bullx S6000 Server Hardware Console

User's Guide

extreme computing

REFERENCE
86 A1 50FD 06

bullx S6000 Server Hardware Console

User's Guide

Hardware

August 2011

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

REFERENCE
86 A1 50FD 06
V11.07.13

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

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 the manufacturer 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

VCCI Statement

This equipment complies with the VCCI V-3/ 2008-4 requirements.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions. A VCCI regulatory label is affixed to the equipment.

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
Products 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.

Safety Recommendations

Danger and Warning Notices

DANGER
Only hot-pluggable components can be serviced (added, removed, replaced) without powering down the equipment.
If the component is NOT hot-swappable, the equipment must be powered down PRIOR to servicing and the AC power cables must be disconnected from the electrical outlet.

DANGER
Failure to disconnect AC power cables before servicing the equipment may result in personal injury and damage to equipment.
It is mandatory to remove AC power cables from electrical outlets before relocating cabinets and systems.

DANGER
Hazardous voltage, current, and energy levels are present inside the power supply.
Hazardous electrical conditions may be present on power, telephone, and communication cables.
Energy hazard:
Remove all jewelry before servicing.

DANGER
The Ultracapacitor may retain a charge after power is removed. This charge may result in personal injury and damage to equipment.
It is mandatory not to touch any parts until the Ultracapacitor has fully discharged.

A faulty Ultracapacitor may release electrolyte fluid.
It is mandatory to wear protection gloves and protection glasses to avoid contact with skin and eyes when handling the Ultracapacitor.

DANGER
The onboard battery should be replaced regularly. It must be replaced with the same or an equivalent type recommended by the manufacturer. There is a danger of explosion if another type is used. Dispose of used batteries according to the manufacturer's instructions.

DANGER
Basic electrical safety precautions should be followed to protect yourself from harm and the drawer from damage.
If an electrical accident occurs, shutdown the power by removing the power cord from the server.

WARNING
Optimum cooling and airflow is ensured when cabinets and systems are closed.
Once the maintenance / service intervention has been completed, all cabinet and system covers and doors should be refitted and closed rapidly.

Important Notices

LABELING

Use labels to note the orientation and position of any cables, components, shielding or connectors removed.

HANDLING STATIC-SENSITIVE DEVICES

The following precautions must be taken when handling static-sensitive devices:

- **Systematically wear an antistatic wriststrap when handling components.**
- **Touch the cabinet frame to release static before handling boards.**
- **Hold cards, boards and drives by the edges.**
- **Only remove the device from the antistatic container when you are ready to install it.**
- **If you need to lay the device down while it is out of the antistatic container, lay it on the conductive foam pad.**

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

This list is not exhaustive. Useful documentation is supplied on the Resource & Documentation CD(s) delivered with your system. You are strongly advised to refer carefully to this documentation before proceeding to configure, use, maintain, or update your system.

- *Site Preparation Guide,* 86 A1 40FA
  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.
- *bullx S6030 Installation Guide*, 86 A1 26FE
  explains how to install and start the server for the first time. This guide is intended for use by qualified support personnel.
- *bullx S6030 Service Guide*, 86 A7 85FB
  explains how to service the server. This guide is intended for use by qualified support personnel.
- *bullx S6010 Installation Guide*, 86 A1 86FB
  explains how to install and start the server for the first time. This guide is intended for use by qualified support personnel.
- *bullx S6010 Service Guide*, 86 A7 87FB
  explains how to service the server. This guide is intended for use by qualified support personnel.
- *bullx Cabling Guide*, 86 A1 94FE
  explains how to cable a bullx multi-modules configuration. This guide is intended for use by server administrators, operators and qualified support personnel.
- *iCare Console User's Guide,* 86 A1 71FA
  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 to Know the Server

This chapter gives an overview of server features and components. It includes the following topics:

1.1. Overview

Bull servers for business and scientific applications are based upon the MESCA architecture (Multiple Environments on a SCalable Architecture), leveraging the latest generation of Intel Xeon processors, Intel QPI protocol, Bull BCS technology and Infiniband QDR interconnect. Servers are designed to attain petascale performance while optimizing power consumption and heat dissipation. Two types of systems are available, according to your needs:

bullx S6010 server

The bullx S6010 server high-density compute node provides up to 4 processor sockets, 32 memory DIMMs, and 1 internal hard disk drive per 1.5U drawer. Its unique "L" design allows 2 modules to be slotted together to offer up to 8 processor sockets, 64 memory DIMMs and 2 internal hard disk drives per 3U assembly.

Up to 4 bullx S6010 servers can be interconnected via the BCS (Bull Coherence Switch) to form a 6U SMP compute node providing up to 16 processor sockets and 128 memory DIMMs in a 6U assembly.

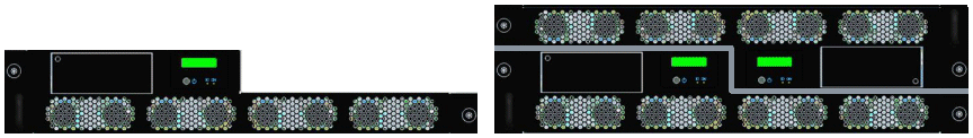


Figure 1-1. bullx S6010 server

bullx S6030 server

The bullx S6030 server compute and/or service node provides up to 4 processor sockets, 32 memory DIMMs, 6 PCI-e slots, and 8 internal hard disk drives per 3U drawer. Optionally, a DVD drive can be installed in a disk drive slot.

Up to 4 bullx S6030 servers can be interconnected via the BCS (Bull Coherence Switch) to form a 12U SMP compute and/or service node providing up to 16 processor sockets, 128 memory DIMMs and 24 PCI-e slots. The addition of LSI boards provides 8 up to 32 internal disks.

Figure 1-2. bullx S6030 server

Servers are rack-mounted in Bull cabinets for optimized deployment time and enhanced reliability.

Figure 1-3. bullx S6000 series

For future reference, you are advised to record the following data indicated on the labels affixed to the server drawer:

System	Data
Product Name	
Product Code	
Product Number	
System Serial Number	

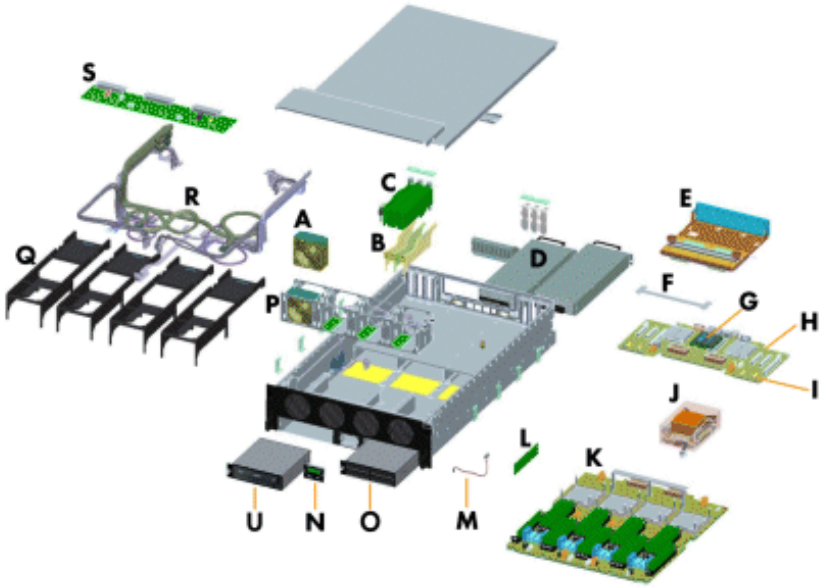
Table 1-1. Server product data

1.2. Components, Controls, LEDs and Ports

1.2.1. bullx S6030 server

Components (Exploded view)

The following diagram shows an exploded view of server components:



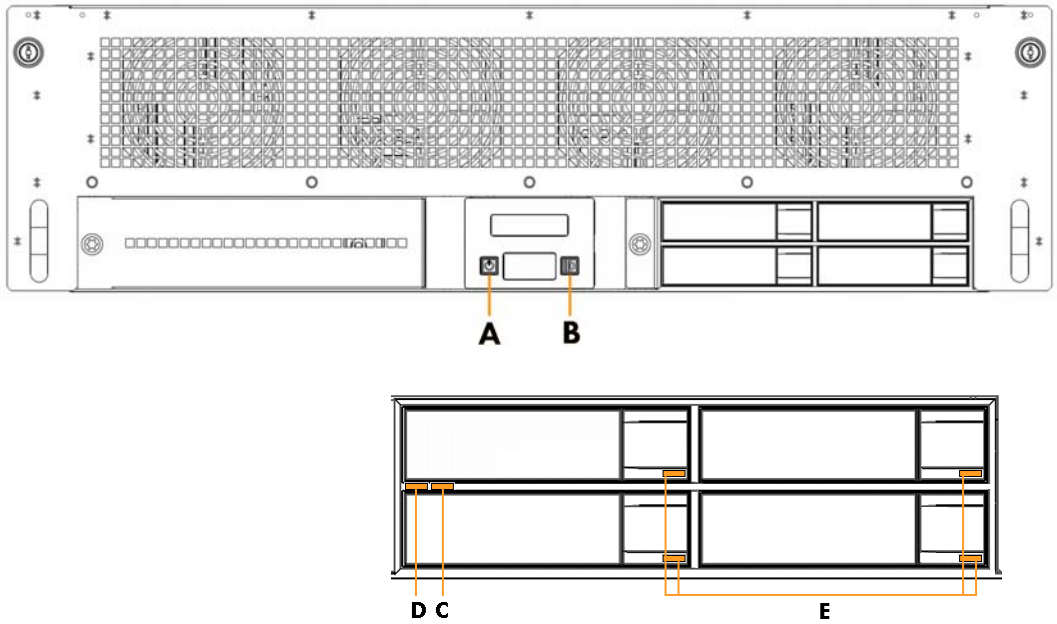
Mark	Description	Quantity
A	Fan Unit	8
B	PCIe Separator	2 to 4
C	PCIe Card	Up to 6
D	Power Supply Unit	1 or 2
E	Dummy CSI Interconnect Board (DSIB) or CSI Interconnect Board (SIB)	1
F	Prepositioner	1
G	Embedded Management Controller	1
H	I/O Legacy Board (ILB)	1
I	ICH battery	1
J	Nehalem Assembly Processor Assembly	Up to 4
K	Memory Xeon Board (MXB)	1
L	Memory Module	Up to 32
M	Anti-Intrusion Switch	1
N	Local Control Panel (LCP)	1
O	Hard Disk Box (HDX)	1 or 2
P	Fan Box	1
Q	Air Duct	4
R	Internal Cable Kit	1
S	Power Distribution Board Unit (PDBU)	1

Mark	Description	Quantity
Not illustrated	Ultra Capacitor	1
U	DVD Drive (Optional)	1

Figure 1-4. Server components - Exploded view

Controls and LEDs (Front view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the front of the server.

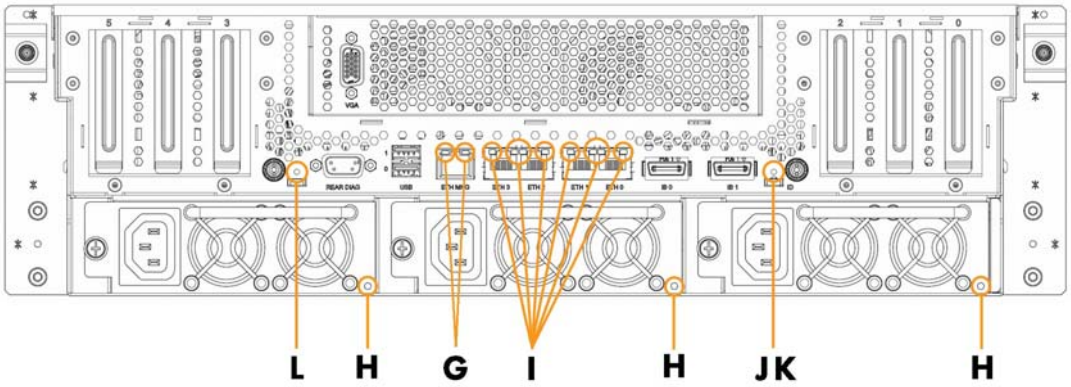


Mark	LED/Button	Color	Description
A	Power LED/Button	Blinking Green Solid Green	Server power on stand-by. Server powered up.
B	ID LED/Button	Blinking Blue	ID button pressed or activated from the Server Hardware Console; simultaneously lights the BLUE ID LED (G) on the rear of the server.
C	Disk Fan Failure LED	Blinking Amber	Disk Fan failure.
D	Disk Overheat LED	Blinking Amber	Disk overheat failure.
E	Disk Activity LED	Blinking Green	Disk active.

Figure 1-5. Server LEDs and buttons - Front view

Controls and LEDs (Rear view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the rear of the server.

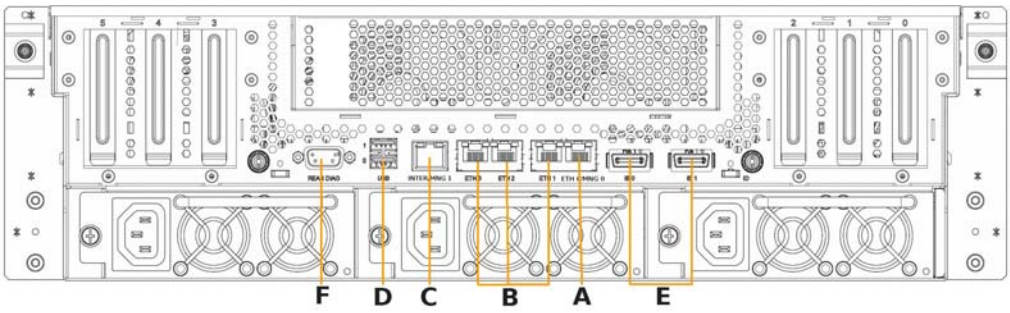


Mark	LED/Button	Color	Description
G	Management Port Left LED	Solid Green Blinking Green	Link active. Link inactive.
G	Management Port Right LED	Solid Orange Off	100 MBit/s. 10 MBit/s.
H	Power Supply Unit LED	Solid Green Blinking Green Blinking Amber	Power supply unit powered up. Power supply unit on stand-by. Power supply unit fault.
I	Gbit Port Left LED	Green Orange Off	1 GBit/s. 100 MBit/s. 10 MBit/s.
I	Gbit Port Right LED	Solid Green Blinking Green	Link established. Link active.
J	Reset Button	N/A	Resets the Embedded Management Controller.
K	ID LED	Blinking Blue	ID button (B) on the front of the server pressed or activated from the Server Hardware Console.
L	Return to Defaults Button	N/A	Returns the Embedded Management Controller settings to default values.

Figure 1-6. Server LEDs and buttons - Rear view

Connection Ports (Rear view)

The following diagram shows the connection ports on the rear of the server.



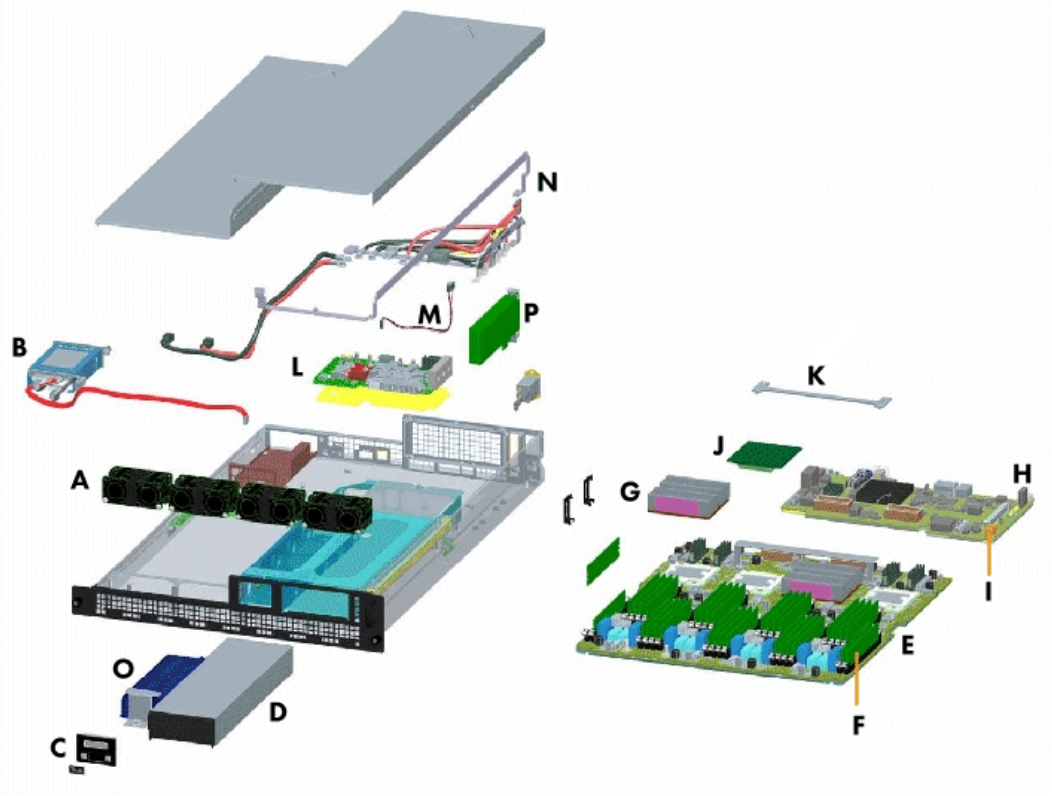
Mark	Description
A	ETH0/MNG0 (RJ45) port: Shared Management / Host network port, or Host network port only if INTER/MNG1 (C) is used for the Management network
B	ETH1, ETH2, ETH3 (RJ45) ports: Enterprise network port
C	INTER/MNG1 (RJ45): Dedicated Management network / module interconnexion port
D	USB key ports
E	INFINIBAND ports: Infiniband network port (Optional)
F	VGA port

Figure 1-7. Server connection ports - Rear view

1.2.2. bullx S6010 server

Components (Exploded view)

The following diagram shows an exploded view of server components:

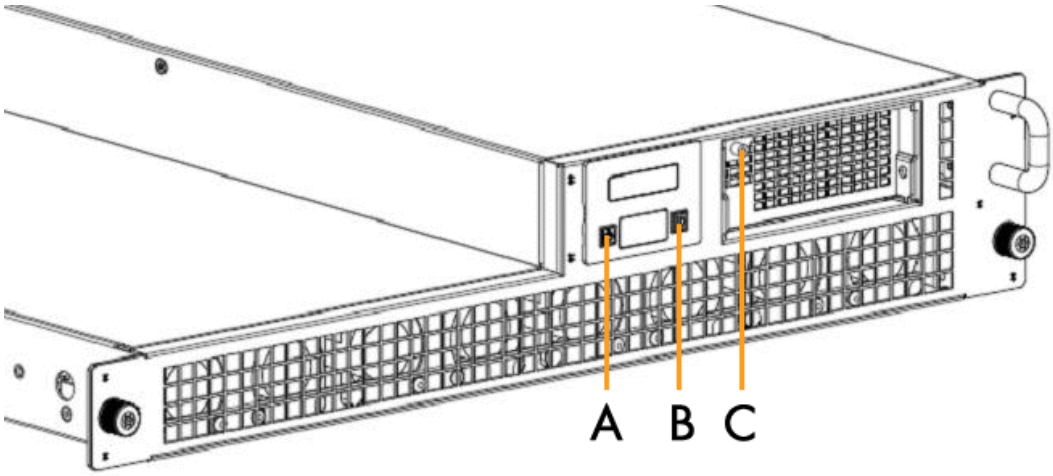


Label	Description	Quantity
A	Cooling Unit	4
B	Hard Disk Drive (HDD)	1
C	Local Control Panel (LCP)	1
D	Power Supply Unit	1
E	Memory Xeon Board (MXB)	1
F	Memory Module	Up to 32
G	Nehalem Assembly Processor	Up to 4
H	I/O Legacy Board (ILBL)	1
I	ICH battery	1
J	Dummy CSI Interconnect Legacy Board (DSIBL)	1
K	Prepositioner	1
L	Power Distribution Board Unit (PDBU)	1
M	Anti-Intrusion Switch	1
N	Internal Cable Kit	1
O	Ultra Capacitor	1
P	PCIe Card	1

Figure 1-8. Server components - Exploded view

Controls and LEDs (Front view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the front of the server.

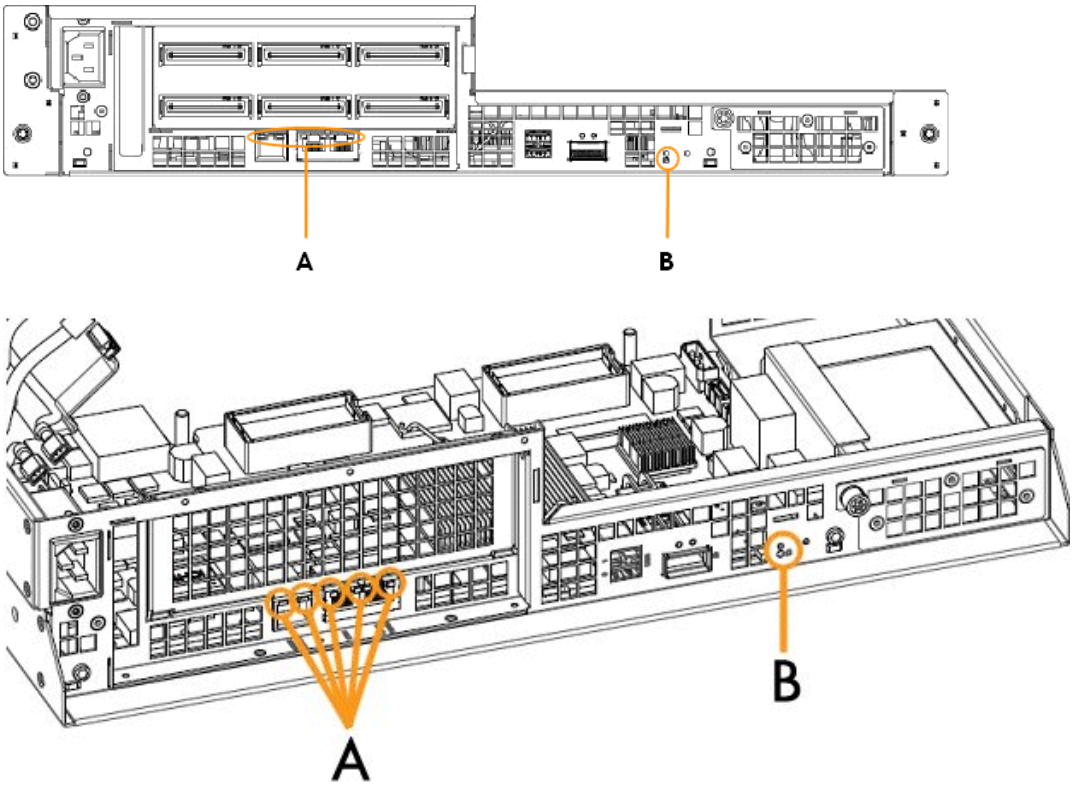


	Label Name	Description
A	Power LED/Button	Flashing Green: server power on stand-by. Still Green: server powered up.
B	ID LED/Button	Flashing Blue: ID button pressed or activated from the Server Hardware Console. Simultaneous lights the BLUE ID LED on the rear of the server.
C	Power Supply Unit Leds	Still Green: power supply unit powered up. Flashing Green: power supply unit on stand-by. Flashing Amber: power supply unit fault.

