

Description	PROC_X PROC_0 runs normally.
Severity	Return to normal.
Direction	Deassertion.
Filter Number	13.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 1.1V: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 1.1V: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 1.8V: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 1.8V: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Filter Number	12.
Direction	Deassertion.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 3.3V CHCD: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 3.3V CHCD: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 3.3V TKW: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 3.3V TKW: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 12V ARARAT: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX 12V ARARAT: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VCC 0: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VCC 0: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VCC 1: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Filter Number	11.
Direction	Assertion.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VCC 1: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VTT 0: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VTT 0: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VTT 1: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Actions	If the problem persists, contact your Customer Service Engineer.
Filter Number	11.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VTT 1: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VDD 0: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VDD 0: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VDD 1: Limit exceeded

Description	This voltage is out of the acceptable range.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	11.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

PX VDD 1: Limit exceeded

Description	This voltage is now OK
Severity	Information.
Direction	Deassertion.
Filter Number	12.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alert Settings, on page 4-49.

B.4. Sub-chassis SEL Messages

Sub-Chassis: Button pressed

Description	The power button has been pressed.
Severity	Information.
Direction	Assertion.
Filter Number	2.
Actions	None.
Comments	Notice that there is no deassertion event. For more information about filters, see Configuring Alert Settings, on page 4-49.

B.5. Power Supply SEL Messages

PS_X: Presence detected

Description	The PS_X power supply is present.
Severity	Information.
Direction	Assertion.
Filter Number	3.
Actions	None.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

PS_X: Presence detected

Description	The PS_X power supply is not or no more present.
Severity	Information.
Direction	Deassertion.
Filter Number	6.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

PS_X: Power supply failure detected

Description	A failure has been detected on the PS_X power supply.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	4.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

PS_X: Power supply failure detected

Description	The previous failure on the PS_X power supply disappeared.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	7.
Actions	None.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

PS_X: Power supply input lost or out of range

Description	An AC failure has been detected by the PS_X power supply.
Severity	Non-critical.
Direction	Assertion.
Filter Number	5.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

PS_X: Power supply input lost or out of range

Description	The PS_X power supply AC input is now correct.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	7.
Actions	None.
Comments	X= 0, 1 or 2. For more information about filters, see Configuring Alert Settings, on page 4-49.

B.6. Power Unit SEL Messages

Pwr Redundancy: Fully redundant

Description	The three power supplies are up and running.
Severity	Information.
Direction	Assertion.
Filter Number	8.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

Pwr Redundancy: Redundancy lost

Description	Only one power supply is up and running.
Severity	Non critical.
Direction	Assertion.
Filter Number	9.
Actions	In a redundant configuration: If the problem persists, contact your Customer Service Engineer. In a non-redundant configuration: None
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

Pwr Redundancy: Non redundant. Insufficient resources

Description	Only one power supply is up and running.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	10.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.7. Fan Device SEL Messages

FAN device: Presence: Device removed / Device absent

Description	In the fan box Y, the fan X is not or no more present.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	20.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	Y= Fan box (0 to 3) and X= Fan unit (0 or 1). For more information about filters, see Configuring Alert Settings, on page 4-49.

FAN device: Presence: Device inserted / Device present

Description	In the fan box Y, the fan X is now present.
Severity	return to OK.
Direction	Assertion.
Filter Number	21.
Actions	None.
Comments	Y= Fan box (0 to 3) and X= Fan unit (0 or 1). For more information about filters, see Configuring Alert Settings, on page 4-49.

FAN device: Speed At or below lower critical threshold (going low)

Description	In the fan box Y, the fan X speed is lesser than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	Y= Fan box (0 to 3) and X= Fan unit (0 or 1). For more information about filters, see Configuring Alert Settings, on page 4-49.

FAN device: Speed At or below lower critical threshold (going low)

Description	In the fan box Y, the fan X speed is now at normal speed.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	Y= Fan box (0 to 3) and X= Fan unit (0 or 1). For more information about filters, see Configuring Alert Settings, on page 4-49.

B.8. PDB SEL Messages

PDB Temperature: At or below lower critical threshold (going low)

Description	The PDB temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

PDB Temperature: At or above upper critical threshold (going high)

Description	The PDB temperature is upper than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

PDB Temperature: At or below lower critical threshold (going low)

Description	The PDB temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

PDB Temperature: At or above upper critical threshold (going high)

Description	The PDB temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.9. LCP SEL Messages

LCP Temperature: At or below lower critical threshold (going low)

Description	The LCP temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

LCP Temperature: At or above upper critical threshold (going high)

Description	The LCP temperature is upper than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

LCP Temperature: At or below lower critical threshold (going low)

Description	The LCP temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

LCP Temperature: At or above upper critical threshold (going high)

Description	The LCP temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.10. BMC SEL Messages

BMC Chipset Error: Transition to Critical from less severe

Description	A chipset uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	24.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Chipset Error: Transition to Non-Recoverable

Description	A chipset uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	24.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Processor Error: Transition to Critical from less severe

Description	A processor uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	25.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Processor Error: Transition to Non-Recoverable

Description	A processor uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	25.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Management controller firmware change was successful

Description	A version change event has occurred.
Severity	Information.
Direction	Assertion.
Filter Number	26.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Management controller firmware change was unsuccessful

Description	A version change event has occurred.
Severity	Non-critical.
Direction	Deassertion.
Filter Number	27.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Management controller firmware change was successful

Description	A version change event has occurred.
Severity	Information.
Direction	Assertion.
Filter Number	26.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Management controller firmware change was unsuccessful

Description	A version change event has occurred.
Severity	Non-critical.
Direction	Deassertion.
Filter Number	27.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: System firmware change was successful

Description	A version change event has occurred.
Severity	Information.
Direction	Assertion.
Filter Number	26.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: System firmware change was unsuccessful

Description	A version change event has occurred.
Severity	Non-critical.
Direction	Deassertion.
Filter Number	27.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Programmable hardware change was successful

Description	A version change event has occurred.
Severity	Information.
Direction	Assertion.
Filter Number	26.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC Version Change: Programmable hardware change was unsuccessful

Description	A version change event has occurred.
Severity	Non-critical.
Direction	Deassertion.
Filter Number	27.
Actions	None.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC sel: sel log full

Description	No more room for a new event in the System Event Log.
Severity	Non-critical.
Direction	Assertion.
Filter Number	28.
Actions	Clear the System Event Log.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC sel: sel log almost full

Description	The System Event Log is 75% full.
Severity	Non-critical.
Direction	Assertion.
Filter Number	28.
Actions	Clear the System Event Log as soon as possible.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC System event:

Description	A system boot event has occurred [7:5] Message class 0 Processor 0 error 1 Processor 1 error 2 Processor 2 error 3 Processor 3 error 4 ILB power error 5 FPGA error 6 System / Environment error 7 Software error [4:0] BMC/SMC step nb : 0-31 see BMC/SMC power steps worksheets [7:6] Sequence nb 0 Power ON sequence 1 Power OFF sequence 2 Reset sequence 3 rfu [5:0] Error nb : 0-63 see error messages worksheet
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	29.
Actions	see error messages worksheet.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC watchdog: Timeout – no specific action

Description	timeout during BIOS init step which causes the configured action.
Severity	Critical.
Direction	Assertion.
Filter Number	30.
Actions	Check other events, then see BIOS postcode.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC watchdog: Timeout followed by hard reset

Description	timeout during BIOS init step which causes the configured action.
Severity	Critical.
Direction	Assertion.
Filter Number	30.
Actions	Check other events, then see BIOS postcode.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC watchdog: Timeout followed by Power Down

Description	timeout during BIOS init step which causes the configured action.
Severity	Critical.
Direction	Assertion.
Filter Number	30.
Actions	Check other events, then see BIOS postcode.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

BMC watchdog: Timeout followed by power Cycle

Description	timeout during BIOS init step which causes the configured action.
Severity	Critical.
Direction	Assertion.
Filter Number	30.
Actions	Check other events, then see BIOS postcode.
Comments	For more information about filters, see Configuring Alert Settings, on page 4-49.