Figure 1-9. Server LEDs and buttons - Front view

Control and LEDs (Rear view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the rear of the server.



Label	Name	Description
A	Ethernet Activity LEDs	Indicates network activity status. There is one management port and 2 Gbit ports. For the management port: Left LED: Still Green: link active. Flashing Green: link inactive. Right LED: Still Orange: rate 100MB/s Extinguished: rate 10 MB/s For the Gbit ports: (to the right of each port) Left LED: Green: rate 1GB/s Orange: 100 MB/s Extinguished: 10 MB/s Right LED: Still Green: link established. Flashing Green: link active.
B	ID LED	Flashing Blue

Figure 1-10. Server LEDs and buttons - Rear view

Connection ports (Rear view)

The following diagram shows the connection ports on the rear of the server.

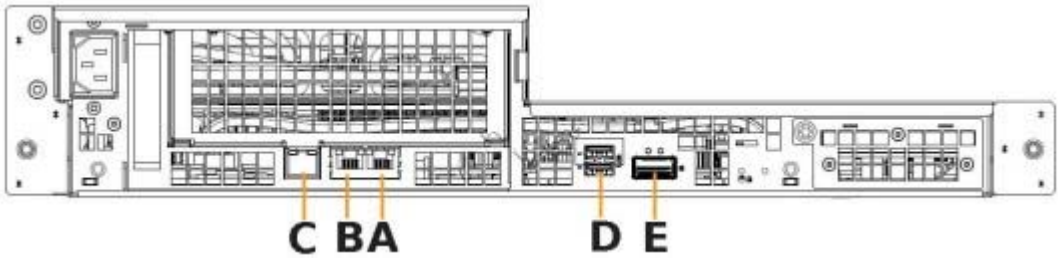


Figure 1-11. Mono-module Server connection ports - Rear view

Mark	Description
A	ETH0/MNG0 (RJ45) port: Shared Management / Host network port, or Host network port only if INTER/MNG1 (C) is used for the Management network
B	ETH1 (RJ45) port: Enterprise network port
C	INTER/MNG1 (RJ45): Dedicated Management network port, or server interconnection port (multi-module models)
D	USB ports
E	INFINIBAND port: Infiniband network port

Chapter 2. 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:

2.1. Starting the Hardware Console

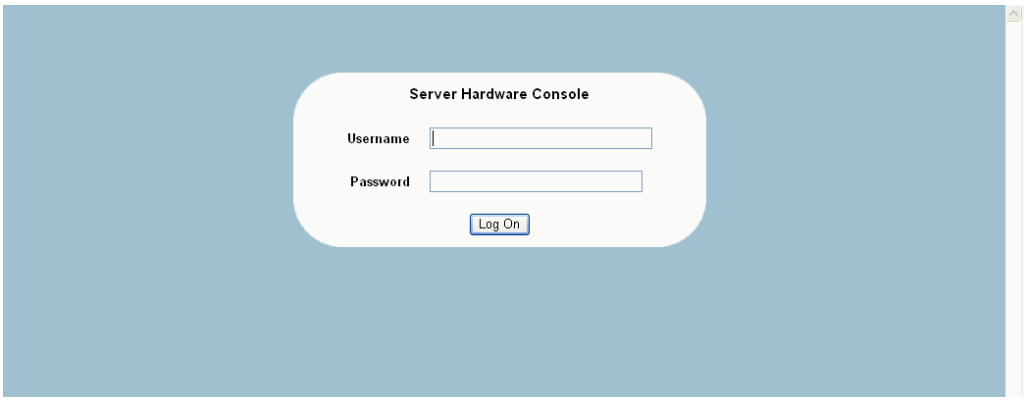
The hardware console is launched from a Web browser using a standard or secure IP address or host name, according to settings.

Prerequisites

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

Procedure

1. Launch your web browser and 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 2-1. Logon

2. Complete the **Username** and **Password** fields and click **Log On**. Once you are authenticated, the **System Control** tab 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.**
If you lose your account details and are unable to connect to the console, please contact your Customer Service Representative.

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

What To Do if an Incident Occurs?

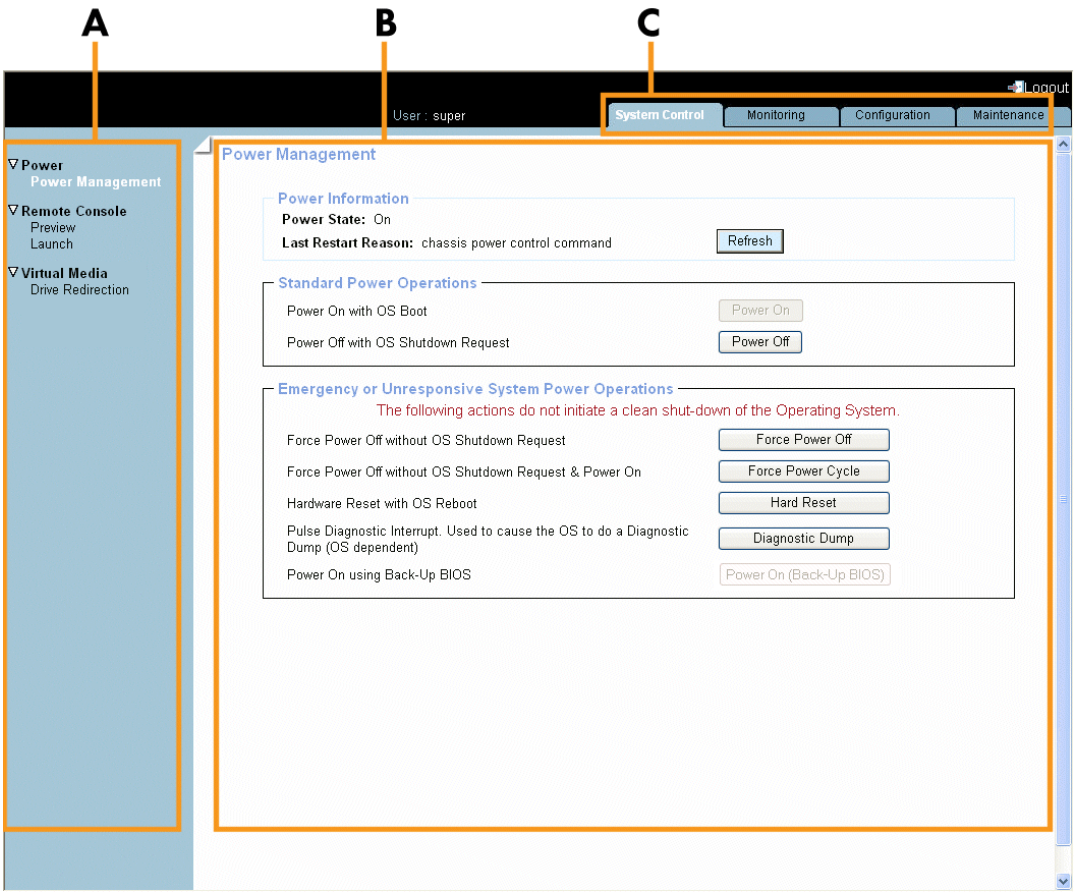
If you cannot connect to the console or if the web pages are displayed incorrectly, one of the following problems may be the cause:

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

2.2. Hardware Console Overview

The Hardware Console is a web-based administration application embedded on the management controller. You can use the Hardware Console to remotely operate, monitor and maintain hardware and to configure the embedded management controller. The Hardware Console can be accessed via the enterprise LAN using a Microsoft Internet Explorer or Mozilla Firefox browser.

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



Console Overview	
A: Navigation tree	Provides access to console features. Note that displayed features differ according to the tab selected.
B: Work pane	The work pane displays the commands and information associated with the item selected in the navigation tree.
C: Tabs	Four tabs allow access to four sets of features accessible from the associated navigation trees: System Control, Monitoring, Configuration and Maintenance.

Figure 2-2. Hardware Console overview

Console Interface Features

The following table lists the features available from the interface and associated permissions.

Tab	Tree Node		Feature	Permission
System Control	Power Management	Power	Power Information	*None*
		Power	Standard Power Operations	Power Control
		Power	Emergency Power Operations	Power Control
	Remote Console	Preview	Preview	Remote Control Access
		Launch	-	Remote Control Access
	Virtual Media	Drive Redirection	Drive Redirection	Virtual Media Upload
Monitoring	System Health	Sensor Status	Viewing and Refreshing	*None*
		System Event Log	Viewing and Refreshing	
			Clearing	Alert Settings & Clear SEL
		Messages	Viewing and Clearing	Log View
Configuration	Global Settings	Platform	Platform Settings	Network Settings
		Managed Server	Managed Server Settings	Network Settings
		Functional Profiles	Functional Profile Settings	Network Settings
	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
		Messages	Event Management Settings	Log Settings Network Settings
	BMC User Management	Users	User Management	User/Group Management
		Groups	Group Management	
		Password	Password Management	Change Password
	Security	Encryption	Encryption Management	Security Settings
		SSL Certificate	SSL Certificate Management	SSL Certificate Management
		User Logon Policy	User Logon Policy Management	Security Settings
		Authentication	Authentication Management	Authentication Settings
		Power Button Lockout	Power Button Lockout Management	Security Settings
		User Lockout	User Lockout Management	
	Remote Console Settings	User Specific	User Specific RC Settings Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine	Remote Console Access
			Transmission Encoding	RC Settings (Encoding)
			Miscellaneous RC Settings	RC Settings (Monitor Mode) RC Settings (Exclusive Access)
			Mouse Hotkey	RC Settings (Hotkeys)
			Remote Console Button Key	
		Keyboard/ Mouse	Keyboard/Mouse Settings	RC Keyboard/Mouse Settings
		Filters	Filter Settings	

Tab	Tree Node		Feature	Permission
	Alert Settings	Policies	Policy Settings	Alert Settings & Clear SEL
		LAN Destinations	LAN Destination Settings	
		General	General Settings	
Maintenance	Hardware Information	Management Controller	Management Controller Information	*None*
		FRU	FRU Information	
		Firmware Version	Firmware Information	
	Firmware Update	*Listed firmware*	Firmware Update	Firmware Update
	Maintenance Operations	Unit Reset	Reset Management Controller	Maintenance/Board Reset
			Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine	Remote Console Access
		Identification LED	ID LED Management	Alert Settings & Clear SEL
		Hardware Exclusion	Hardware Exclusions	Maintenance/Board Reset
		Connected Users	Connected Users Information	*None*

Table 2-1. Interface features and permissions

2.3. Stopping the Hardware Console

You can stop the console at any time by clicking the **Logout** link (

)in the upper-right corner of the console.

You can stop the console at any time by clicking the **Logout** button.

2.4. 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 6, Configuring the Server Management Controller, and are listed below by order of priority:

- Configuring Network Settings for Remote Access, on page 6-6
- Configuring the Managed Server Name, on page 6-3
- Configuring Platform Identification Settings, on page 6-2
- Modifying Internal Clock Settings, on page 6-10
- Setting Up the Remote System Console, on page 4-2

Note The other configuration tasks can be performed when required.

Important **If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for installation instructions.**

2.5. Installing the KiraTool Utility

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

You are advised to install this utility so that you can back up and restore your configuration data.

Note For updated information concerning *KiraTool*, refer to the associated documentation available on the *Resource and Documentation CD*.

Windows Version

1. Locate the *KiraTool* self-extracting executable file (for example, KiraTool.exe) on the *Resource and Documentation CD*.
2. Double-click the file with your left mouse-button and follow the instructions on the screen.
3. At the end of the procedure, select FINISH and a KiraTool icon will automatically appear on your desktop.
4. To use the KiraTool utility, click the icon to open a standard Windows Command Line box in the correct directory.
   The following commands and options are available:

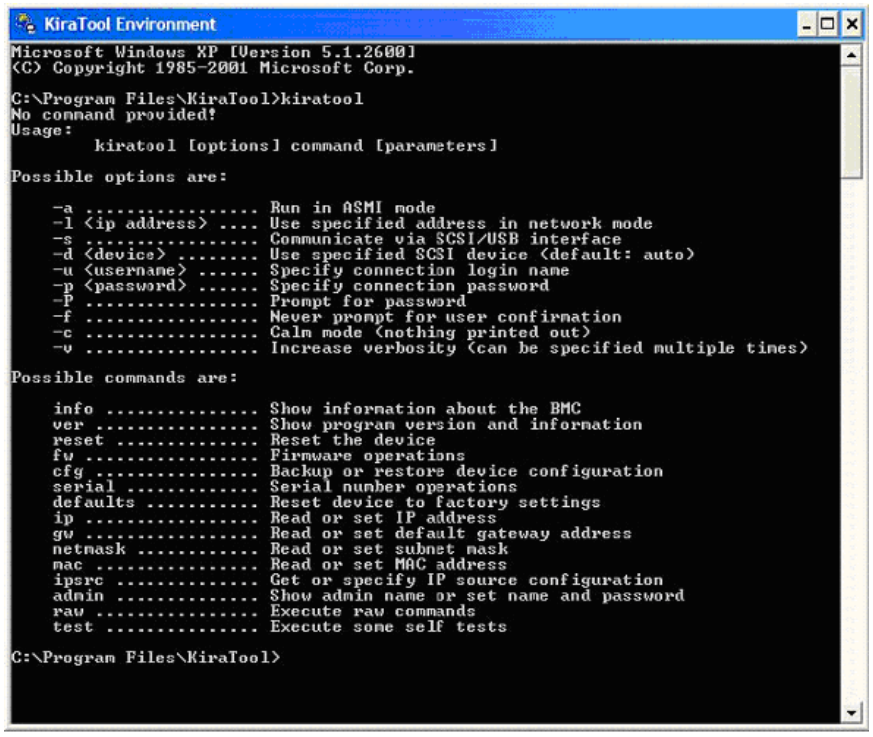


Figure 2-3. KiraTool Commands and Options - Windows

Linux Version

1. Locate the KiraTool executable file (for example KiraTool) on the *Resource and Documentation CD* .
2. Copy the executable file to a directory in your $PATH environment, for example **/usr/local/bin**. As such $PATH system directories are protected, you must log on as **root**:

```
linux # cp kiratool /usr/local/bin
linux # chmod 755 /usr/bin/local/kiratool
```

3. Load the **sg kernel module** (required to run the KiraTool utility):

```
modprobe sg
```

4. Start the KiraTool utility by invoking the executable file.
   The following commands and options are available:

Figure 2-4. KiraTool Commands and Options - Linux

Chapter 3. Managing Power

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

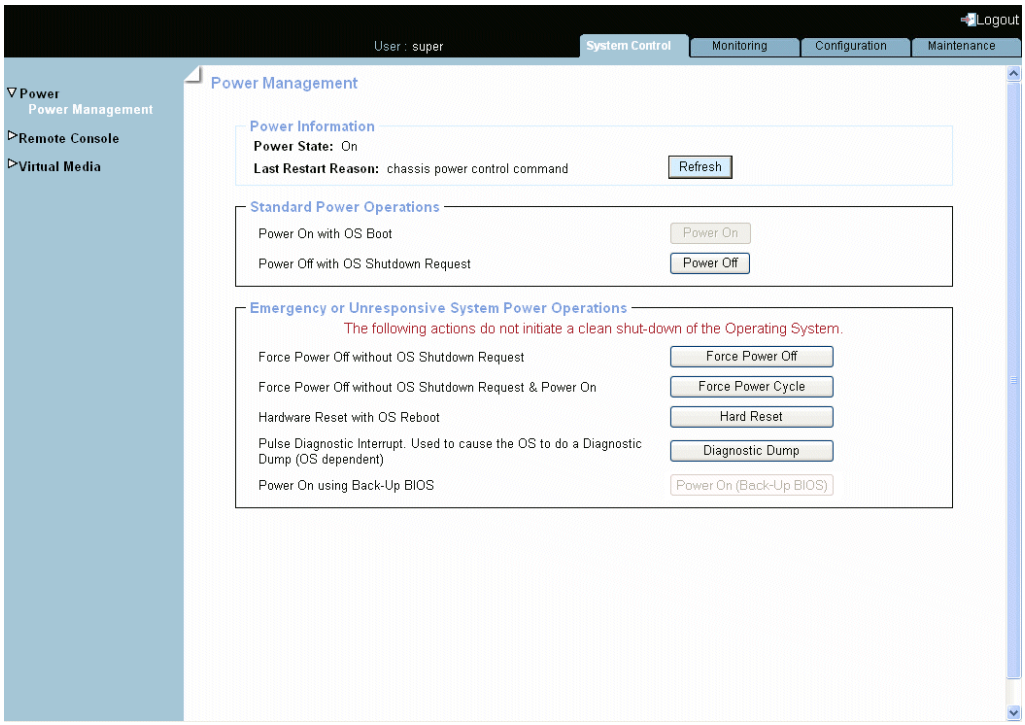
3.1. Power Management Features Overview

The **Power Management** page allows you to check system power status, perform standard power on/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 3-1 below.

Procedure

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



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	
Power State	2 possible values: • On • Off
Last Restart Reason	Several possible values explaining which action last caused a restart, as detailed in Table 3-1 below.
Refresh button	Allows you to update displayed data.
Standard Power Operations	
Power On button	Accessible only when the system is powered off. Launches the power up sequence. During this sequence, hardware is powered up 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. Note: The Operating System must be configured to accept the power off request.
Emergency or Unresponsive System Power Operations	
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.
Diagnostic Dump button	Triggers a Pulse Diagnostic Interrupt for error debugging and diagnosis. The Operating System dumps the contents of memory to disk and the system is reset.
Power On (Back-Up BIOS) button	Performs a power up sequence using a back-up version of the BIOS. This feature is used to restart the server when BIOS integrity is no longer ensured.

Figure 3-1. Power management features overview

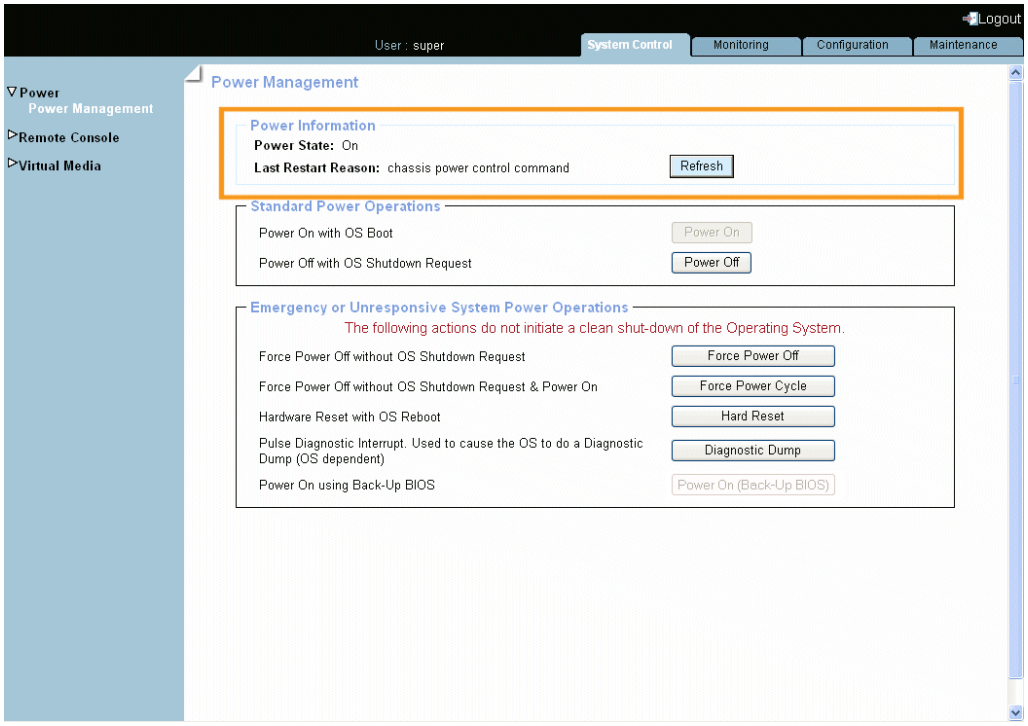
3.2. Checking Power Status

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.



Power Information	
Note: For details on other power management features, see Figure 3-1, on page 3-3.	
Power State	2 possible values: • On • Off
Last Restart Reason	Several possible values explaining which action last caused a restart, as detailed in Table 3-1 below.
Refresh button	Allows you to update displayed data.

Figure 3-2. Checking power status

The following table details the values that may potentially appear in the **Last Restart Reason** 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 push-button.
Power-up via push-button	The server was restarted with the server push-button.
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 3-1. Power information - potential last restart reasons

3.3. Powering On the Server from the Console

The server can be powered on from the Power Management page Standard Power 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.**

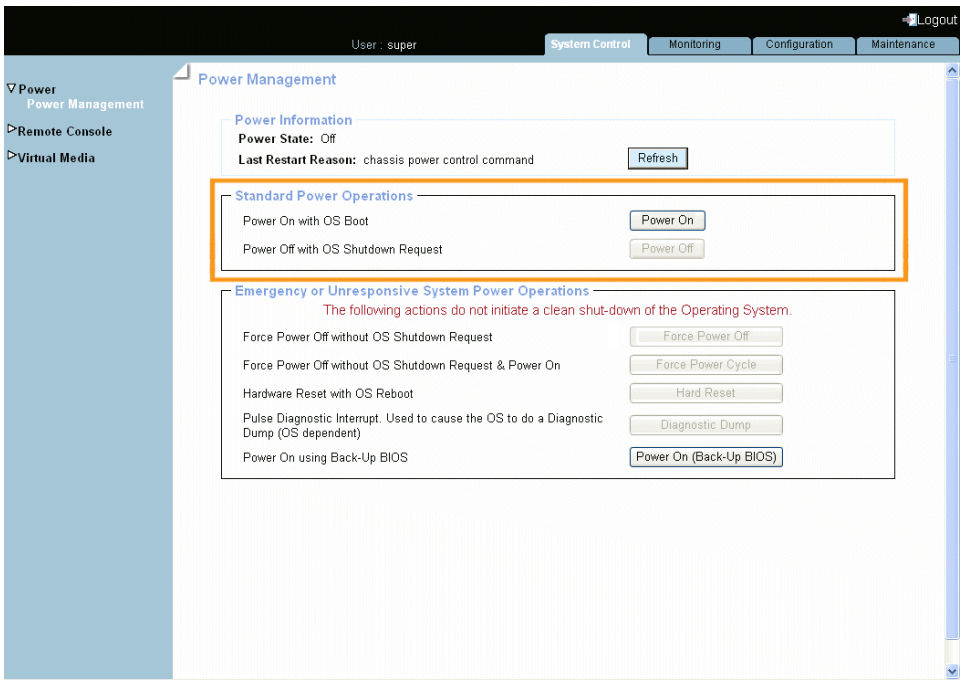
Prerequisites

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.