B.11. Fan Box SEL Messages

FAN Box redundancy: Fanbox_X fully redundant

Description	Both of the fans in the Fanbox X are up and running.
Severity	Information.
Direction	Assertion.
Filter Number	17.
Actions	None.
Comments	X= Fan box (0 to 3). For more information about filters, see Configuring Alert Settings, on page 4-49.

FAN Box redundancy: Fanbox_X Redundancy lost

Description	Only one fan in the fanbox is up and running.
Severity	Non-critical.
Direction	Assertion.
Filter Number	18.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X= Fan box (0 to 3). For more information about filters, see Configuring Alert Settings, on page 4-49.

FAN Box redundancy: Fanbox_X Non redundant: Insufficient resources

Description	None of the fans is working in the fanbox_X.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	19.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	X= Fan box (0 to 3). For more information about filters, see Configuring Alert Settings, on page 4-49.

B.12. Power System Board SEL Messages

Power System Board: ACPI Pwr State: Working

Description	The system is powered on.
Severity	Information.
Direction	Assertion.
Filter Number	1.
Actions	None.
Comments	Notice that there is no deassertion event. For more information about filters, see Configuring Alert Settings, on page 4-49.

Power System Board: ACPI Pwr State: Soft off

Description	The system is powered off.
Severity	Information.
Direction	Assertion.
Filter Number	1.
Actions	None.
Comments	Notice that there is no deassertion event. For more information about filters, see Configuring Alert Settings, on page 4-49.

Appendix C. Backup/Restore the Configuration Data

This appendix contains the configuration data backup and restore procedures using the *KiraTool Environment utility*. It includes the folllowing topics:

- Backup Configuration Data, on page C-1
- Restore Configuration Data, on page C-1

C.1. Backup Configuration Data

1. Check that the *KiraTool Environment utility* is installed : the "Kira Tool Environment" icon must be present on your desktop.
   (For more information about the *KiraTool Environment utility* installation refer to Configuration Data Backup/Restore Tool on page 1-8.
2. From your desktop double click the "Kira Tool Environment" icon to open the dialog box.
3. Enter the following command:

```
kiratool cfg backup <filename>
```

where <*filename*> is the name of the file in which the configuration data is to be saved.

4. Carefully note the file name . It will be used later in the case of a restore operation.

C.2. Restore Configuration Data

1. Check that the *KiraTool Environment utility* is installed : the "Kira Tool Environment" icon must be present on your desktop.

Note For the *KiraTool Environment utility* installation, refer to Configuration Data Backup/Restore Tool in the *NovaScale 9006 Server Hardware Console User's Guide*.

2. Get the backup file name from the system administrator.
3. From your desktop double click the "Kira Tool Environment" icon to open the dialog box.
4. Enter the following command:

```
kiratool cfg restore <filename> forcemac
```

where:

<*filename*> is the backup file name from which the configuration data is restored.

forcemac (optional):
if used, restore the MAC address contained in the backup file.
if not used, keep the MAC address of the board

WARNING
The forcemac option is only to be used in the case of a data restoration on the same Embedded Management Board (OPMA), not in the case of a board replacement.

Glossary

A

ACPI

Advanced Configuration and Power Interface.
An industry specification for the efficient handling of power consumption in desktop and mobile computers. ACPI specifies how a computer's BIOS, operating system, and peripheral devices communicate with each other about power usage.

ARU

Add / Removeable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. An ARU can be nested and is not necessarily separable from other ARUs. A ARU is also known as an PMU.

B

Backup

A copy of data for safe-keeping. The data is copied form computer memory or disk to a floppy disk, magnetic tape or other media.

Base Operating System

The Operating System that is booted at initialization.

BCS

Bull Coherent Switch. This is the Bull eXternal Node Controller. Provides SMP upgradeability up to 16 processors. The BCS ensures global memory and cache coherence, with optimized traffic and latencies, in both IPF-preferred and XPF-preferred variants.

BIOS

Basic Input / Output System. A program stored in flash EPROM or ROM that controls the system startup process.

BIST

Built-In Self-Test.
See POST.

Bit

Derived from BInary digiT. A bit is the smallest unit of information a computer handles.

BMC

Baseboard Management Controller. See Embedded Management Controller.

BT

Block Transfer. One of the three standardized IPMI System interfaces used by system software for transferring IPMI messages to the BMC. A per-block handshake is used to transfer data (higher performance).

Byte

A group of eight binary digits (bit) long that represents a letter, number, or typographic symbol.

C

Cache Memory

A very fast, limited portion of RAM set aside for temporary storage of data for direct access by the microprocessor.

CD-ROM
Compact DisK Read-Only Memory. High-capacity read-only memory in the form of an optically readable compact disk.

CIM
Common Information Model Standard DMTF. Provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions.

Clipping
An Event filter criterion. Clipping is defined on a Count / Time basis aimed at routing a pre-defined number of messages only. Identical messages are counted and when the number of messages indicated in the Count field is reached within the period of time indicated in the **Time** field, no other messages will be selected for routing.

CMC
Corrected Memory Check condition is signaled when a hardware corrects a machine check error or when a MCA condition is corrected by firmware.

CMCI
Corrected Memory Check Interrupt.

CMCV
Corrected Memory Check Vector.

CMOS
Complementary Metal Oxide Semiconductor.
A type of low-power integrated circuits. System startup parameters are stored in CMOS memory. They can be changed via the system setup utility.

Cold Reset
A reset operation immediately following power-up. Also called Power-up reset.

Core
Core is the short name for the processor execution core implemented on a processor. A core contains one or more threads (logical processors).

CPLD
Complex Programmable Logic Device. A programmable logic device with a non volatile memory.

CRU
Customer Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by End User as a single entity.

CSE
Customer Service Engineer.

D

Default Setting
The factory setting your server uses unless instructed otherwise.

Device Driver
A software program used by a computer to recognize and operate hardware.

DIMM
Dual In-line Memory Module. The smallest system memory component.

DMA
Direct Memory Access. Allows data to be sent directly from a component (e.g. disk drive) to the memory on the motherboard). The microprocessor does not take part in data transfer enhanced system performance.

DNS
Domain Name Server. A server that retains the addresses and routing information for TCP/IP LAN users.

DPS
Distributed Power Supply.

DRAM
Dynamic Random Access Memory is the most common type of random access memory (RAM).

DSIB
Dummy BCS Interconnect Board.

DVO
Digital Video Out.

E

EEPROM
Electrically Erasable Programmable Read-Only Memory. A type of memory device that stores password and configuration data.

EFI
Extensible Firmware Interface. A specification for a firmware-OS interface.

EFI Shell
Simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the EFI Shell provides a set of basic commands used to manage files and the system environment variables. See Shell.

EMI
Electro-Magnetic Interference.

Embedded Management Controller
Also known as BMC (Baseboard Management Controller). This controller, embedded on the main system board, provides out-of-band access to platform instrumentation, sensors and effectors.

EMM
Embedded Management Module. Software embedded in the server module to implement management functions and accessible from the Hardware Console graphical interface.

EPROM
Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code is not lost when the computer is powered off.

ERP
Error Recovery Procedure.

Error
Manifestation of a fault. All faults do not result in an error. See Fault.