Standard Power Operations	
Note: For details on other power management features, see Figure 3-1, on page 3-3.	
Power On button	Launches the power up sequence. During this sequence, hardware is powered up 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 3-3. Powering on the server from the console

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 Launching the Remote System Console, on page 4-10.

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

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.

3.4. Powering Off the Server from the Console

The server can be powered off from the Power Management page Standard Power 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.**

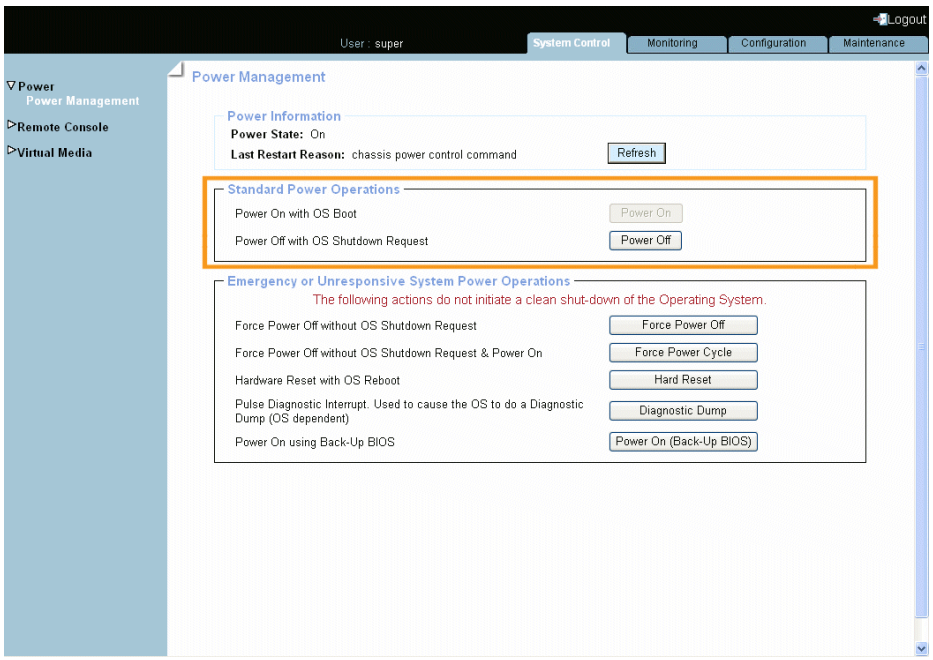
Prerequisites

You have Power Control permission

The Power Off button is enabled

Procedure

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



Standard Power Operations Box	
Note: For details on other power management features, see Figure 3-1, on page 3-3.	
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. Note: The Operating System must be configured to accept the power off request.

Figure 3-4. Powering off the server from the console

2. From the **Standard 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 Launching the Remote System Console, on page 4-10.

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

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 off sequence has not completed.
- The system is frozen.
- The system is not set up to accept the power off sequence.

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**.

3.5. 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 buttons may not be enabled. You can update power status by using the Refresh button.**

Prerequisites

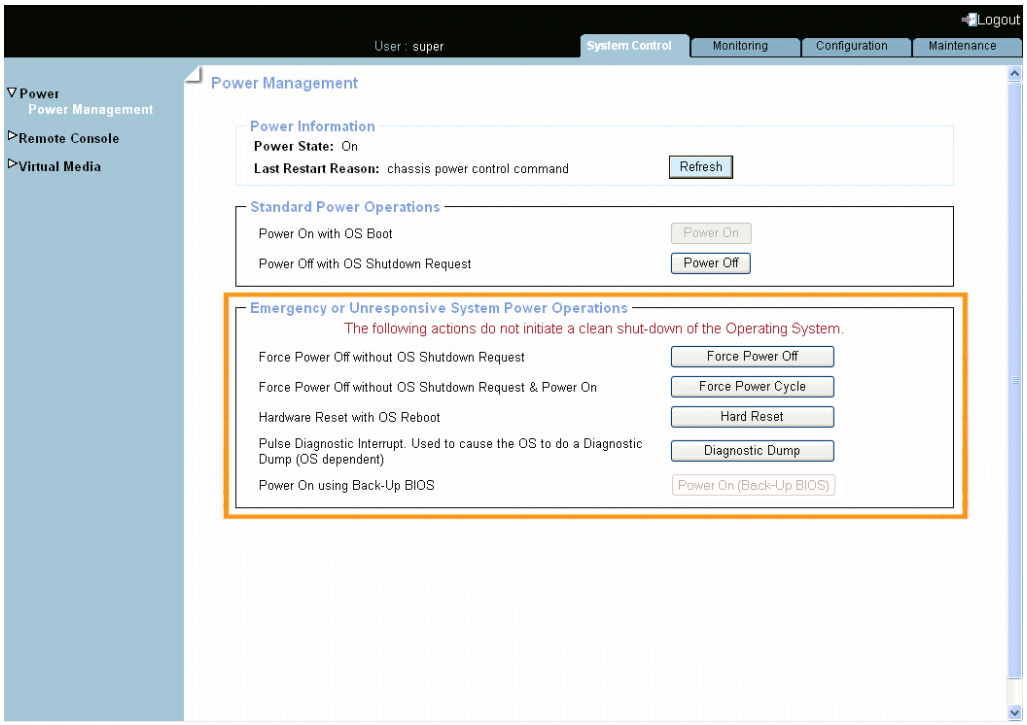
You have Power Control permission

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 respond 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.



Emergency or Unresponsive System Power Operations	
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 3-1, on page 3-3.	
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.
Diagnostic Dump button	Triggers a Pulse Diagnostic Interrupt for error debugging and diagnosis. The Operating System dumps the contents of memory to disk and the system is reset.
Power On (Back-Up BIOS) button	Performs a power up sequence using a back-up version of the BIOS. This feature is used to restart the server when BIOS integrity is no longer ensured.

Figure 3-5. Emergency Power Off

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.

Chapter 4. Using the Remote System Console

This chapter explains how to set up and use the remote system console. It includes the following topics:

4.1. 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.

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

Notes For everyday use, end users will 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).

The Remote System Console can be configured to suit your needs from the Hardware Console, as explained in the following sections.

Note Writing data to a virtual CD/DVD media is NOT supported.

Prerequisites

The Remote System Console is a Java Applet that establishes a TCP connection to the system's embedded management controller (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.

4.1.1. Configuring User Specific Settings

The **Remote Console Settings** page allows you to configure certain 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 Remote Console Settings: you are using the **super** user account

Transmission Encoding: you have the **RC Settings (Encoding)** permission

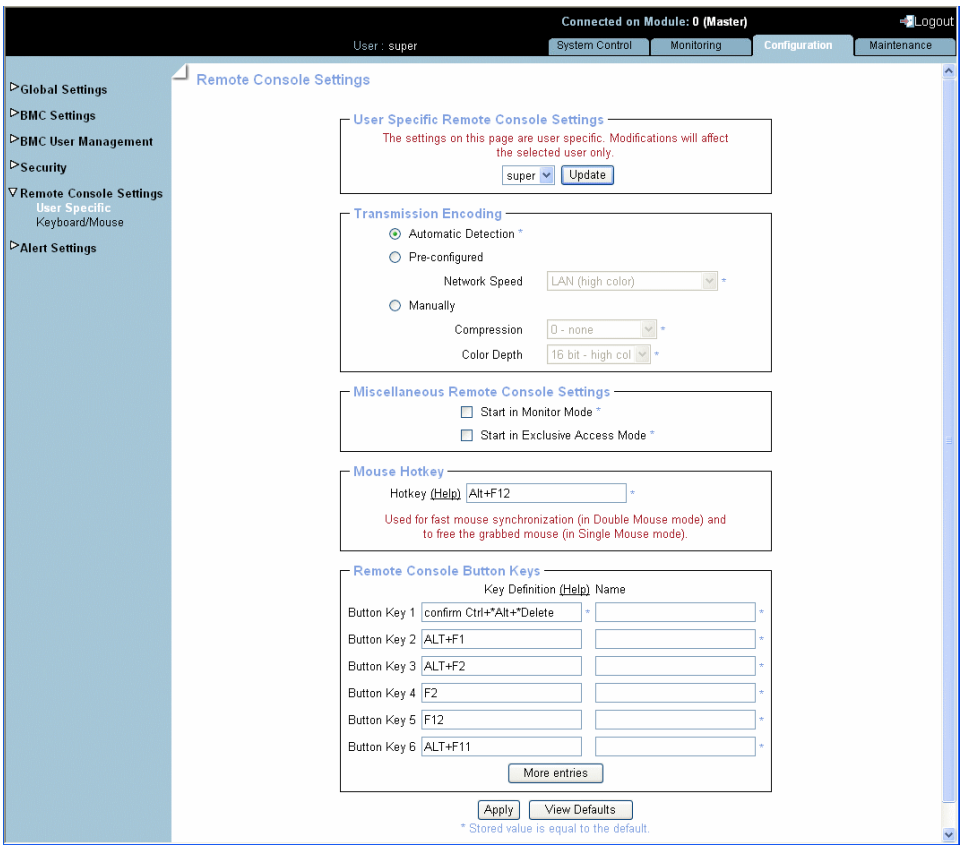
Exclusive Access: you have the **RC Settings (Exclusive Access)** permission

Monitor Mode: you have the **RC Settings (Monitor Mode)** permission

Mouse Hotkey and Remote Console Button keys: 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.



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.	
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 Color 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.
Start in Exclusive Access Mode	Select this option to start the Remote System Console with the Exclusive Access option enabled.
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 Configuring the Keyboard and Mouse, on page 4-6.

Remote Console Button Keys	
This box allows you to define up to 32 key combinations that can be sent to the remote server. By default, the confirm Control+Alt+Delete key combination is defined for Button Key 1, where confirm means that a confirmation dialog will request the user to confirm this action before the key combination is sent to the remote server.	
More Entries	To add more entries, select this button and complete the Key Definition as explained in the associated Help topic.
Key Definition	Key combination to be sent to the remote server.
Name	Optional name for easy identification of the action associated with the key combination.
Help	Explains how to define key combinations.
View Defaults button	Allows you to display factory-default values. Click **Apply** to restore factory-default configuration.

Figure 4-1. Remote System Console - User Specific Settings

2. Complete the required fields and click **Apply**.
3. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required.

4.1.2. Configuring the Keyboard and Mouse

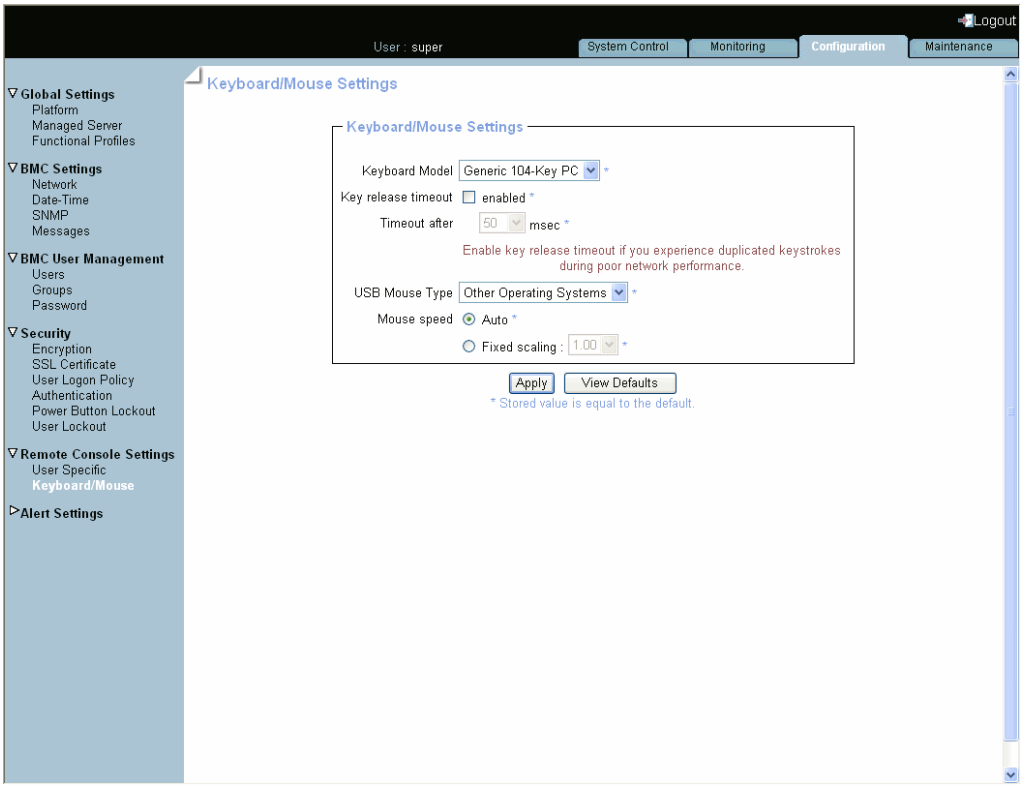
This page allows you to configure Keyboard and Mouse settings to use your local mouse and keyboard to control the remote server through the Remote System Console.

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 Model	Use the drop-down list to select your keyboard type.
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.
USB Mouse Type	Mice transmit their movement using absolute or relative values, depending on the remote operating system.
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 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. Click **Apply** to restore factory-default configuration.

Figure 4-2. Remote System Console - Keyboard and Mouse Settings

2. Change the keyboard and mouse parameters as required and click **Apply**.
3. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required.

4.1.3. Sharing Local Drives

The virtual media drive redirection feature allows you to mount floppy or CD-ROM image files and to share your local drives (floppy drives, CD-ROM, USB keys, hard disks...) with the remote system over a TCP network connection. You can connect image files either using the Hardware Console or through the Remote System Console. The local drives sharing feature is available using the Remote System Console only.

This section describes how to enable/disable the Remote System Console drive redirection feature. You can also enable write support so that the remote system can write data to the shared drives.

Note Writing data to a virtual CD/DVD media is NOT supported.

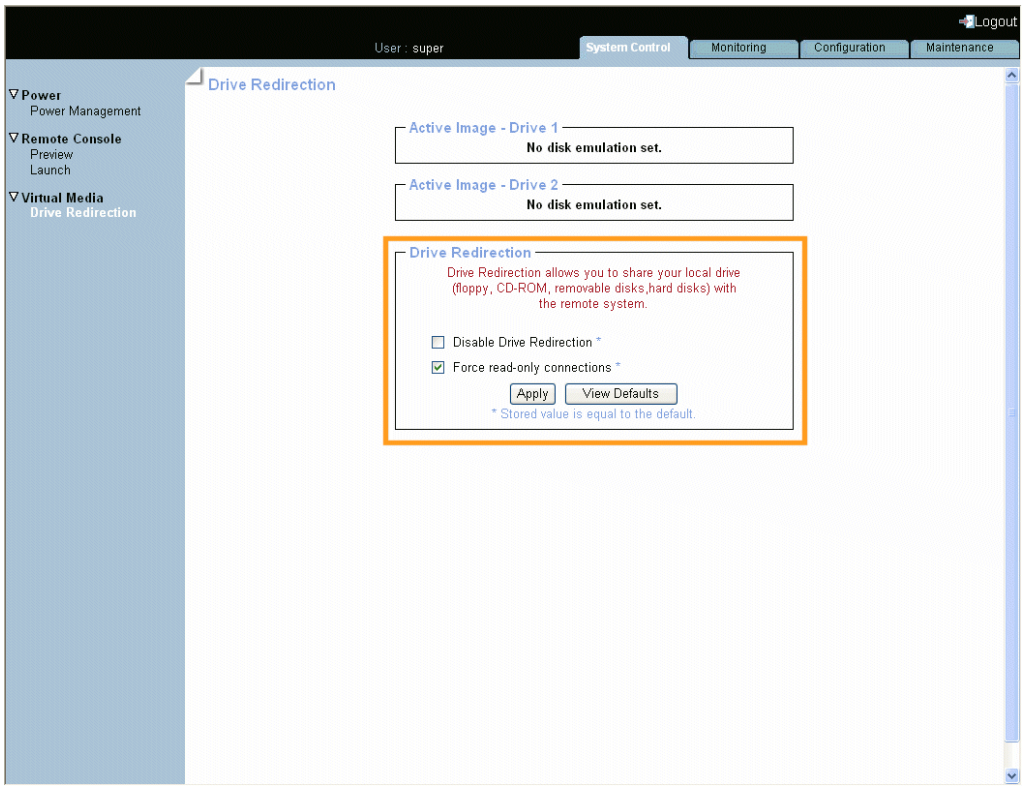
Prerequisites

You have **Virtual Media Upload** permission

Note To enable/disable the Hardware Console drive redirection feature, assign/remove the **Virtual Media Upload** permission.

Procedure

1. From the **System Control** tab, click **Virtual Media > Drive Redirection** to open the **Drive Redirection** page.



Active Image - Drive # Boxes	
Active Image - Drive #	Displays details about the current connected image or drive and provides command buttons, which may differ depending on the connected component. When no image or drive is connected, the message No disk emulation is set is displayed.
Drive Redirection Box	
Disable Drive Redirection	Clear this check box to enable the Remote System Console virtual media drive redirection feature. Select this check box to disable Remote System Console virtual media drive redirection feature.
Force read-only connections	Select this check box to disable write support, shared drives are read-only. Data can be read by the remote system, but not overwritten for enhanced data integrity and system security - Recommended. Clear this check box to enable write support. **WARNING: enable write support with care as you may damage data and file systems.**
View Defaults button	Allows you to display factory-default values.

Figure 4-3. Drive Redirection

2. Select or clear the check boxes depending on your needs and click Apply.

4.2. Launching the Remote System Console

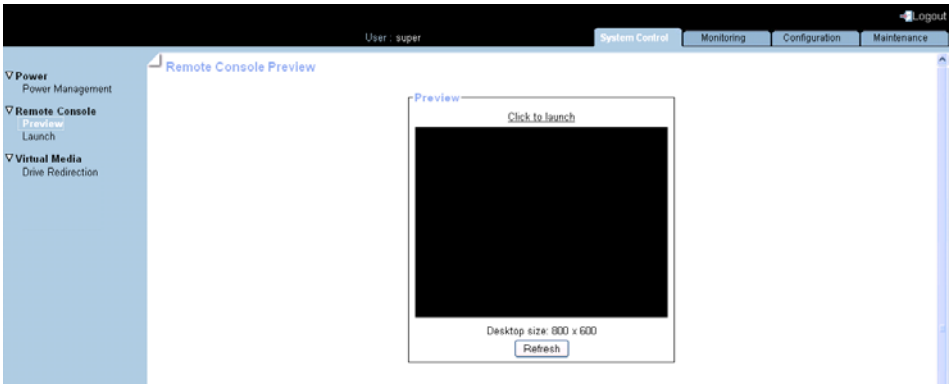
The Remote System Console can be previewed and/or launched, at any time, directly from the Hardware Console.

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.

1. From the **System Control** tab, expand the **Remote Console** menu.
   - If you want to preview the Remote System Console, go to step 2.
   - If you want to preview and then launch the Remote System Console, go to step 3.
   - If you want to launch the Remote System Console directly, go to step 4.
2. To preview the Remote System Console from the Hardware Console, click **Preview** to open the **Remote Console Preview** page.
   The display is not refreshed dynamically. If required, click the **Refresh** button to update the display.



Preview Box	
Click to launch link	Click this link to launch the Remote System Console.
Refresh button	The display is not refreshed dynamically, click this button to refresh the Remote System Console display.
Desktop size information	Current Remote System Console desktop size.

Figure 4-4. Remote Console Preview

3. To preview and then launch the Remote System Console, click **Preview** to open the **Remote Console Preview** page and then click the **Click to launch** link. The Remote System Console opens in a new window.
4. To directly launch the Remote System Console, click **Launch**. The Remote System Console opens in a new window.

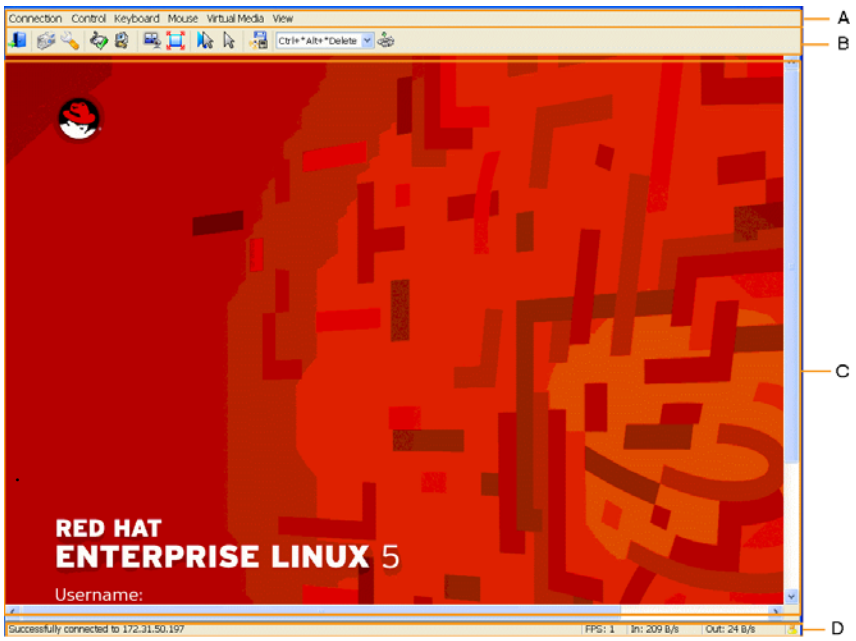
What To Do if an Incident Occurs?

- Network settings are incorrect.
- Java Runtime Environment (JRE) version 1.4 or higher is not installed on your computer.
- Your network is not configured to support the RFB protocol.

Contact your network administrator.

4.2.1. 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.

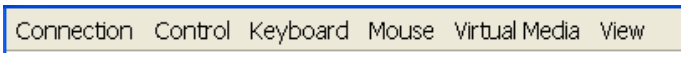


Item	Description
A: Menu bar	The Menu bar gives access to the following menus: • Connection • Control • Keyboard • Mouse • Virtual Media • View For details, see Remote System Console Menus, on page 4-12.
B: Toolbar	The Toolbar gives access to the following controls: • Exit • Screenshot • Properties • Enter/Leave Monitor Only Mode • Enter/Leave Exclusive Access Mode • Scaling • Full Screen Mode • Virtual Media • Select Keyboard Macro • Send Keyboard Macro • Sync Mouse (Reserved) • Single Cursor Mode For details, see Remote System Console Toolbar, on page 4-13.
C: Remote desktop	This area displays the remote system desktop screen.
D: Statusbar	The Statusbar provides connection information.

Figure 4-5. Remote System Console overview

4.2.2. Remote System Console Menus

This section describes the features available to configure and use the Remote System Console **menu** bar.



Menu Name	Menu Items	Description
Connection	Properties	Select to display and define remote video options.
	Connection Info	Select to display remote connection information, such as Device Address, Connection Port, Incoming/Outgoing Speed, ...
	Save Screenshot	Select to save the remote screen.
	Screenshot to Clipboard	Select to copy the remote screen to clipboard.
	Exit	Select to close the remote connection.
Control	Enter Monitor Only Mode	Select to disable remote keyboard and mouse interaction.
	Enter Exclusive Access Mode	Select to force the remote sessions of all other users to close until the exclusive user disables the option or exits.
	Chat Window	Select to display a chat window allowing you to interact with other users logged on to the remote system console.
Keyboard	Keyboard Macros	Select the required keyboard macro from the list displayed.
	Local Keyboard Mapping	Select keyboard language from the list displayed.
Mouse	Sync Mouse	Reserved.
	Single Cursor Mode	Select to disable / enable the local mouse. Press Alt+F12 to leave this mode.
Virtual Media	Virtual Media	Select to display and connect virtual media. See Virtualizing Media, on page 4-14 for details.
View	Scaling	Select to display and define remote window scaling type and quality options.
	Full Screen Mode	Select to display the remote console in Full Screen Mode. Press Ctrl+Alt+F to leave this mode.
	Show Toolbar	Select to show the remote console toolbar. Deselect to hide the remote system console toolbar.
	Show Statusbar	Select to show the remote console statusbar. Deselect to hide the remote console statusbar.

Figure 4-6. Remote System Console menus

Important **If you experience a problem with your keyboard, click Keyboard > Local Keyboard Mapping. Select any other keyboard language and then reselect the required keyboard language. The problem should be resolved.**

4.2.3. Remote System Console Toolbar

This section describes the features available from the Remote System Console Toolbar.

Button Icon	Button Name	Description
	Exit	Select to close the remote connection.
	Screenshot to Clipboard	Select to copy the remote screen to clipboard.
	Properties	Select to display and define remote video options.
	Enter Monitor Only Mode	Select to disable remote keyboard and mouse interaction. A red cross appears. Select again to cancel.
	Enter Exclusive Access Mode	Select to force the remote sessions of all other users to close until the exclusive user disables the option or exits. A red cross appears. Select again to cancel.
	Scaling	Select to display and define remote window scaling type and quality options.
	Full Screen Mode	Select to display the remote console in Full Screen Mode. Press Ctrl+Alt+F to leave this mode.
	Virtual Media	Select to display and connect virtual media. See Virtualizing Media, on page 4-14 for details.
Ctrl+*Alt+*Delete	Keyboard Macros	Select the required keyboard macro from the list displayed.
	Send Keyboard Macro	Send the selected keyboard macro.
	Sync Mouse	Reserved.
	Single Cursor Mode	Select to disable / enable the local mouse. Press Alt+F12 to leave this mode.

Figure 4-7. Remote System Console toolbar

4.3. Virtualizing Media

Using the Virtual Media 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.

This section guides you through the following procedures:

- Virtualizing a Local Drive, on page 4-15
- Virtualizing an Image File, on page 4-16
- Virtualizing a Local Folder, on page 4-17

4.3.1. Virtualizing a Local Drive

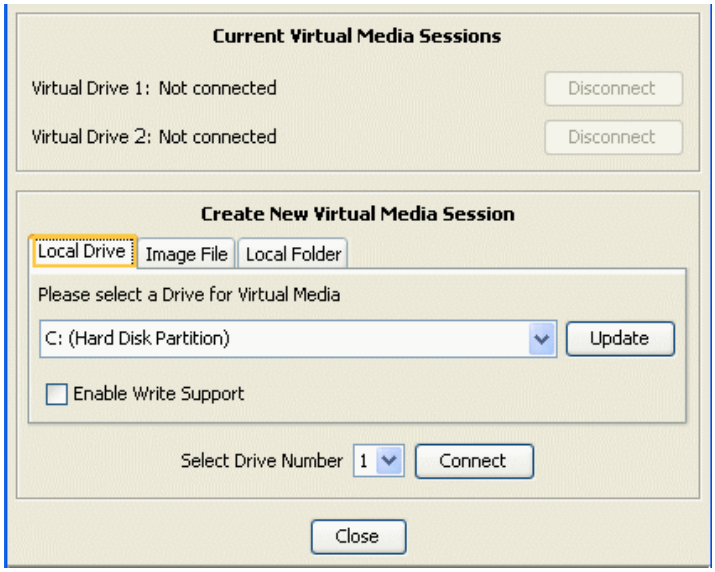
You can select any of the local drives and make them accessible to the remote server.

Prerequisites

Drive redirection is enabled from the Hardware Console

Procedure

1. From the Remote System Console menu bar, select **Virtual Media**, or select the **Virtual Media** button ( ) from the toolbar. The **Virtual Media** dialog opens, displaying **Current Virtual Media Sessions** status and **Local Drive** tab options in the **Create New Virtual Media Session** field.



Current Virtual Media Sessions	
Virtual Drive X	Two possible values: Connected / Not connected
Disconnect button	Press this button to disconnect a drive. When no drive is connected, this button is grayed out.
Create New Virtual Media Session - Local Drive Tab	
Select a Drive for Virtual Media list	Press the scroll arrow to select the required local drive.
Enable Write Support checkbox	Select this checkbox to allow data to be written to the local drive.
Select Drive Number list	Press the scroll arrow to select the required drive mount number.
Update button	Press this button to update the local drive list.
Connect button	Press the Connect button to mount the drive. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled.

Figure 4-8. Virtual Media - Local Drive

2. Configure the local drive as explained above and click **Connect**. The local drive is now mounted and can be used by the remote server to read and/or write (if enabled) data.

4.3.2. Virtualizing an Image File

You can emulate up to two image files as USB devices and make them accessible to the remote server.

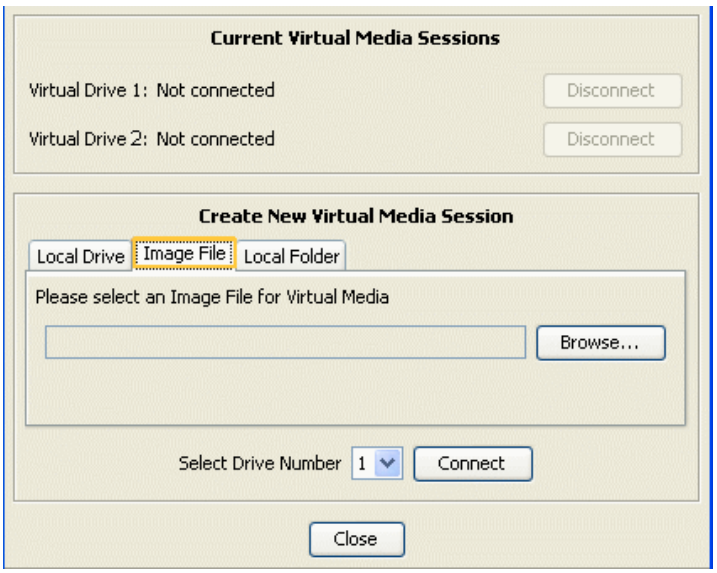
Prerequisites

Drive redirection is enabled from the Hardware Console

The image file has been created

Procedure

1. From the Remote System Console menu bar, select **Virtual Media**, or select the **Virtual Media** button ( ) from the toolbar. The **Virtual Media** dialog opens, displaying **Current Virtual Media Sessions** status and **Local Drive** tab options in the **Create New Virtual Media Session** field.
2. Select the **Image File** tab.



Current Virtual Media Sessions	
Virtual Drive X	Two possible values: Connected / Not connected
Disconnect button	Press this button to disconnect a drive. When no drive is connected, this button is grayed out.
Create New Virtual Media Session - Image File Tab	
Select an Image File for Virtual Media list	Press the Browse button to select the required image file.
Select Drive Number list	Press the scroll arrow to select the required drive mount number.
Connect button	Press the Connect button to mount the image file. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled.

Figure 4-9. Virtual Media - Image File

3. Mount the image file as explained above and click **Connect**. The image file is now mounted and can be used by the remote server.

4.3.3. Virtualizing a Local Folder

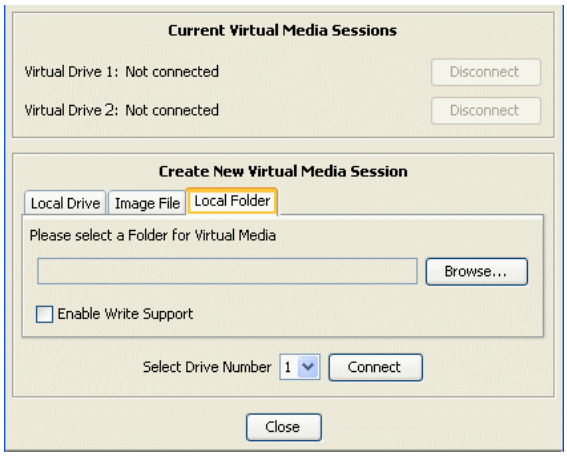
You can select any of the local folders on your local computer and make them accessible to the remote server.

Prerequisites

Drive redirection is enabled from the Hardware Console

Procedure

1. From the Remote System Console menu bar, select **Virtual Media**, or select the **Virtual Media** button ( ) from the toolbar. The **Virtual Media** dialog opens, displaying **Current Virtual Media Sessions** status and **Local Drive** tab options in the **Create New Virtual Media Session** field.
2. Select the **Local Folder** tab.



Current Virtual Media Sessions	
Virtual Drive X	Two possible values: Connected / Not connected
Disconnect button	Press this button to disconnect a drive. When no drive is connected, this button is grayed out.
Create New Virtual Media Session - Local Folder Tab	
Select a Folder for Virtual Media list	Press the Browse button to select the required image file.
Enable Write Support checkbox	Select this checkbox to allow data to be written to the local folder.
Select Drive Number list	Press the scroll arrow to select the required drive mount number.
Connect button	Press the Connect button to mount the drive. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled.

Figure 4-10. Virtual Media - Local Folder

3. Configure the local folder as explained above and click **Connect**. The local folder is now mounted and can be used by the remote server to read and/or write (if enabled) data.

4.4. Stopping the Remote System Console

The Remote System Console can be stopped at any time by selecting **Connection > Exit** from the menu bar, or selecting the **Exit** button () from the toolbar.

Chapter 5. Monitoring the Server

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

Important **Information to help you troubleshoot the server in the event of incorrect operation is given in Troubleshooting the server on page A-1.**

5.1. 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 6, Configuring the Server Management Controller, and are listed below:

- Configuring the Board and Security Message Log, on page 6-12
- Configuring Alert Settings, on page 6-47

5.2. Checking Monitoring Sensors

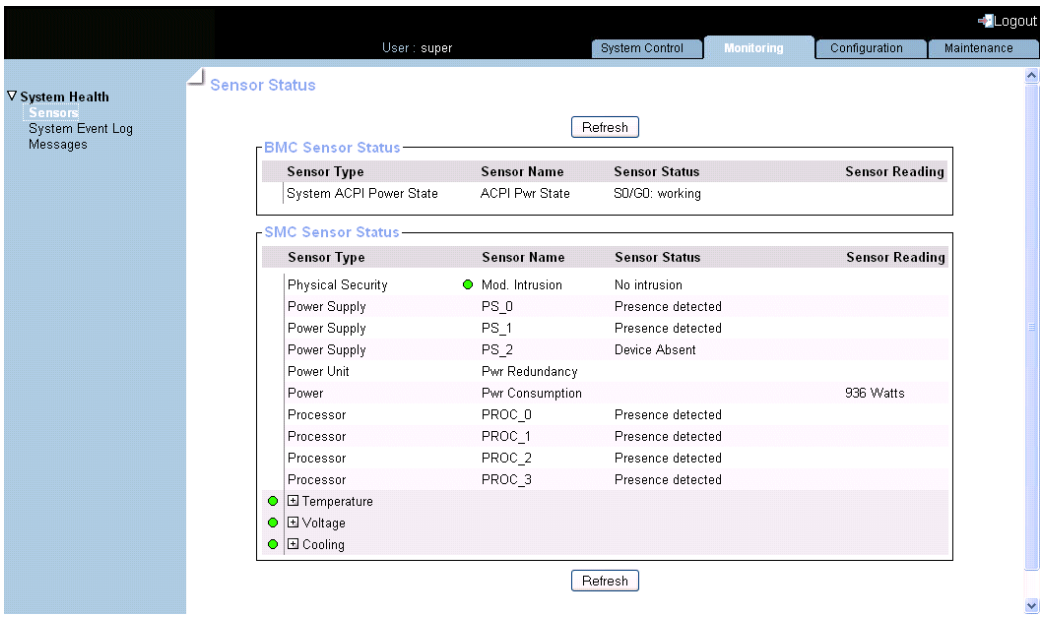
The system is equipped with various sensors that monitor the status of hardware components, such as:

- Power status
- Presence, absence, redundancy of components
- Voltage values
- Temperature values
- Fan speed
- Physical intrusion
- etc.

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.

   If a component icon is not green, see Appendix A Troubleshooting the Server for more information.



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 top and bottom of the page, to update the display.
Status Icons Description	
The status icons to the left of certain sensors indicate the status of the monitored component with regard to nominal threshold values. NOTE: The status of Temperature, Voltage and Cooling sensors is monitored both individually and globally. By default, the global status of Temperature or Voltage or Cooling sensors is reflected by the icon to their left. To view the status of individual sensors, select the corresponding Expand button. If the status of an individual sensor becomes critical (RED), the corresponding global sensor status icon will turn RED.	
GREEN	NORMAL Operation correct. No problem has been detected.
RED	CRITICAL A problem has been detected. Immediate preventive or corrective action is required. If a component icon is not green, see Appendix A Troubleshooting the Server for more information.
GRAY	Sensor not available.

Figure 5-1. Sensor Status

Values and readings are detailed in Predefined Alert Filters Description, on page A-2.

5.3. Checking 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 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.

Note **The iCare Console automatically collects System Event Logs and can be configured to automatically empty the System Event Log. Please refer to the *iCare Console User's Guide* for details.**

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.

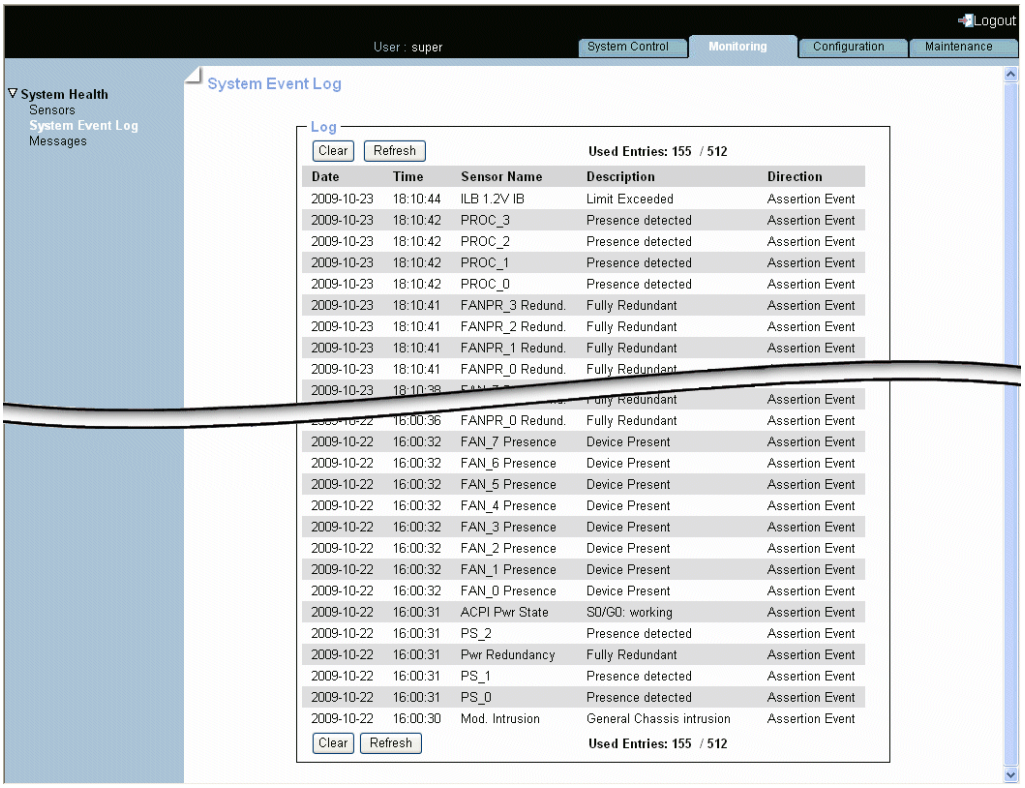


Figure 5-2. System Event Log

- 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 and associated operations to recover are explained in Appendix A - Troubleshooting the Server.

5.4. Checking the Board and Security Messages Log

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 **Log View** permission

Procedure

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

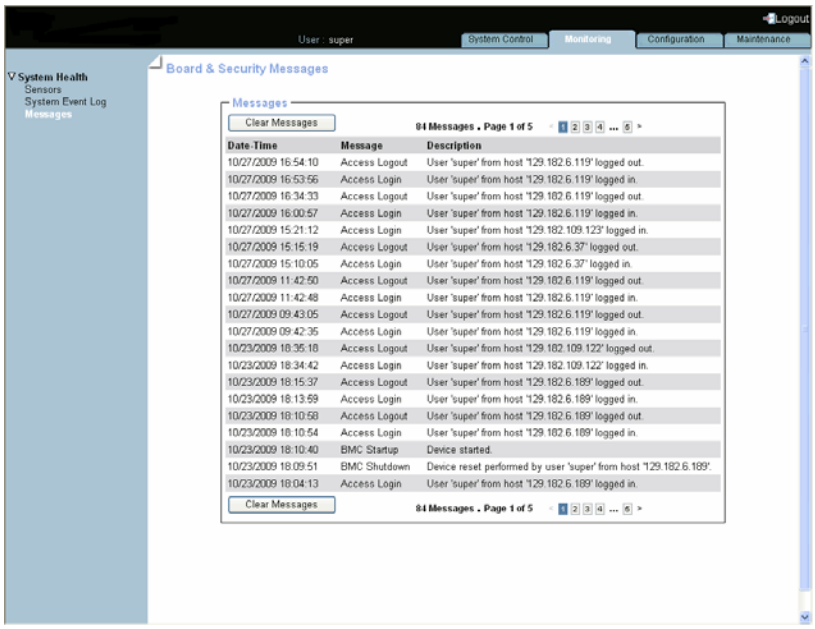


Figure 5-3. Board & Security Messages

2. Browse messages, as required, using the navigation arrows or page number 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.**

5.5. Downloading and Deleting BIOS Log

The BIOS logs are sent to the EMM. If your server is not monitored by the iCare Console, you can obtain and delete these BIOS logs with the Hardware Console.

Note You are adviced to monitor your servers with iCare Console. The BIOS logs are then collected in the iCare Console database. You can read, delete and restore the database with the iCare Console interface. The BIOS logs are managed by the iCare Console and suppressed from the EMM.

WARNING
Don't use this Hardware Console feature to manage BIOS Logs if your server is monitored by iCare Console.

You can query the BIOS logs to help your hardware failure analyze or to perform preventive maintenance.

In case of UNCORRECTABLE ERRORS or FATAL ERRORS detected by the processor of the resource, the BIOS logs all the registers containing CORRECTABLE ERROR, UNCORRECTABLE ERROR, or FATAL ERRORS.

Note Over 15 UNCORRECTABLE ERRORS and 6 FATAL ERRORS collected by the EMM logs are lost.

Prerequisites

You have **Log View** permission

Procedure

1. From the **Maintenance** tab, click **Maintenance Operations > BIOS Logs** to open the **BIOS Logs** page.

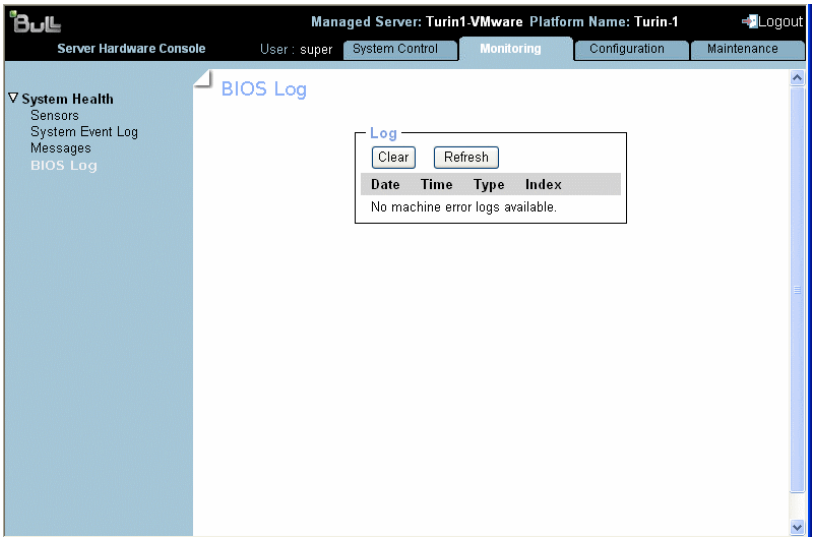


Figure 5-4. BIOS Logs

Chapter 6. Configuring the Server Management Controller

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

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

6.1. Configuring Platform Identification Settings

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Each server drawer must be given a **unique** Platform ID and Platform Name for easy and reliable identification by management and maintenance software such as Bull System Manager (BSM) and iCare.