Error Detection
The process that determines the deviation between observed behavior and specified behavior.

ESD
ElectroStatic Discharge. An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

Event
The generation of a message (event message) by a software component and that is directed to the Event Manager.

Exclude
See Include / Exclude.

F

Fail-Over

Backup operational mode in which the functions of a system component (such as a processor, server, network, or database, for example) are assumed by secondary system components when the primary component becomes unavailable through either failure or scheduled down time.

Fatal Error

A fatal error may compromise system integrity and it may not be possible to continue operation. See Error.

Fault

An erroneous state resulting from observed behavior deviating from specified behavior. Some faults may result in an error. See Error.

Flash EPROM

Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the the system firmware code. This code can be replaced by an updated code from a floppy disk, but is not lost when the computer is powered off.

Firewall

A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

Firmware

An ordered set of instructions and data stored to be functionally independent of main storage.

FPGA

Field Programmable Gate Array. Device containing programmable logic components and programmable interconnects.

FRU

Field Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by Customer Service Engineers as a single entity.

FTP

File Transfer Protocol. A standard Internet protocol: the simplest way of exchanging files between computers on the Internet. FTP is an application protocol that uses Internet TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It is also commonly used to download programs and other files from other servers.

G

GUI

Graphical User Interface.

H

HA

High Availability. Refers to a system or component that is continuously operational for a desirably long length of time.

Hard Reset

A reset event in the system that initializes all components and invalidates caches.

Hardware

The physical parts of a system, including the keyboard, monitor, disk drives, cables and circuit cards.

Hardware Corrected Error

Correctable errors are corrected by hardware while software is completely oblivious to their occurence. See Error.

Hardware Partition
A set of hardware components that can boot and run a Base OS image.

Hard Partitioning
Ability to split a platform into a number of independent smaller hardware partitions or to merge multiple independent hardware partitions to form a single larger hardware partition.

Hardware Uncorrected Error
Uncorrectable errors are not corrected by hardware, but are contained. System state remains intact and the process and system are restartable. A system shutdown may be required. See Error.

HPC
High Performance Computing.

Host Operating System
The Operating System that is booted at initialization and that is a Virtual Machine Monitor (VMM) and a number of guest OS.

Hot-Plugging
The operation of adding a component without interrupting system activity.

Hot-Swapping
The operation of removing and replacing a faulty component without interrupting system activity.

HT
HyperThreading. See Multi-Threading.

HTTP
HyperText Transfer Protocol.
In the World Wide Web, a protocol that facilitates the transfer of hypertext-based files between local and remote systems.

I

I2C
Intra Integrated Circuit.
The I2C (Inter-IC) bus is a bi-directional two-wire serial bus that provides a communication link between integrated circuits (ICs).
The I2C bus supports 7-bit and 10-bit address space devices and devices that operate under different voltages.

IB
InfiniBand.

IC
Integrated Circuit. An electronic device that contains miniaturized circuitry. See Chip.

iCare
he iCare Console (insight Care) is a web-based administration application which provides tools for hardware unit maintenance.

ICH
Input Output Hub. Provides a connection point between various I/O components and Intel processors.

ICMB
Intelligent Chassis Management Bus.
Name for the architecture, specifications, and protocols used to interconnect intelligent chassis via an RS-485-based serial bus for the purpose of platform management.

ILB I/O Legacy Board.

Interface
A connection between a computer and a peripheral device enabling the exchange of data. See Parallel Port and Serial Port.

Include / Exclude

A physically present ARU can be logically connected to / disconnected from the hardware partition at boot time, under control of the Platform Management software. This is a static logical operation.
An excluded ARU can be reserved as a spare, locked for future user (Pay-As-You-Grow), or marked as failed.

Initialization

The set of firmware or micro-code sequences that follow warm or cold reset.

I/O

Input /Output. Describes any operation, program, or device that transfers data to or from a computer.