Prerequisites

You have Network Settings permission

Procedure

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

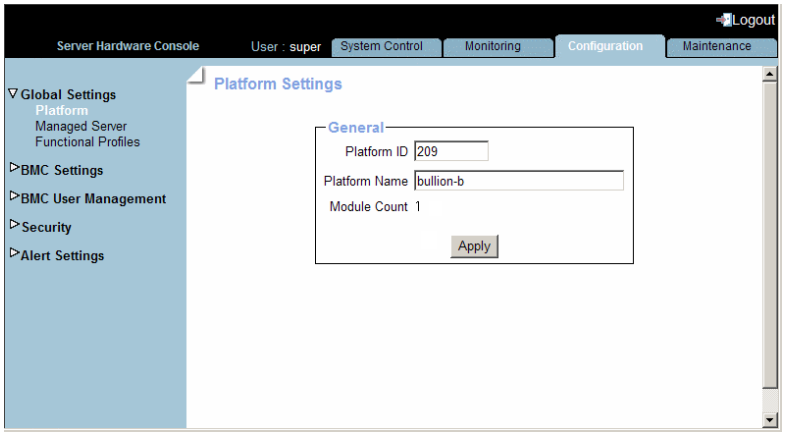


Figure 6-1. Platform Settings

2. Complete the fields and click Apply.

Note The Module Count field is read-only.

6.2. Configuring the Managed Server Name

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Prerequisites

You have Network Settings permission

Procedure

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

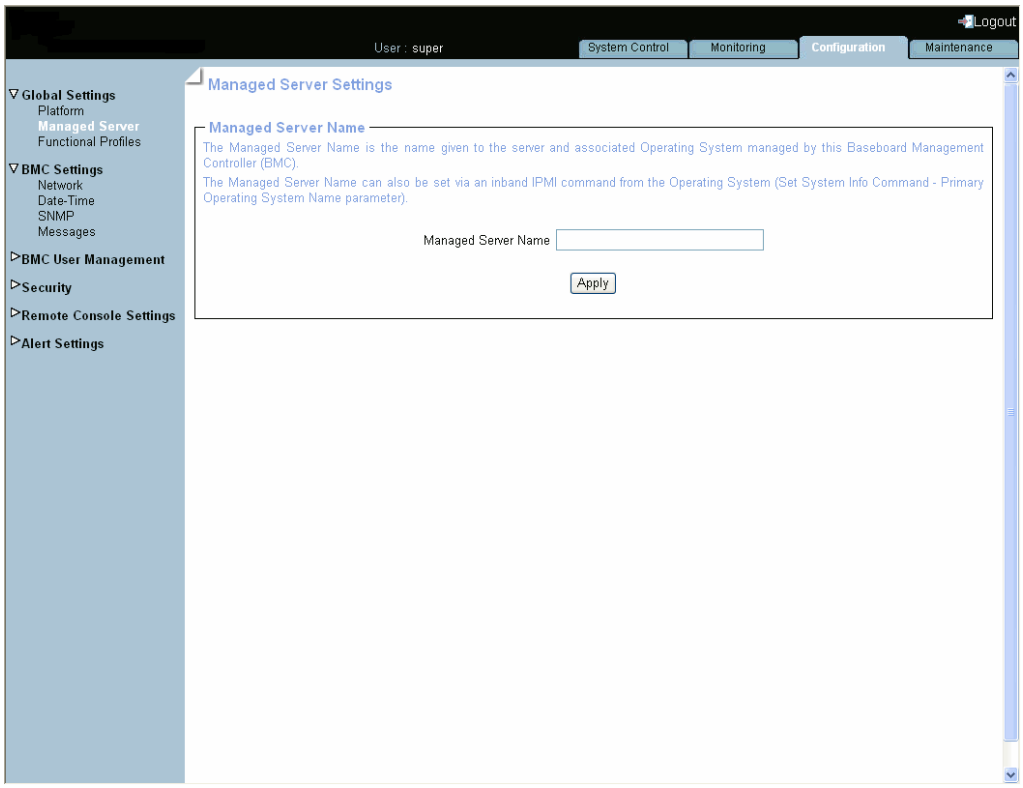


Figure 6-2. Managed Server Settings

2. Complete the field and click Apply.

6.3. Modifying Functional Profile Settings

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

A Functional Profile is a set of parameters defining the Power Restore Policy and the use of Full Fan Speed at system power-on. You can define up to two Functional Profiles (0 or 1) for your system and select one or the other at power-on.

Note When the system power state is ON, the current Functional Profile is displayed, but cannot be modified.

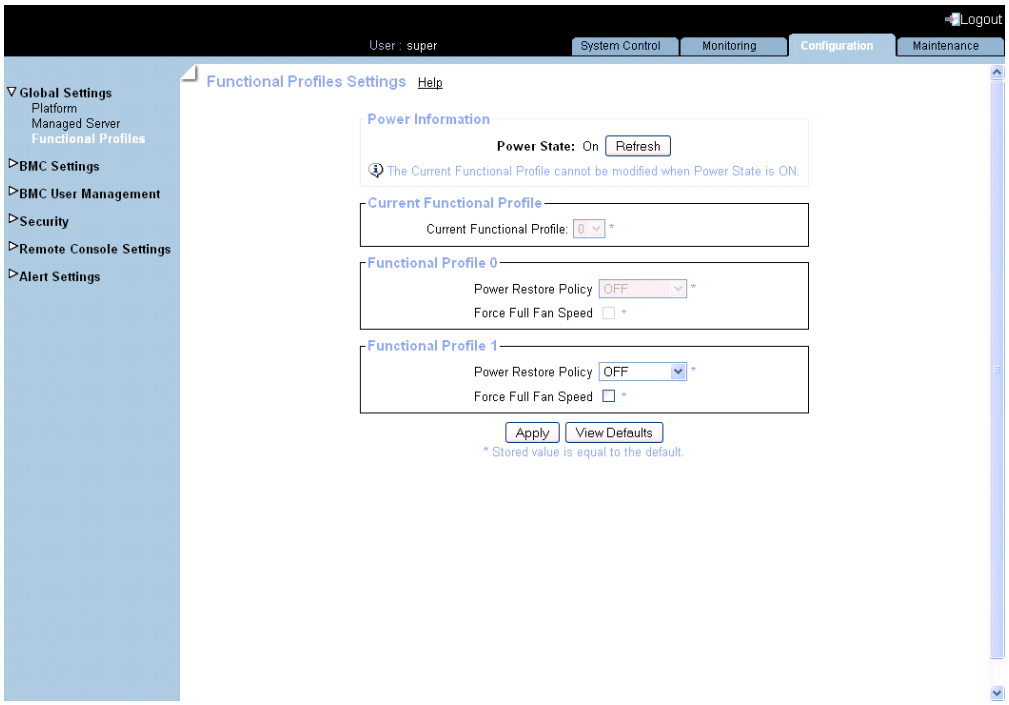
Prerequisites

System is powered OFF

You have Network Settings permission

Procedure

1. From the Configuration tab, click Global Settings > Functional Profiles to open the Functional Profiles Settings page.



Power Information Box	
Power State	2 possible values: • On • Off
Refresh button	Allows you to update displayed data.
Current Functional Profile Box	
Current Functional Profile drop-down list	Use the drop-down list to define a Functional Profile or to select the Functional Profile you want to apply at the next power-on. Note: when the system power state is ON, the Current Functional Profile is displayed, but cannot be modified.
Functional Profile <x> Box	
Power Restore Policy drop-down list	Use the drop-down list to select the power restore policy you want to apply when AC power returns after a system AC power loss: • Select OFF if you want the system to remain off when AC power returns. • Select RESTORE if you want the system to return to the same power state as before the AC power loss. • Select ON if you want the system to power on when AC power returns.
Force Full Fan Speed check box	Select the check box to force full fan speed. At next power-on, the fan speed will always be set at maximum speed, without any regulation by firmware.
View Defaults button	Allows you to display factory-default values. Click Apply to restore factory-default configuration.

Figure 6-3. Functional Profiles Settings

2. Complete the page to comply with your requirements and click Apply.

6.4. Configuring Network Settings for Remote Access

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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

Prerequisites

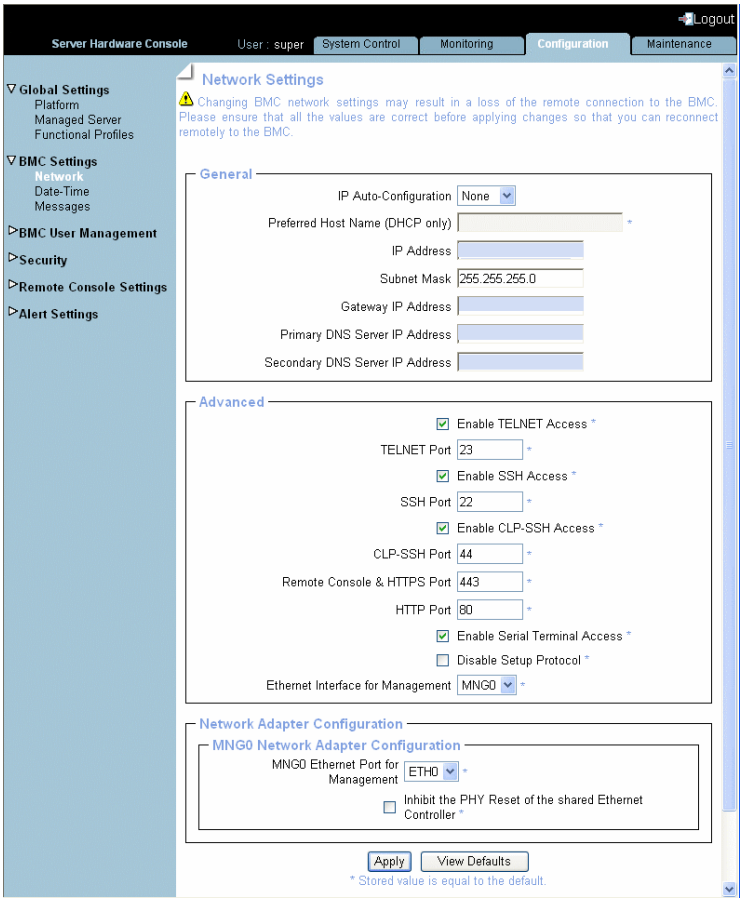
You have Network Settings permission

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.



General 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	
Enable TELNET Access	Select this option to allow connection using a Telnet client. You need SSH/Telnet Access permission.
TELNET Port	The Telnet port number (Factory-default: 23).
Enable SSH Access	Select this option to allow connection using an SSH client. You need SSH/Telnet Access permission.
SSH Port	The Secure Shell (SSH) port number (Factory-default: 22).
Enable CLP-SSH Access	Select this option to allow connection from an SSH Command Line Prompt (CLP). You need SSH/Telnet Access permission.
CLP-SSH Port	The CLP-SSH port number (Factory-default: 44).
Remote Console & HTTPS Port	The port number used for standard HTTPS connectons (Factory-default: 443).
HTTP Port	The port number used for standard HTTP connections (Factory-default: 80).
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 need SSH/Telnet Access permission.
Disable Setup Protocol	Select this option to prevent the *psetup (Windows) tool* and/or *mc-setup (Linux) tool*, used to discover the server on the LAN during initial setup, from re-detecting this server when installing new servers.

Advanced Box	
Ethernet Interface for Management	The Ethernet port number used to connect the embedded management controller to the Enterprise LAN. By default, Ethernet port ETH0/MNG0 is used : both the management and host networks share this connection and the network cable is connected to ETH0/MNG0. Alternatively, you can separate management and host networks by using Ethernet port INTER/MNG1 for the management network and MNG0 for the host network. In this case, select MNG1 and then connect the management network cable to INTER/MNG1 and the host network cable to MNG0.
MNG0 Network Adapter Configuration	
MNG0 Ethernet Port for Management	Select Ethernet port ETH0 or ETH1
Inhibit the PHY Reset of the shared Ethernet Controller	Select this option to prevent the Ethernet Controller from being reset when the server is reset.
MNG1 Network Adapter Configuration	
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. • **100Mbps**: 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. Click **Apply** to restore factory-default configuration.

Note * According to server model and network configuration both **MNGx Network Adapter Configuration Boxes** may not be visible.

Figure 6-4. Network Settings - 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. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

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.

6.5. Modifying Internal Clock Settings

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The Date/Time Settings page allows you to set up the embedded management controller's 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. You will have to reset the date and time in the event of a power cut.

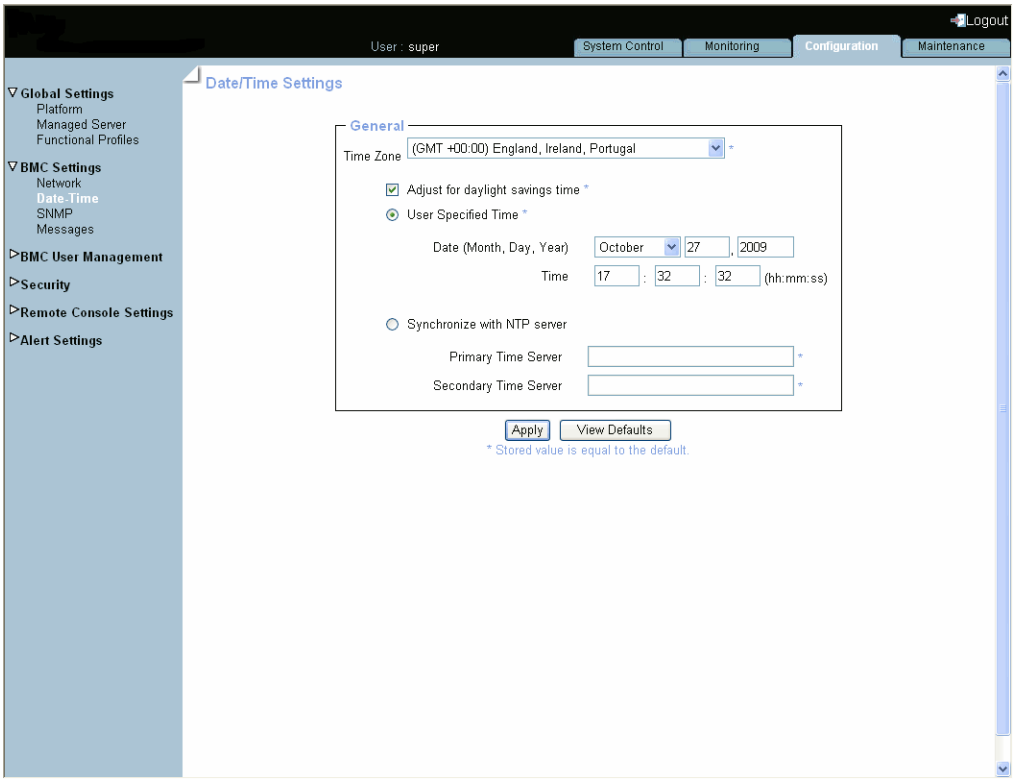
Prerequisites

You have Date/Time Settings permission

If you want to use NTP, you must 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.



General	
Time Zone	Use this drop-down list to set the difference between local and universal time.
Adjust for daylight savings time	Select this option to automatically adjust to local daylight savings time (DST).
User Specified Time	This option allows you to manually set the server internal clock. Enter manually both the date and local time and check that the Time Zone setting is correct.
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 Time Zone drop-down list.
View Defaults button	Allows you to display factory-default values.

Figure 6-5. Date/Time Settings - factory-default values

2. If required, change the **Time Zone** value and select or clear the **Adjust for daylight savings time** check box.
3. Click either **User Specified Time** or **Synchronize with NTP Server**, complete the appropriate fields and click **Apply**.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.6. Configuring the Board and Security Message Log

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

This section describes how to configure the Board and Security Messages log, which records non-IPMI events, such as power-on errors, user authentication, connections, 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

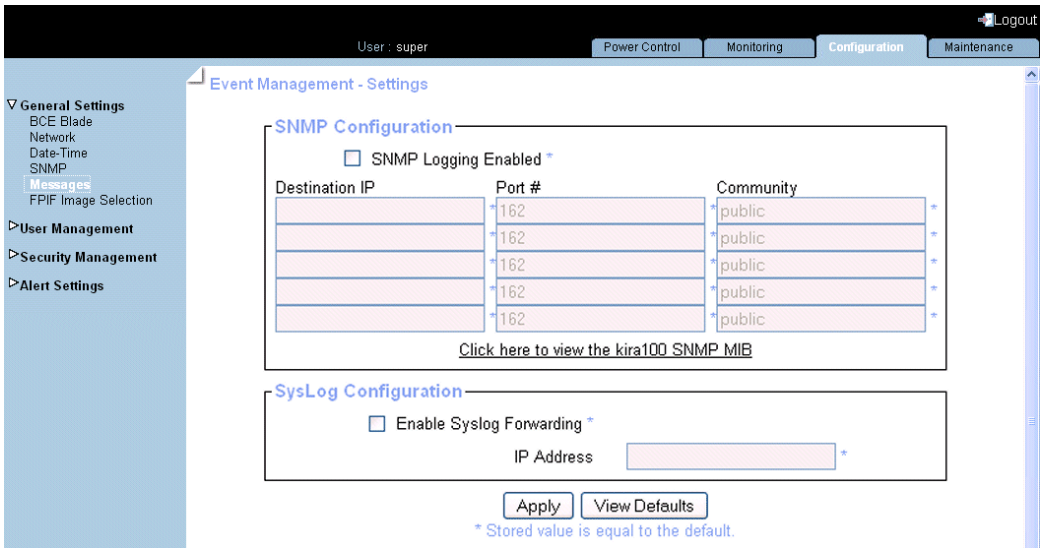
You have Log Settings permission

You have configured your SMTP / SNMP server for messaging

You have configured your Syslog / SNMP server for messaging

Procedure

1. From the Configuration tab, click BMC Settings > Messages to display the Event Management - Settings page:



SNMP Configuration	
SNMP Logging Enabled	When selected, this option allows Board and Security messages to be sent by SNMP trap.
Destination IP	SNMP manager IP address and port number
Port #	
Community	SNMP community name for the SNMP manager (example: public)
Click here to view ... link	This link allows you to view and save, as a .txt file, the system MIB file. This file is required by your SNMP Manager to interpret trap messages.
SysLog Configuration	
Enable Syslog Forwarding	When selected, this option allows Board and Security messages to be sent by the syslog protocol, to centralize the Board and Security logs on a Linux platform.
IP Address	Linux platform IP address.

Figure 6-6. Event Management Settings - factory-default values

2. Complete the fields as required.
3. Click **Apply**.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7. Managing Users

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

6.7.1. Creating a User Account

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.
- **users** 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 **users** group are modifiable.

Important **The system 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

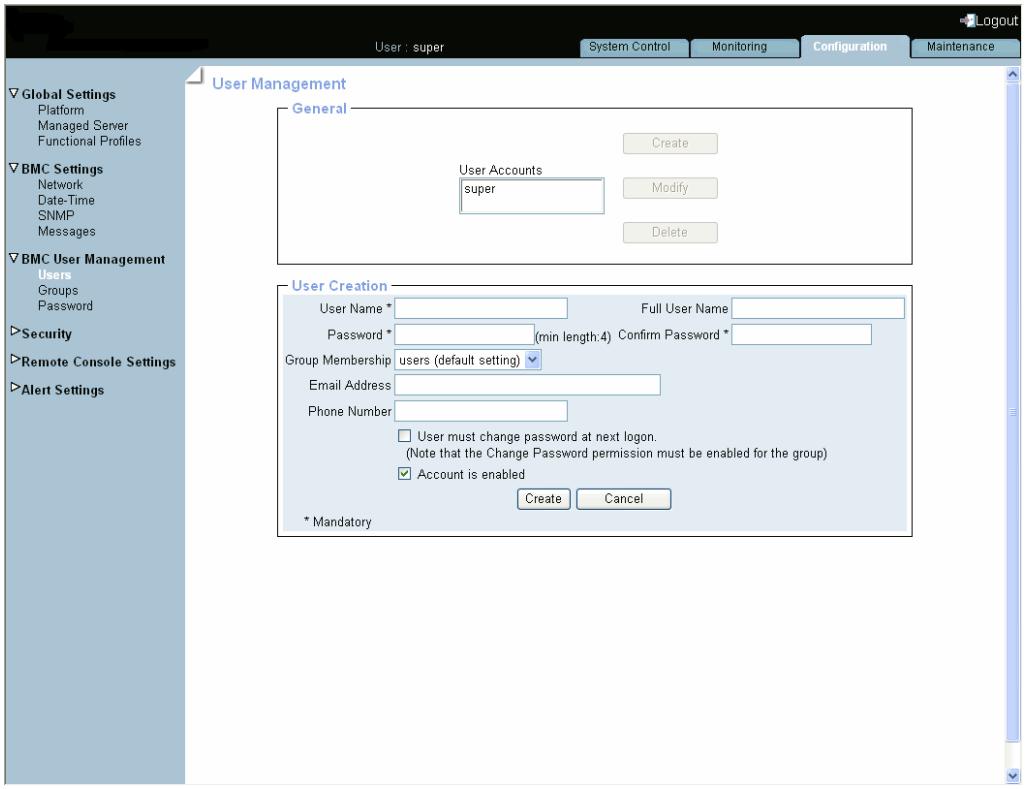
You have User/Group Management permission

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 Creation** dialog.



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.

User Creation	
Email Address	User's email address. Example: john.smith@acme.com.
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 6-7. User Management - User Creation

3. Complete the fields as required.
4. Click **Apply**. The user is created and appears in the **User Accounts** box.
5. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.2. Displaying User Account Details

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

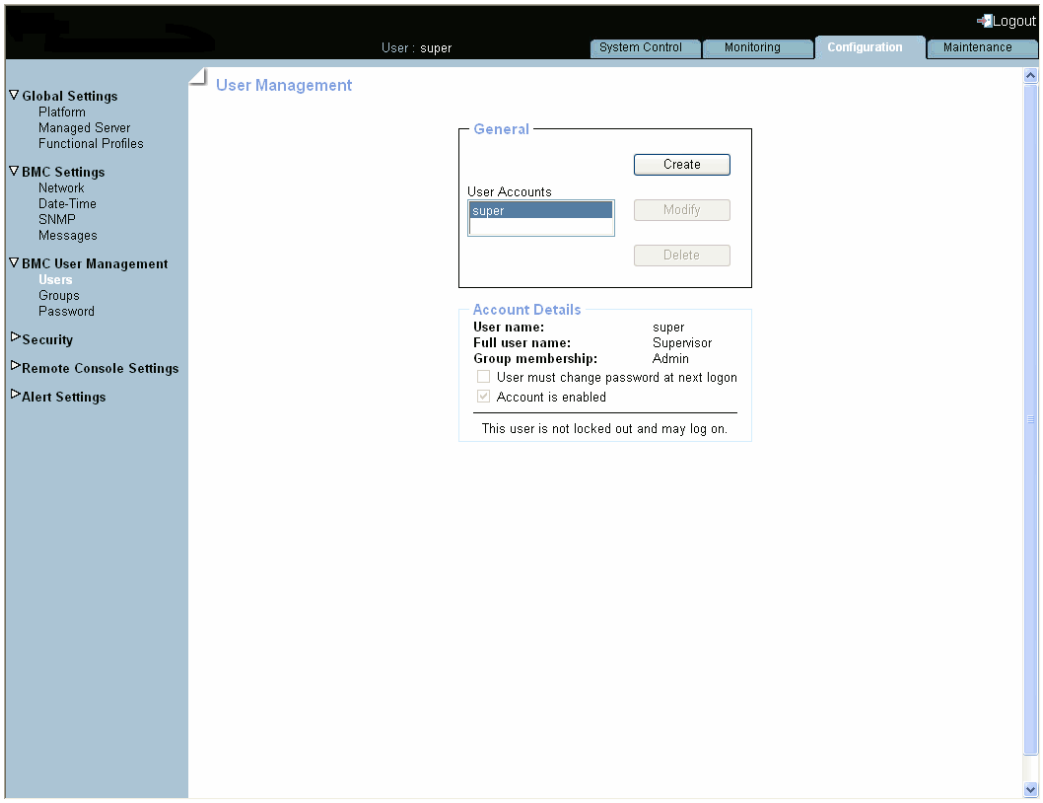
For easy user management, you can display the basic details of any user account at any time. You may want to use this feature, for example, to check user account details after the creation or modification of a user account or to check whether a user is locked out or not.