IOH

Input/Output Hub. An Intel QPI agent that handles I/O requests for processors.

IP

Internet Protocol. The protocol by which data is sent from one computer to another via the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IPL

Initial Program Load. It defines the firmware functional phases during the system initialization.

IPM

Intelligent Platform Management.

IPMB

Intelligent Platform Management Bus.
Abbreviation for the architecture and protocol used to interconnect intelligent controllers via an I2C based serial bus for the purpose of platform management.

IPMI

Intelligent Platform Management Interface.
A specification owned by Intel which describes mechanisms and devices to completely offload the task of managing system hardware from the primary CPU.

J

Jumper

A small electrical connector used for configuration on computer hardware.

K

KCS

Keyboard Controller Style. One of the standardized IPMI System interface, that system software can use for transferring IPMI messages to the BMC. Data are transferred using a per-byte handshake.

KVM

Keyboard Video Mouse. Hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse.

L

LAN

Local Area Network. A group of computers linked together within a limited area to exchange data.

LCP

Local Control Panel. Module consisting of a controller, a LCD color display, a green and a blue LED and a Power ON button.

LDAP
Lightweight Directory Access Protocol. Application protocol for querying and modifying directory services running over TCP/IP.

LED
Light Emitting Diode. A small electronic device that glows when current flows through it.

Legacy Application
An application in which a company or organization has already invested considerable time and money. Typically, legacy applications are database management systems (DBMSs) running on mainframes or minicomputers.

Logical Partition
When the Base Operating System is a Virtual Machine Monitor, a logical partition is the software environment used to run a Guest Operating System.

Logical Processor
See Thread.

LUN
Logical Unit Number. Term used to designate Logical Storage Units (logical disks) defined through the configuration of physical disks stored in a mass storage cabinet.

M

MAC
Media Access Control. A data communication protocol sub-layer that provides addressing and channel access control mechanisms allowing several terminals or network nodes to communicate within a multipoint network, typically a local area network (LAN).

MC
Management Controller.

MESCA
Multiple Environments on a Scalable Csi-based Architecture.

Memory
Computer circuitry that stores data and programs. See RAM and ROM.

Microprocessor
An integrated circuit that processes data and controls basic computer functions.

MII
Media Independent Interface. A standard interface used to connect a Fast Ethernet (i.e. 100Mb/s) chip to a physical layer tranceiver. The MII may connect to an external transceiver device via a pluggable connector or simply connect two chips on the same printed circuit board. See MAC.

MIMD
Multiple Instruction Multiple Data

Mirrored volumes
A mirrored volume is a fault-tolerant volume that duplicates your data on two physical disks. If one of the physical disks fails, the data on the failed disk becomes unavailable, but the system continues to operate using the unaffected disk.

MTB
Memory and Tukwila Board.

MTBF
Mean Time Between Failure. An indicator of expected system reliability calculated on a statistical basis from the known failure rates of various components of the system. Note: MTBF is usually expressed in hours.

Multicore
Presence of two or more processors on a single chip.

Multimedia

Information presented through more than one type of media. On computer systems, this media includes sound, graphics, animation and text.

Multi-Tasking

The ability to perform several tasks simultaneously. Multi-tasking allows you to run multiple applications at the same time and exchange information among them. See Task.

Multi-Threading

The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.

Depending on core design, the instructions issued for execution by the core at a given cycle may be either **Hyper-Threading** (HT) - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or **Simultaneous Multi-Threading** (SMT) - from both threads.

N

NFS

Network File System. A proprietary distributed file system that is widely used by TCP/IP vendors. Note: NFS allows different computer systems to share files, and uses user datagram protocol (UDP) for data transfer.

NIC

Network Interface Controller.

NUMA

Non Uniform Memory Access. A method of configuring a cluster of microprocessors in a multiprocessing system so that they can share memory locally, improving performance and the ability of the system to be expanded.