Prerequisites

You have **User/Group Management** permission

Procedure

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



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.
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 6-8. User Management - Account Details

6.7.3. Modifying a User Account

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You can edit user account information at any time.

6.7.3.1. Updating 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 the Password, on page 6-24.

Prerequisites

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

Procedure

1. From the **Configuration** tab, click **BMC User Management > Users** to display the **User Management** page.

1. From the **Configuration** tab, click **> 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 6-7, on page 6-16.

4. Click **Modify**. User account details are changed.
5. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.3.2. Changing Group

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. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.4. Disabling/Enabling User Accounts

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.5. Forcing User Password Changes

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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

The Group has **Change Password** permission

Procedure

1. Check that **Change Password** permission is enabled for the group to which the user belongs:
   a. From the **Configuration** tab, click **User Management > Groups** to display the **Group Management** page.
   b. Select the group to which the user belongs and click **Permissions** to display the **Group Permissions** page.
   c. Check that **Change Password** permission is enabled for the group. If this is not the case, enable the **Change Password** permission for the group.
2. From the **Configuration** tab, click **User Management > Users** to display the **User Management** page.
3. Select the user account in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
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.

6.7.6. Deleting a User Account

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

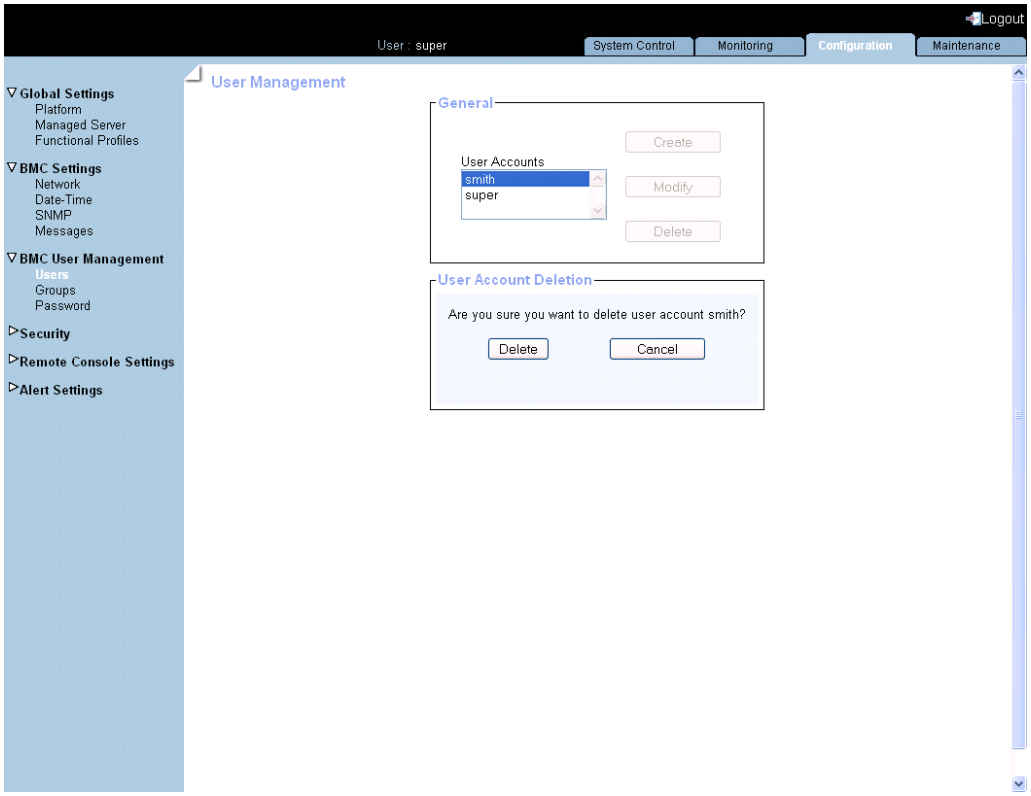


Figure 6-9. User Account Deletion

3. Click **Delete** to confirm. The user is removed from the list and from the associated group.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.7. Manually Unlocking a User Account

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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 **User/Group Management** 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.

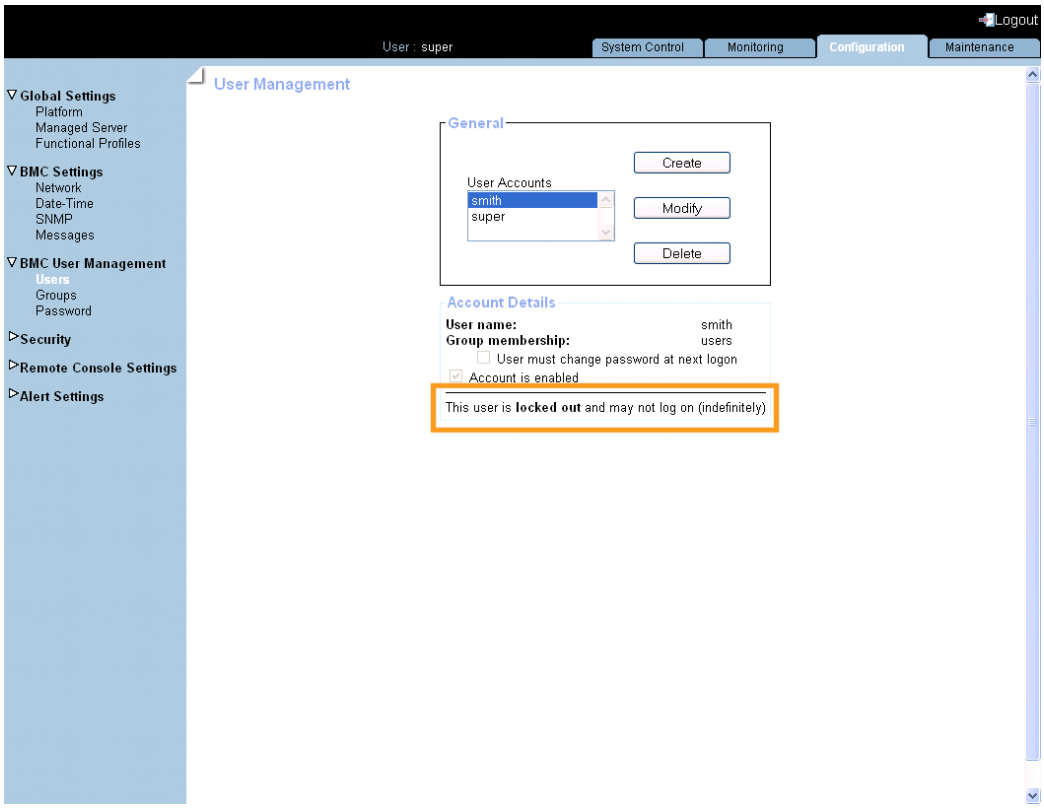
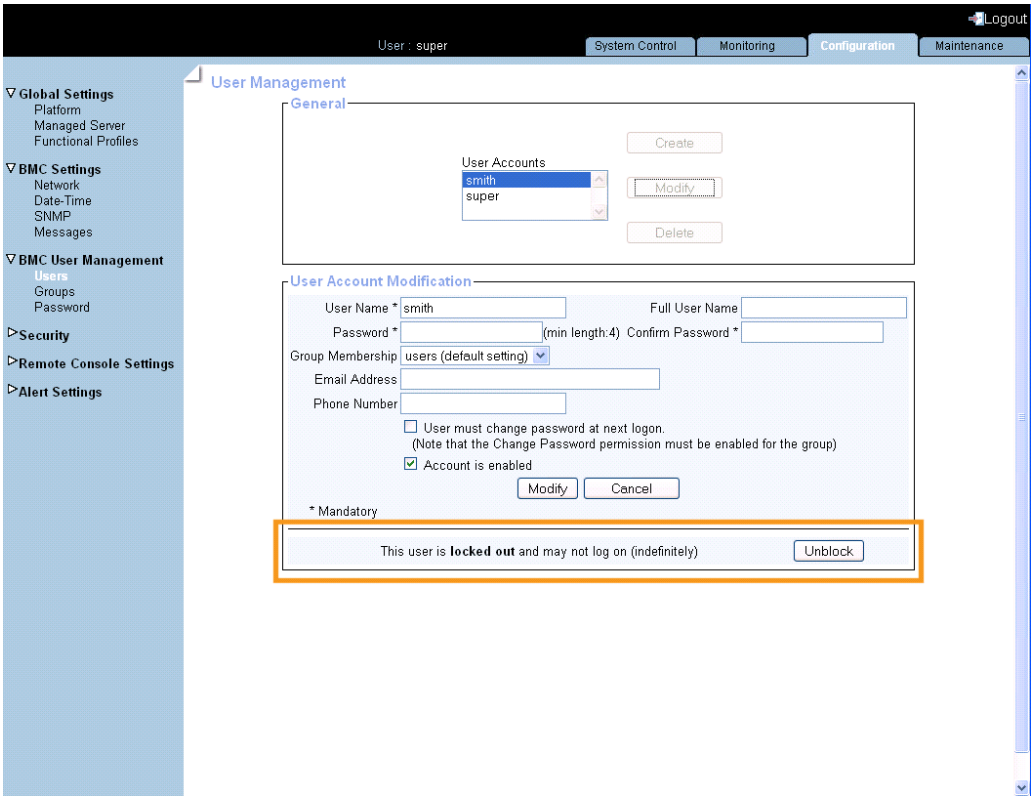


Figure 6-10. User Management - Locked-out user

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



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

6.7.8. Modifying the Password

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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

Prerequisites

You have **Change Password** permission

Procedure

1. From the **Configuration** tab, click **BMC User Management > Password** to display the **Password Management** page.

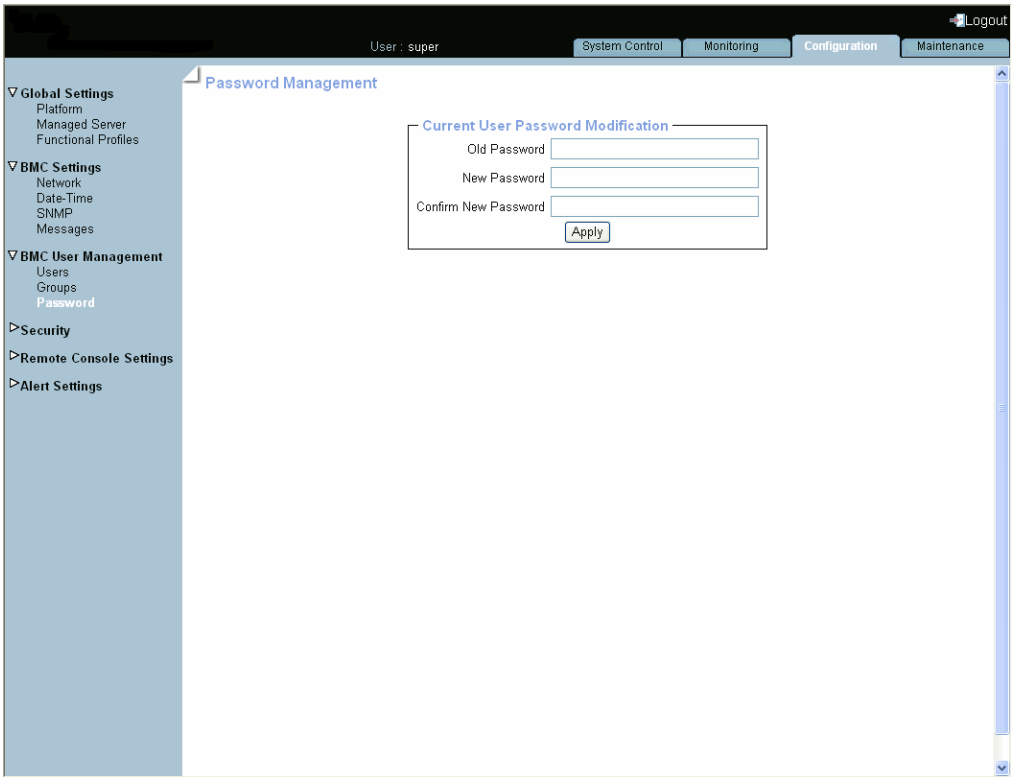


Figure 6-11. Password Management

Important

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

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

6.7.9. Creating a Group

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.
- **Users** group with no permissions and no predefined users.

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

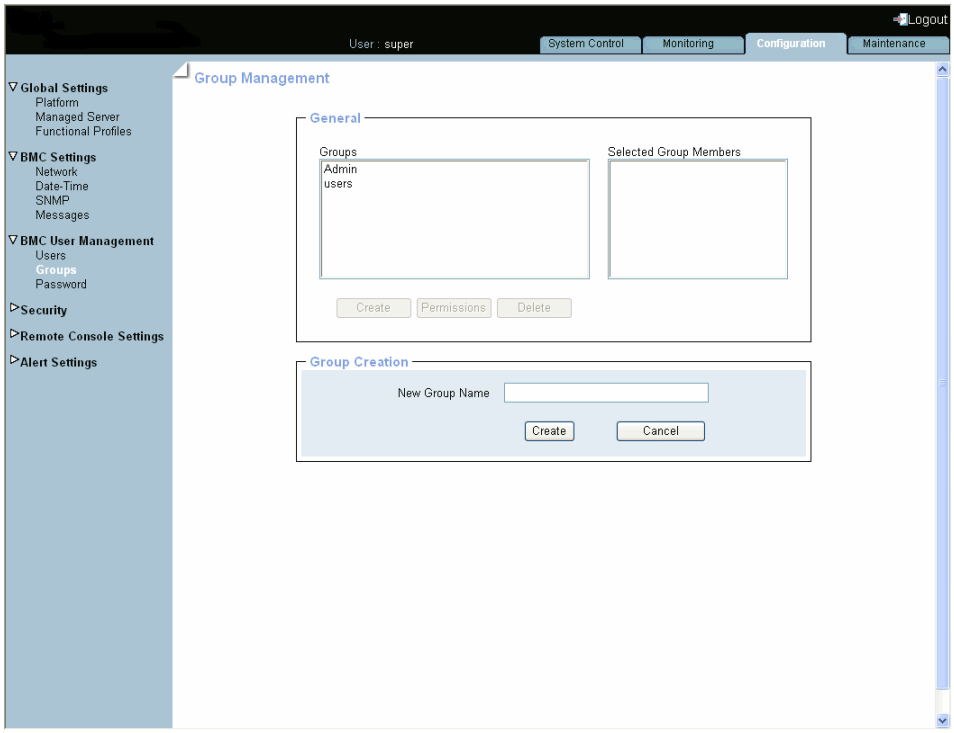
Important **Predefined groups and users cannot be renamed or deleted, but the default super user password can be changed.**
Permissions for the Admin group are not modifiable.
Permissions for the Users group are modifiable.

Prerequisites

You have **User/Group Management** permission

Procedure

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



Group Creation	
New Group Name	Name given to the group. Restrictions: • Name limited to 32 characters. • Forbidden characters: \"'`&*%|~?/ and space.

Figure 6-12. Group Management - Group Creation

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. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.10. Configuring Permissions

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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

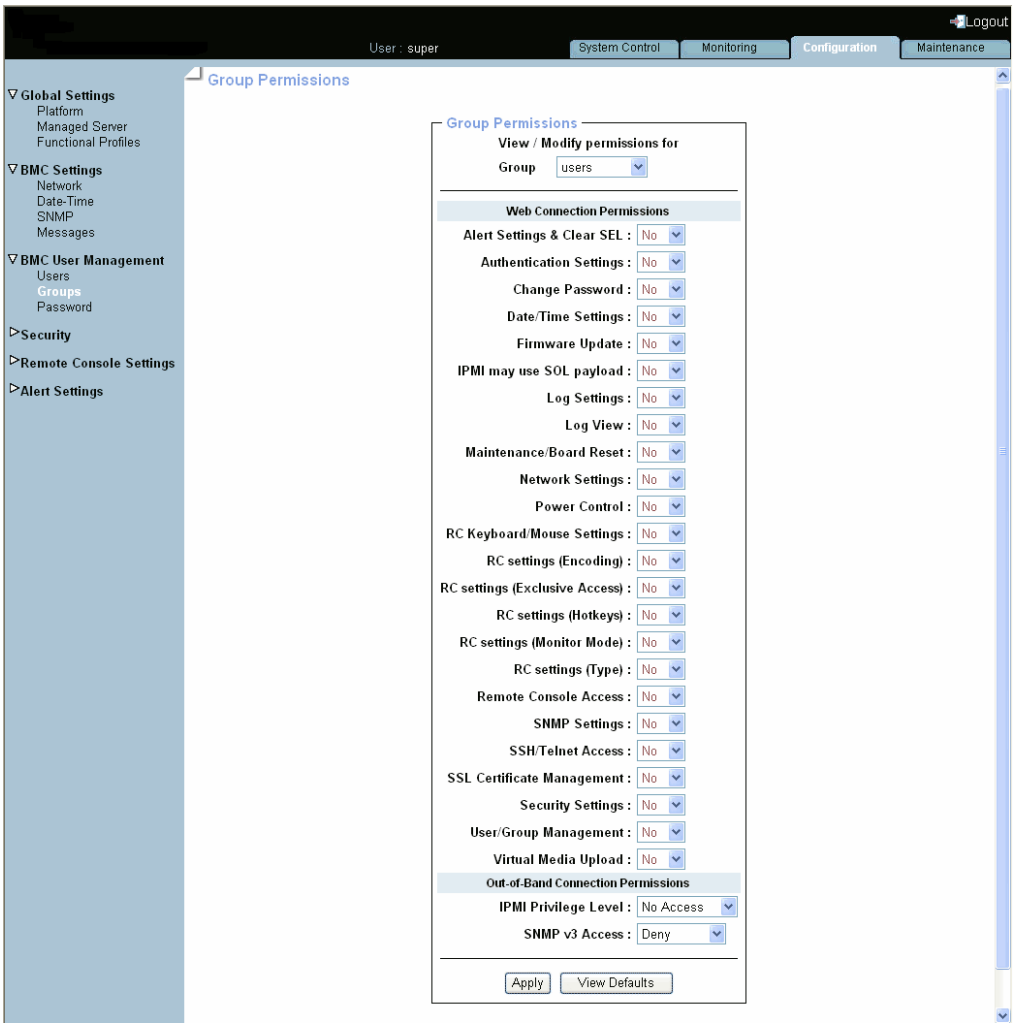
You have User/Group Management permission

You have 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.



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 6-1 and 6-2 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.
Out-of-Band Connection Permissions	The 'IPMI Privilege Level' drop-down list allows you to set a role for the selected group. See Table 6-3 and the IPMI specification for more details.
SNMP v3 Access	User accounts with this permission can send SNMP v3 commands through the LAN.

Figure 6-13. Group Permissions

3. Use Tables 6-1 and 6-2 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. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

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 Controller	Maintenance
FRU	Maintenance
Firmware Version	Maintenance
Connected Users	Maintenance

Table 6-1. Hardware 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
Authentication Settings	Authentication	Configuration
Change Password	Password	Configuration
Date/Time Settings	Date-Time	Configuration
Firmware Update	*Listed Firmware Upgrades*	Maintenance
IPMI may use SOL payload	Serial-Over-Lan connection (User accounts with this permission can launch a SOL session)	-
Log Settings	Messages	Configuration
Log View	Messages	Monitoring
Maintenance/Board Reset	Reset Management Controller	Maintenance
Maintenance/Board Reset	Hardware Exclusion	Maintenance
Network Settings	Platform	Configuration
	Managed Server	Configuration
	Functional Profile Settings	Configuration
Network Settings	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 (Exclusive Access Mode)	Configuration
RC settings (Hotkeys)	Mouse Hotkey Remote Console Button Key	Configuration
RC settings (Monitor mode)	Miscellaneous Remote Console Settings (Monitor Mode)	Configuration
RC settings (Type)	*Reserved*	-
Remote Console Access	Preview	System Control
	Launch	System Control
Remote Console Access	Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine	Maintenance
SSH/Telnet Access	SSH/Telnet connection (User accounts with this permission can send SSH/Telnet commands through the LAN)	-
SSL Certificate Management	SSL Certificate	Configuration

Configurable Permission	Feature	Tab
Security Settings	Encryption	Configuration
	User Logon Policy	Configuration
	Power Button Lockout	Configuration
	User Lockout	Configuration
User/Group Management	Users	Configuration
	Groups: Management	Configuration
	Groups: Permissions	Configuration
Virtual Media Upload	*Listed Virtual Media*	System Control

Table 6-2. Hardware Console: Configurable permissions

Out-of-Band Connection Permissions	
IPMI Privilege Level	Possible values: • No Access (default) • Callback • User • Operator • Administrator • OEM For more details about IPMI privilege levels, refer to the IPMI specification.
SNMP v3 Access	SNMP v3 connection (User accounts with this permission can send SNMP v3 commands through the LAN). Possible values: • Deny (default) • Read-only • Read-Write

Table 6-3. IPMI: Out-of-Band privileges

6.7.11. Viewing Group Membership

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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 to display the Group Management page.
2. In the Groups list, select a group. The group members appear in the Selected Group Members list.

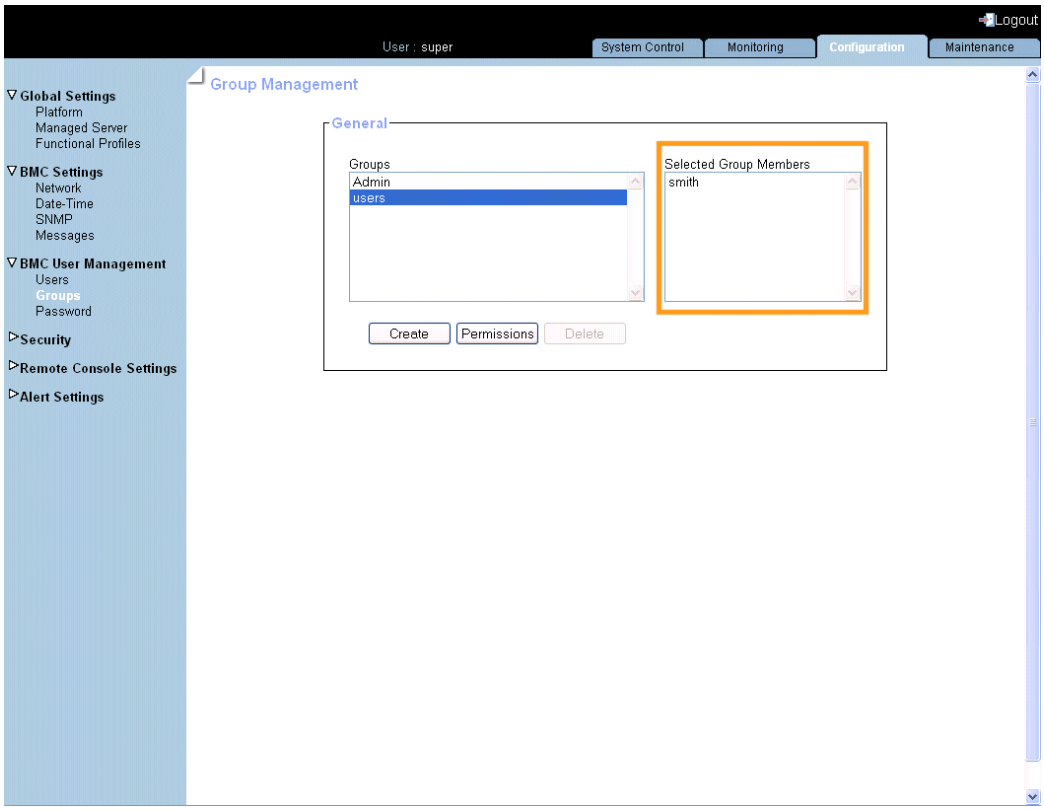


Figure 6-14. Group Management

6.7.12. Deleting a Group

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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** to display the **Group Management** page.
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.

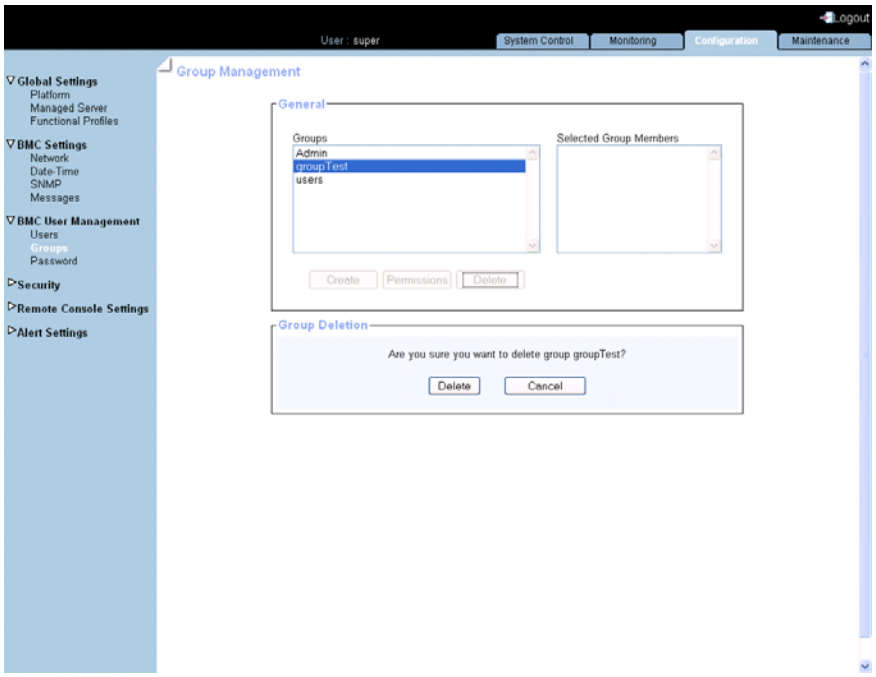


Figure 6-15. Group Management - Group Deletion

3. Click **Delete**. The group is deleted and disappears from the **Groups** box.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8. Configuring Security Parameters

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

6.8.1. Forcing HTTPS Connections

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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 generic 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.**

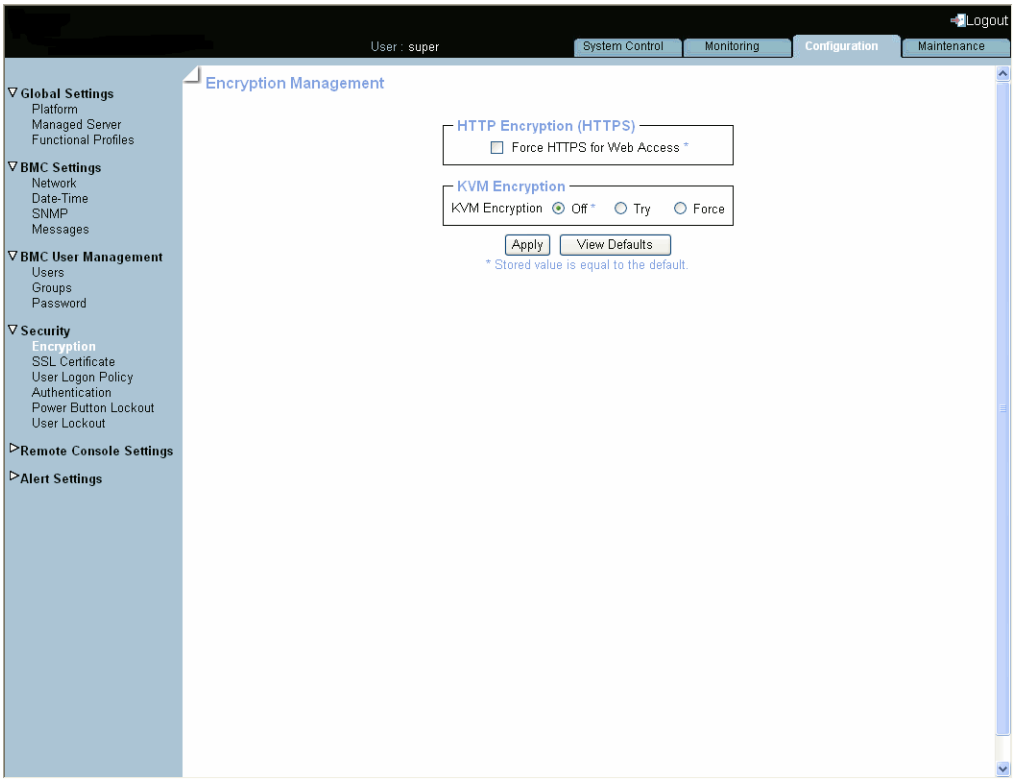
Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 6-6.

Prerequisites

You have Security Settings permission

Procedure

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



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 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. Click Apply to restore factory-default configuration.

Figure 6-16. Encryption Management - factory-default values

2. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.
3. Select the required options and click Apply.

6.8.2. Getting and Installing a New SSL Certificate

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

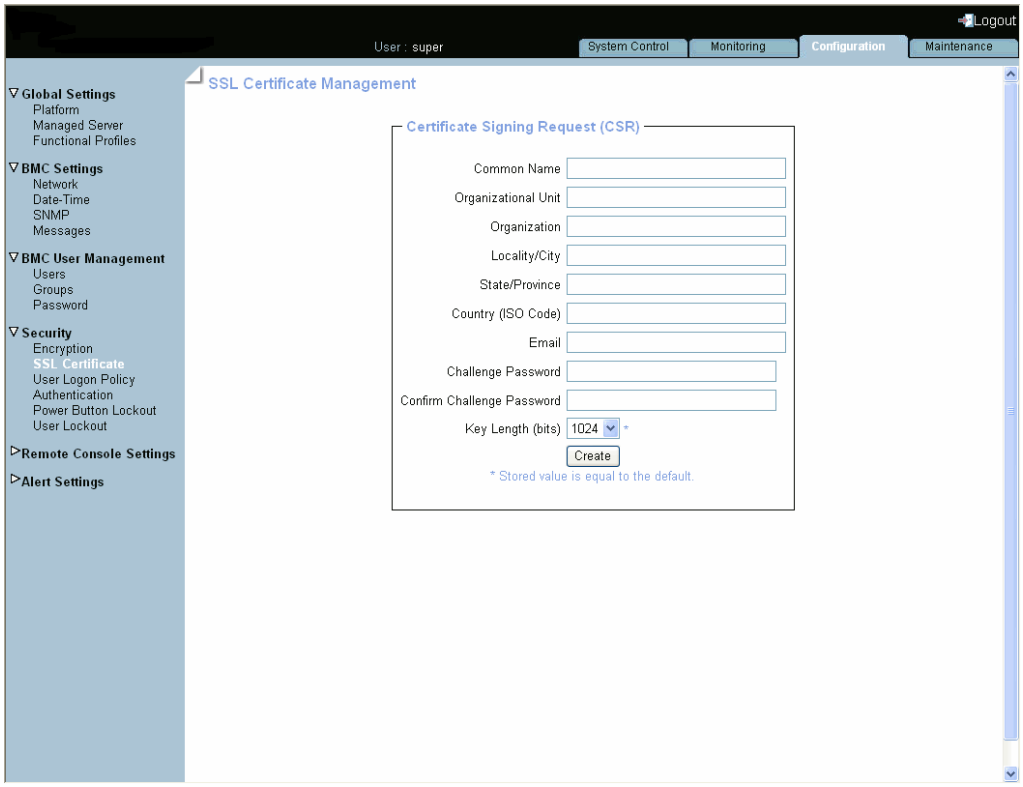
Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 6-6 .

Prerequisites

You have SSL Certificate Management permission

Procedure

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



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 system is accessed using HTTPS.
Organizational Unit	Generally the name of the department (within your organization) using the system (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 minimum 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 6-17. SSL Certificate Management

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. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.3. Configuring the Logon Policy

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

This page allows you to define how a user session should be managed in terms of the number of open sessions, password aging and idle timeout.

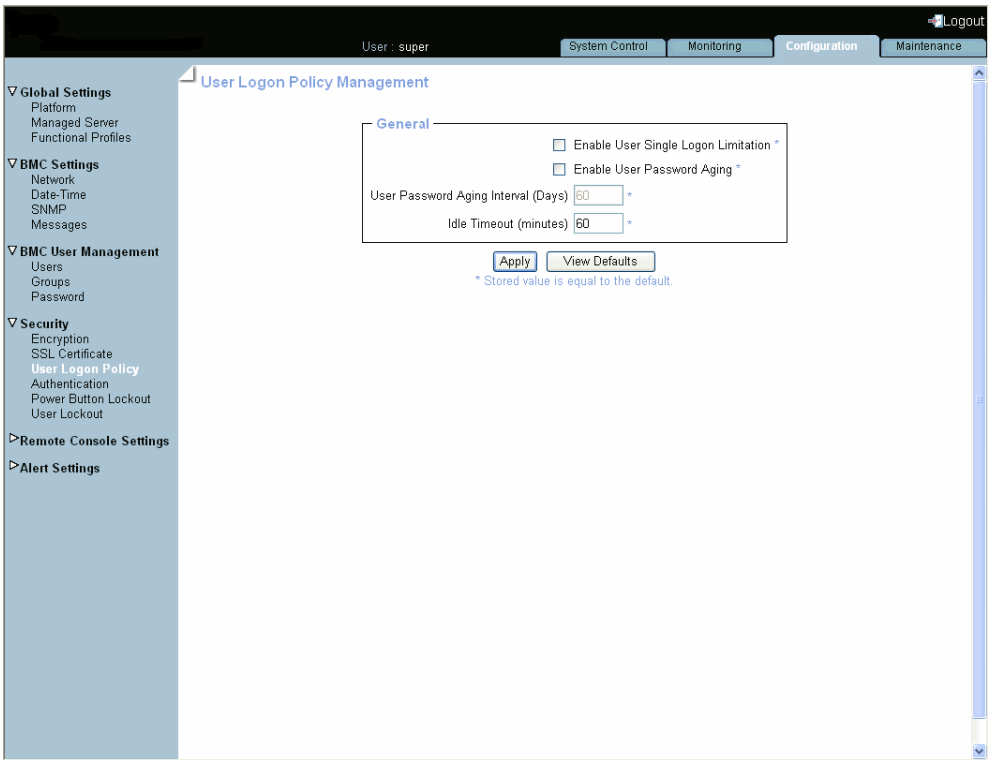
Prerequisites

You have **Security 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.



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.
Idle Timeout (Minutes)	Time after which the user is automatically disconnected, in minutes.
View Defaults button	Allows you to display factory-default values. Click **Apply** to restore factory-default configuration.

Figure 6-18. User Logon Policy Management - factory-default values

2. Select or clear the check boxes as required and click Apply.
3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.4. Managing Authentication

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

- **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

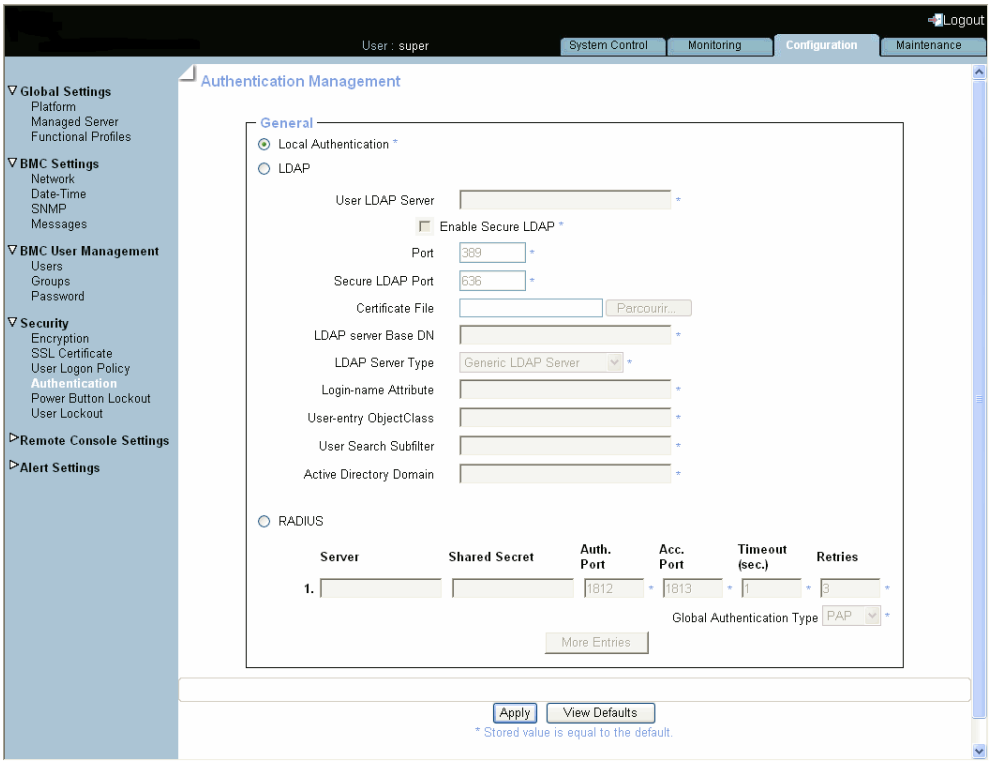
You have Authentication Settings permission

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.



General	
Local Authentication	Select to enable local console authentication.
LDAP	Select to enable LDAP server authentication.
• User LDAP Server	Enter LDAP server hostname or IP address.
• Enable Secure LDAP	Select to enable secure LDAP server authentication.
• Port	Enter the LDAP server port number used to listen to authentication requests.
• Secure LDAP Port	Enter the secure LDAP server port number used to listen to authentication requests.
• Certificate File	Browse to select the secure connection certificate supplied by the secure LDAP server administrator.
• LDAP Server Base DN	Enter the starting node to search for user accounts. Example: dc=users,dc=domain,dc=com
• LDAP Server Type	Enter 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.
• Login-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 ObjectClass	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 Search Subfilter	Restricts the search to certain user accounts. (example: (&(objectClass=person)(ou=System Validation)))
• Active Directory Domain	(Microsoft Active Directory only): Active Directory domain as it is configured in your Active Directory server. Example: users.domain.com
RADIUS	Select to enable RADIUS authentication
• Server	Enter the RADIUS server hostname or IP address.

General	
• 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	Enter the RADIUS server port number used to listen to authentication requests (#1812 by default).
• Acc. Port	Enter the RADIUS server port number used to listen to accounting requests (#1813 by default).
• Timeout (sec.)	Enter the maximum 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	Enter the maximum number of retries if a request cannot be completed.
• Global Authentication Type	Select the authentication type used by the RADIUS server.
• More Entries	If you use more than one RADIUS server, click this button to add authentication configurations.
View Defaults button	Allows you to display factory-default values. Click Apply to restore factory-default configuration.

Figure 6-19. Authentication Settings - factory-default values

2. Depending on your needs, click **Local Authentication**, **LDAP** or **RADIUS** and complete the appropriate fields and click **Apply**.
3. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.5. Enabling/Disabling the LCP Power Button

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

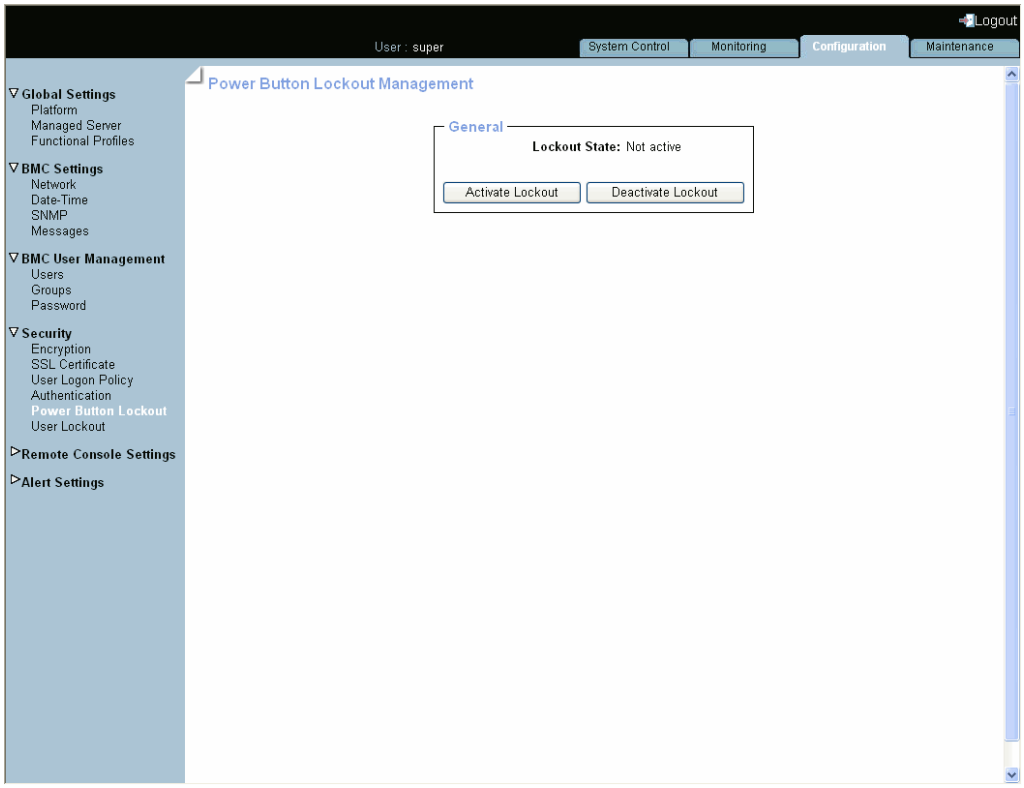
The server is equipped with a physical power button located on the Local Control Panel (LCP). This power button can be locked to prevent tampering.

Prerequisites

You have **Security Settings** permission

Procedure

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



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

Figure 6-20. Power Button Lockout Management

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

6.8.6. Configuring User Account Lockout

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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

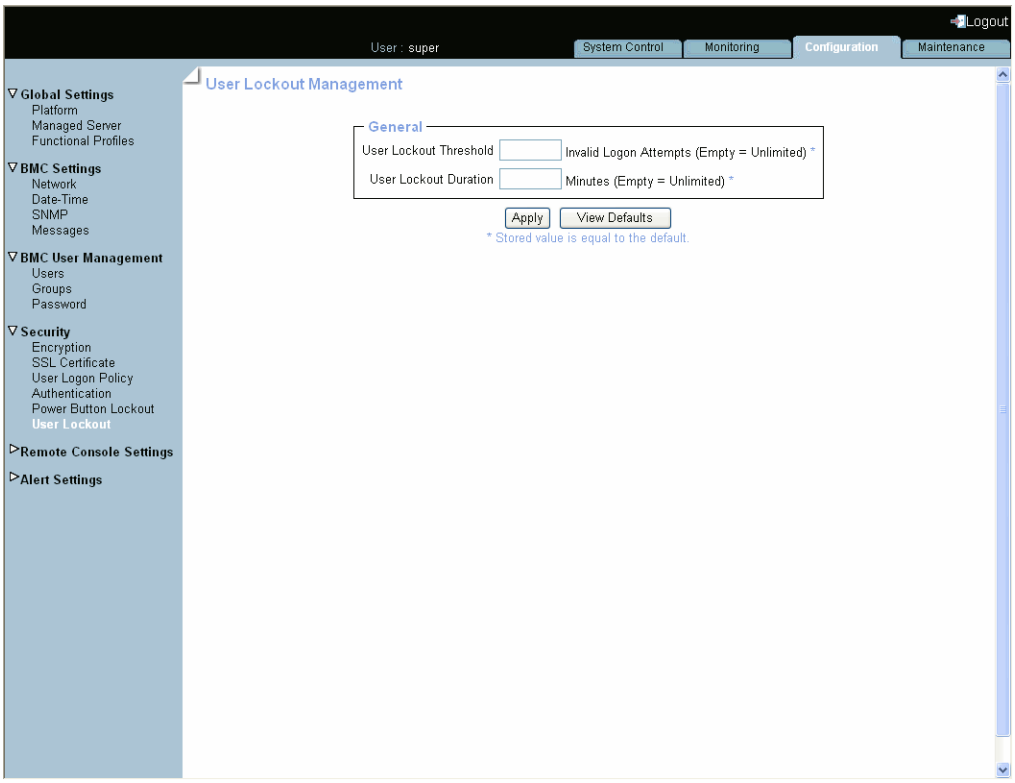
Prerequisites

You have **Security 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.