NVRAM

Non Volatile Random Access Memory. A type of RAM that retains its contents even when the computer is powered off. See RAM and SRAM.

O

OF

Open Firmware. Firmware controlling a computer prior to the Operating System.

Off-Lining

See On-Lining / Off-Lining.

On-Lining / Off-Lining

On-lining and off-lining are dynamic logical operations.

On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected).

Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

OOB

Out Of Band. Access to system platform management that does not go through the OS or other software running on the main processors of the managed system.

Operating System

See OS.

OPMA

Open Platform Management Architecture Board.

OS
Operating System. The software which manages computer resources and provides the operating environment for application programs.

P

Password
A security feature that prevents an unauthorized user from operating the system.

PCI
Peripheral Component Interconnect. Bus architecture supporting high-performance peripherals.

PCIe
PCI Express. Latest standard in PCI expansion cards.

PDB
Power Distribution Board. Sub-assembly of the Power Supply Module.

PDU
Power Distribution Unit. Power bus used for the connection of peripheral system components.

PEF
Platform Event Filtering.
A feature in IPMI that enables the BMC to generate a selectable action (e.g. power on/off, reset, send Alert, etc.) when a configurable event occurs on the management system.

ping
A basic Internet program that lets you verify that a particular IP address exists and can accept requests. The verb "to ping" means the act of using the ping utility or command.

PIROM
Processor Information ROM contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S-spec numbers, and a 64-bit processor number.

Plugging / Unplugging
Plugging and unplugging are static physical operations and represent the physical insertion / removal of a standard ARU.
Plugging and unplugging procedures guarantee the electrical protection of live parts.

PMU
Physically Manageable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. A PMU can be nested and is not necessarily separable from other PMUs. A PMU is also known as an ARU.

PNP
Plug aNd Play. The ability to plug a device into a computer and have the computer recognize that the device is there.

POR
Power On Reset. Operation performed at the power on of the system.

POST
Power On Self Test. When power is turned on, POST (Power-On Self-Test) is the diagnostic testing sequence (or "starting program") that a computer runs to determine if hardware is working correctly.

Power-up Reset
See Cold Reset.

Processor
Each processor contains one or more dies in a single package. Each die contains one or more cores. Each core contains one or more threads (logical processors). Each processor is housed in a processor socket.
definition

PROM
Programmable Read-Only Memory.

PSB
Power Supply Box. AC powering unit providing DC to a server. Each Power Supply Module comprises a certain number of Power Supply Units (PSU) and a Power Distribution Board (PDB).

PSMI
Power Supply Management Interface.

PSU
Power Supply Unit. Sub-assembly of the Power Supply Module.

Q

QPI
Quick Path Interconnect. High-speed point-to-point Intel interface, used to interconnect processors and I/O Hubs, and optionally node controllers (BCS).

R

RADIUS
Remote Authentication Dial-In User Service. Authentication protocol. Radius is a server for remote user authentication and accounting. Its primary use is for Internet Service Providers, though it may be used on any network that needs a centralized authentication and/or accounting service for its workstations.

RAID
Redundant Array of Independent Disks. A method of combining hard disk drives into one logical storage unit for disk-fault tolerance.

RAM
Random Access Memory. A temporary storage area for data and programs. This type of memory must be periodically refreshed to maintain valid data and is lost when the computer is powered off. See NVRAM and SRAM.

RAS
Reliability, Availability, Serviceability.

Real-Time Clock
The Integrated Circuit in a computer that maintains the time and date.

Reset
A set of hardware-based events that result in a deterministic initial hardware state.

Recoverable Error
Recoverable errors include errors that are software correctable or hardware / software uncorrectable, for which servicing may be required for containment and restoration. See Error.

RFB
Remote Frame Buffer. Simple protocol for remote access to graphical user interfaces.

RFI
Radio Frequency Interference.

RMII
Reduced Media Independent Interface. A standard that reduceds the number of signals/pins required to connect an Ethernet chip to physical layer transceiver. See MII.

RJ45
8-contact regular jack.

ROM
Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code cannot be altered and is not lost when the computer is powered off. See BIOS, EPROM and Flash EPROM.

RTC
Real Time Clock.

S

SAS
Serial Attached SCSI. A data transfert technology used to move data to and from computer storage devices such as hard drives and tape drives.

SATA
Serial ATA. A computer bus technology for connecting hard disks and other devices.

SDR
Sensor Data Record. SDRs provide the information that tells management software what sensors, events, management controllers, and FRU information is available from a given IPMI implementation.

SDRR
Sensor Data Record Repository. A required feature of an embedded management controller, this is the material list for IPMI.

SDRAM
Synchronous Dynamic Random Access Memory.
A type of DRAM that runs at faster clock speeds than conventional memory. See DRAM.

SEL
System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.
A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

Server Hardware Console
Graphical user interface used to access the management software embedded in the server module. See Hardware Console.

Simultaneous Multi-Threading
See Multi-Threading.

SMBIOS
System Management BIOS.

SM-BUS
System Management Bus.

SMI
System Management Interrupt.

SMP
Symmetrical Multi Processor. The processing of programs by multiple processors that share a common operating system and memory.

SMT
Simultaneous Multi-Threading.

SNC
Scalable Node Controller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

SNMP
Simple Network Management Protocol. The protocol governing network management and the monitoring of network devices and their functions.

SOAP
Simple Object Access Protocol. A call-response mechanism for XML documents.

Socket
Central Processing Unit mutlticore interface.

SOL
Serial Over LAN. Mechanism that enables the input and output of the serial port of a managed system to be redirected via an IPMI session over IP.

SPD
Serial Presence Detect. DIMM PROM.

SR
Scratch Register. Internal registers of both the Tukwila processor and the I/O Hub used as scratch area.

SRAM
Static RAM. A temporary storage area for data and programs. This type of memory does not need to be refreshed, but is lost when the system is powered off. See NVRAM and RAM.

SSH
Secure Shell. Network protocol that allows data to be exchanged using a secure channel between two networked devices.

Surprise Reset
A warm reset operation occuring during software operations, without allowing the OS to perform a graceful shutdown. The hardware partition may be in a hang-up situation preventing normal software partitions.

SVGA
Super Video Graphics Array.

T

TCP
Transmission Control Protocol. A set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.

TCP/IP
Transmission Control Protocol / Internet Protocol. The basic communication language or protocol of the Internet.

T&D
Tests and Diagnostics.

Thread
A thread or logical processor is the execution context within a single core and the software visibility of multi-threading. A single multi-threaded processor contains two or more threads (or logical processors).

Thresholding
An Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, this message is selected for routing.

TKW
TUKWILA Intel Itanium Processor (4 cores per die).

U

Unplugging
See Plugging / Unplugging.

URL
Uniform / Universal Resource Locator. The address of a file (resource) accessible on the Internet.

USB

Universal Serial Bus. A plug-and-play interface between a computer and add-on devices. The USB interface allows a new device to be added to your computer without having to add an adapter card or even having to turn the computer off.

V

VGA

Video Graphics Array.

VLAN

Virtual Local Area Network. A local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

VMM

Virtual Machine Monitor.

W

WAN

Wide Area Network. Geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN).

Warm Reset

The second and successive reset after a cold reset. See Cold Reset.

WOL

A feature that provides the ability to remotely power on a system through a network connection.

X

XCSI

Extended Common System Interface. High-speed point-to-point Bull interface, used to interconnect servers. XCSI ports are located and managed in the BCS (node controller).

XML

eXtended MarkUp Language. A flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

XNC

External Node Controller. See BCS.

Y

No entries.

Z

ZOAR

Double port Intel GB Ethernet chips.

Index

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

REFERENCE
86 A1 70FA 00