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. Click **Apply** to restore factory-default configuration.

Figure 6-21. User Lockout Management - factory-default values

2. Complete the fields and click **Apply**.
3. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9. Configuring Alerts

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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 SNMP and SMTP Servers, on page 6-47.
- Configure the event trap server IP address(es) and/or email recipient address(es). For details, see Configuring LAN Destinations, on page 6-49.
- Configure the alert transmission policy(ies). For details, see Configuring Alert Policies, on page 6-52.
- Select the events you want to report. For details, see Managing Predefined Event Filters, on page 6-54 and Customizing an Event Filter, on page 6-57.

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.**

6.9.1. Configuring SNMP and SMTP Servers

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

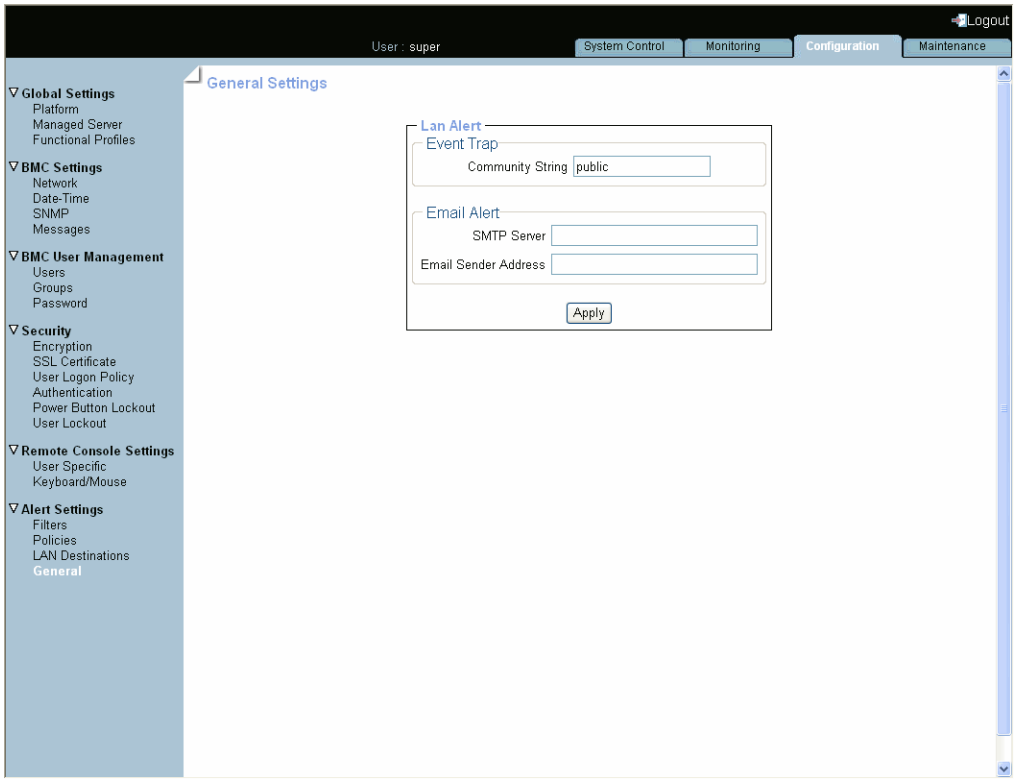
To be able to send events as alerts to SNMP managers and/or email recipients, you need to supply event trap server and email server details.

Prerequisites

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

Procedure

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



LAN Alert	
Community String	If you want to use Platform Event Trap (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 6-22. Alert General Settings

2. Complete the fields as required and click Apply.
3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.2. Configuring LAN Destinations

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

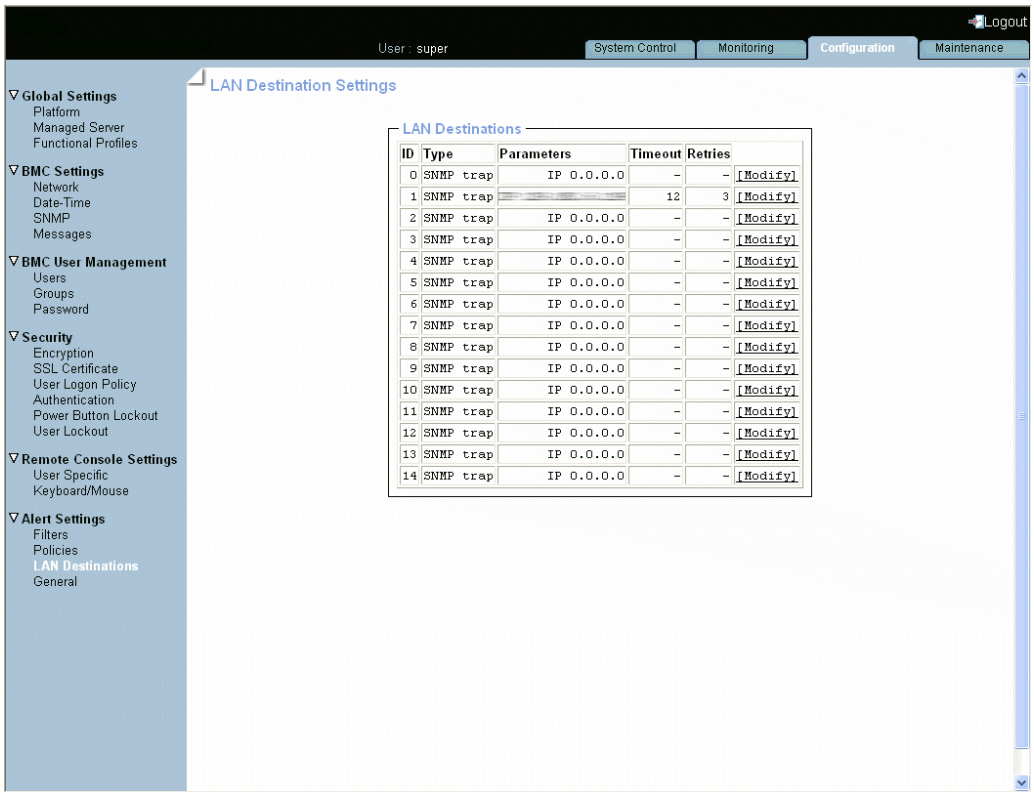
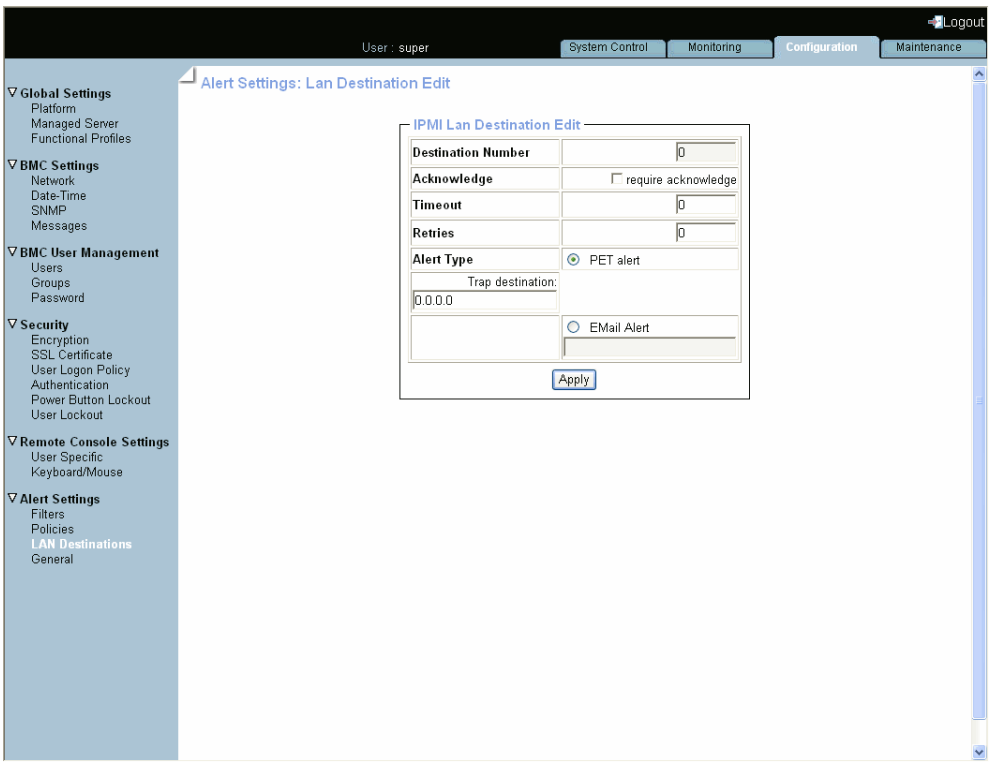


Figure 6-23. LAN Destination Settings

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.



IPMI LAN Destination Edit	
Destination Number	Read-only. Predefined number used to identify the destination to which alert messages are to be sent.
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.
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 destination	PET alerts only. SNMP manager IP address. Example: 192.x.x.x.
EMail Alert	Email alerts only. Recipient's email address. Example: john.smith@bull.net

Figure 6-24. Alert Settings: LAN Destination Edit

3. Complete the fields as required and click Apply.
4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.3. Configuring Alert Policies

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

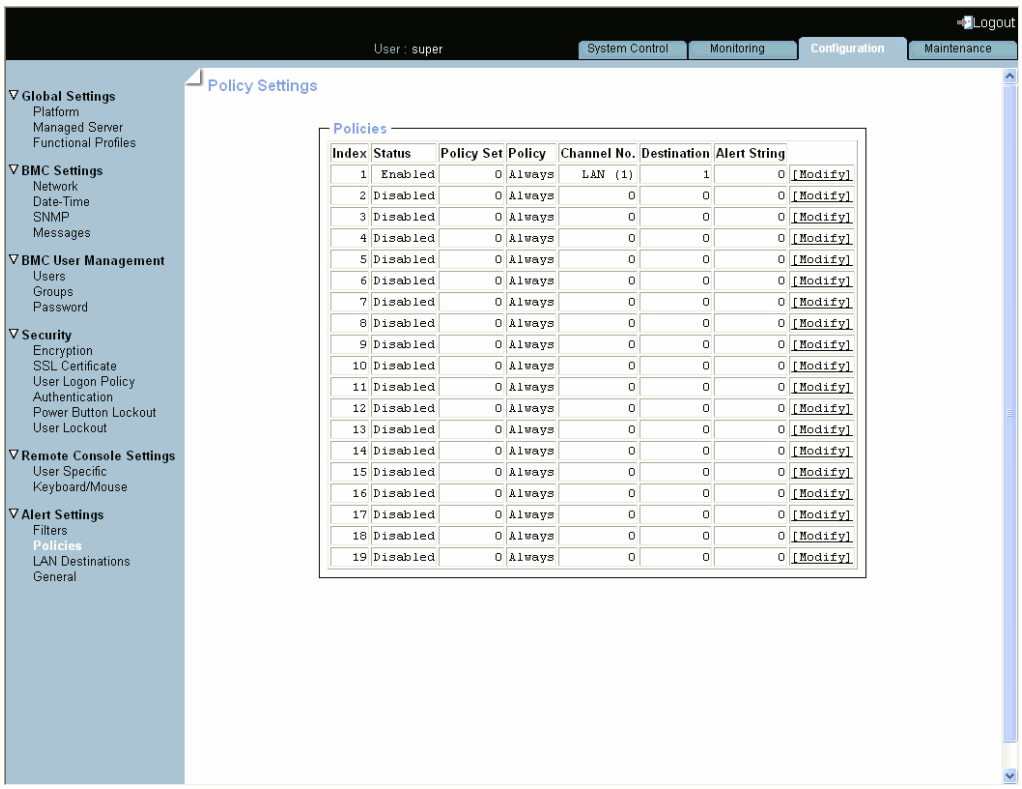
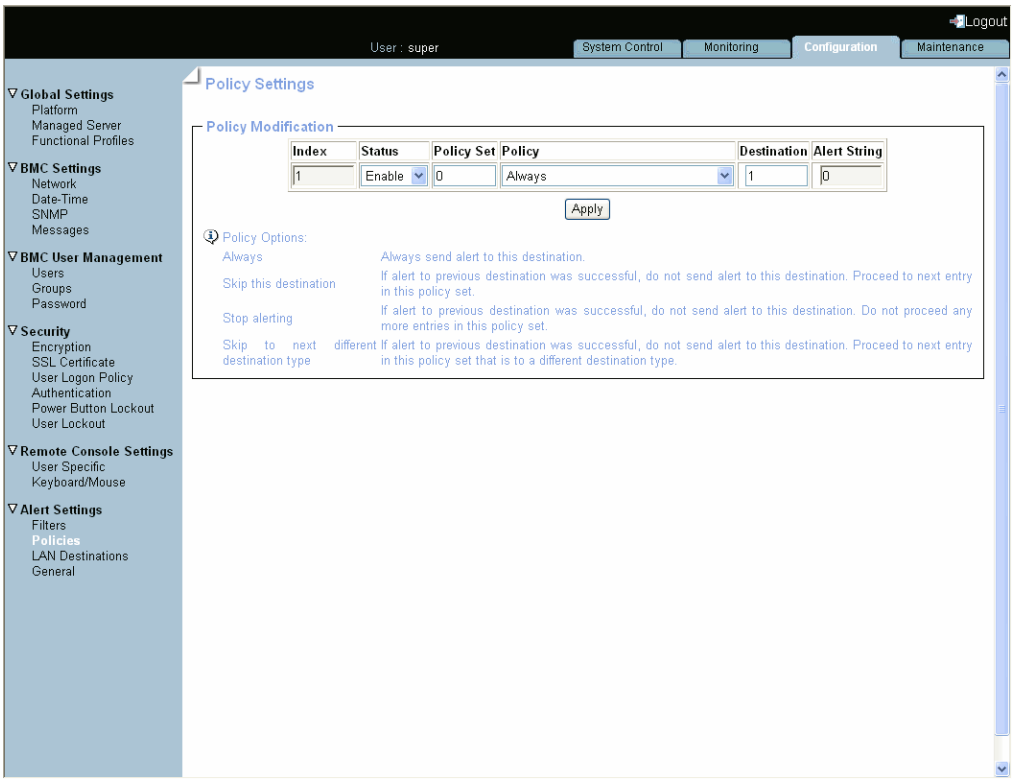


Figure 6-25. Alert policy settings

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



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	
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 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 6-26. Alert policy settings - Modification

3. Complete the required fields and click **Apply**.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

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.

6.9.4. Managing Predefined Event Filters

WARNING
If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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. **The last filter in the list of predefined filters covers ALL events.**

For details, refer to Predefined Alert Filters Description, on page A-2.

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 Customizing an Event Filter, on page 5-5.

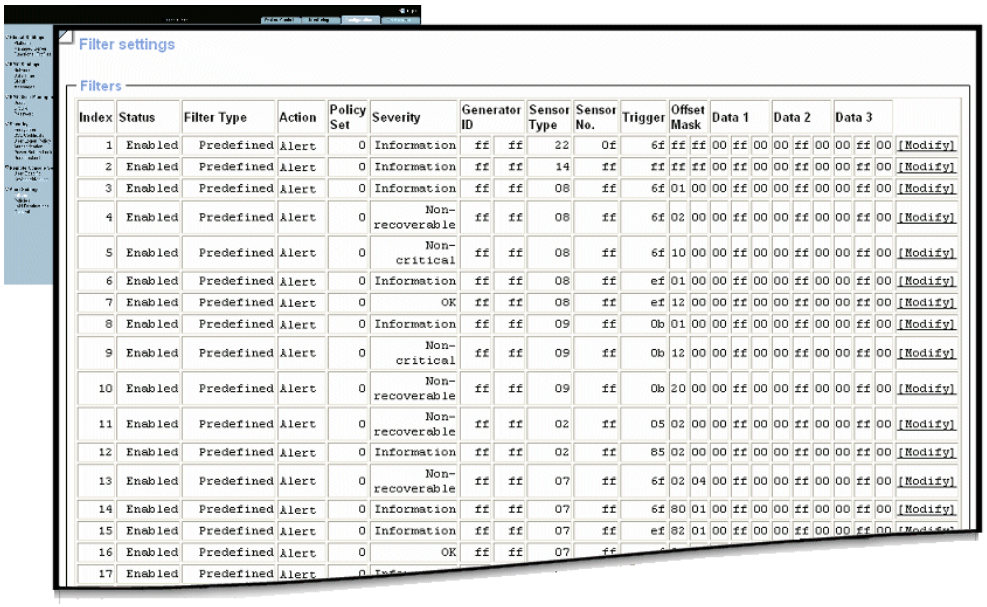
Important **If you disable filters, the corresponding events will not be transmitted to the iCare Console.**

Prerequisite

You have Alert Settings & Clear SEL permission

Procedure

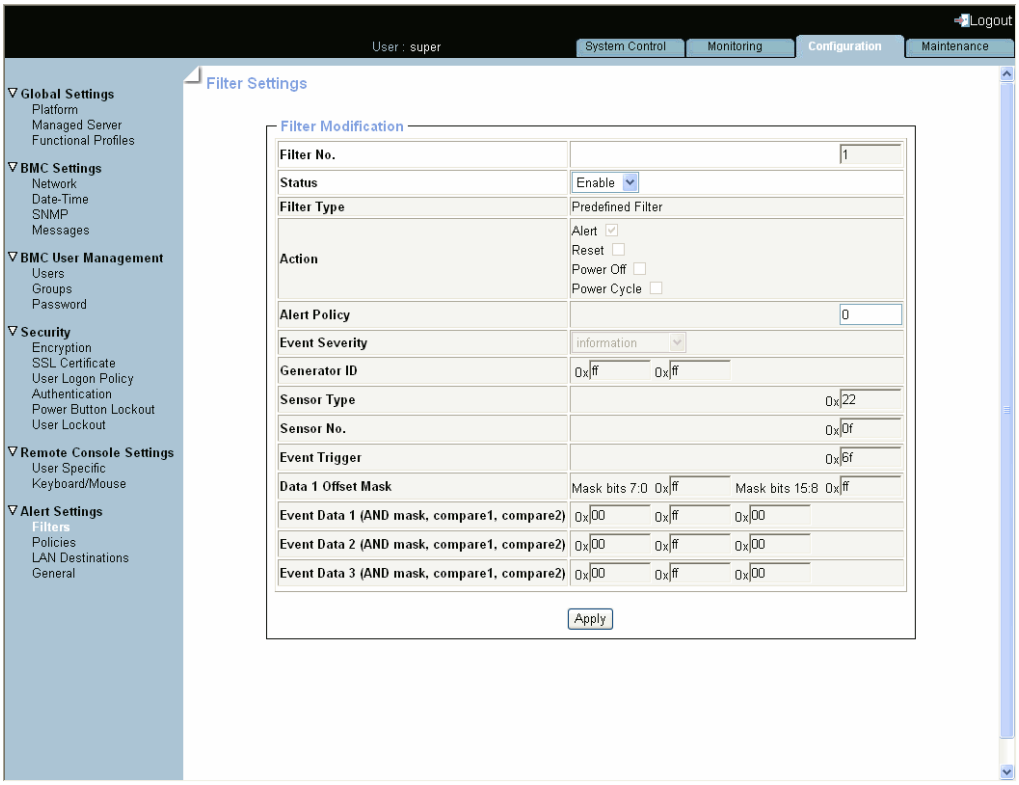
1. From the Configuration tab, click Alert Settings > Filters to display the Filter Settings page.



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	[Modify]
2	Enabled	Predefined	Alert	0	Information	ff	ff	14	ff	ff	ff	ff	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	[Modify]
4	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	08	ff	6f	02	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	[Modify]
6	Enabled	Predefined	Alert	0	Information	ff	ff	08	ff	ef	01	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	[Modify]
8	Enabled	Predefined	Alert	0	Information	ff	ff	09	ff	0b	01	00	00	ff	00	00	ff	00	[Modify]
9	Enabled	Predefined	Alert	0	Non-critical	ff	ff	09	ff	0b	12	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	[Modify]
11	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	02	ff	05	02	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	[Modify]
13	Enabled	Predefined	Alert	0	Non-recoverable	ff	ff	07	ff	6f	02	04	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	[Modify]
15	Enabled	Predefined	Alert	0	Information	ff	ff	07	ff	ef	82	01	00	ff	00	00	ff	00	[Modify]
16	Enabled	Predefined	Alert	0	OK	ff	ff	07	ff										
17	Enabled	Predefined	Alert	0															

Figure 6-27. Managing predefined filters

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



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 LAN Destinations, on page 6-49) • Reset: the server is reset. • Power Off: the server is powered down. • Power Cycle: the server is restarted
Alert Policy	Read-only: 0.
Event Severity	Read-only, according to predefined severity.
Generator ID	Read-only. For further details, you may consult the official *IPMI Specification*.
Sensor Type	
Sensor No.	
Event Trigger	
Data 1 Offset Mask	

Filter Modification	
Event Data 1 (AND mask, compare1, compare2)	
Event Data 2 (AND mask, compare1, compare2)	
Event Data 3 (AND mask, compare1, compare2)	

Figure 6-28. Modifying predefined filters

3. In the **Status** drop-down list, select either **Enable** or **Disable** depending on your needs and click **Apply**.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.5. Customizing an Event Filter

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

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.

Prerequisites

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

Procedure

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

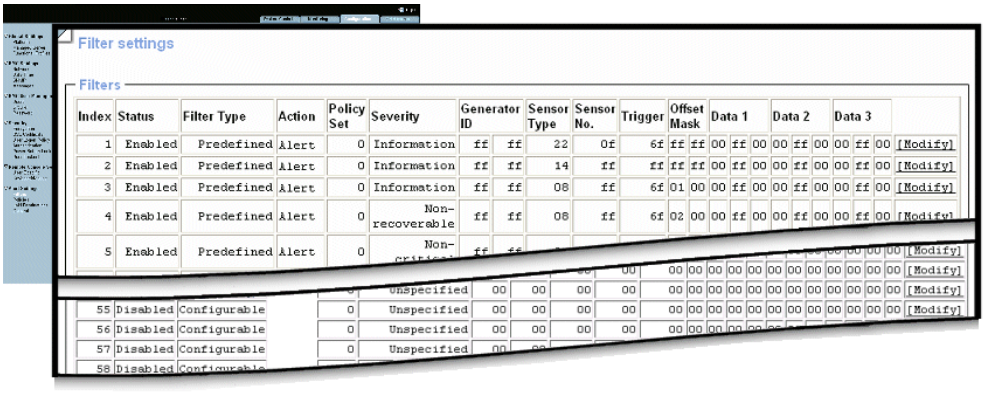
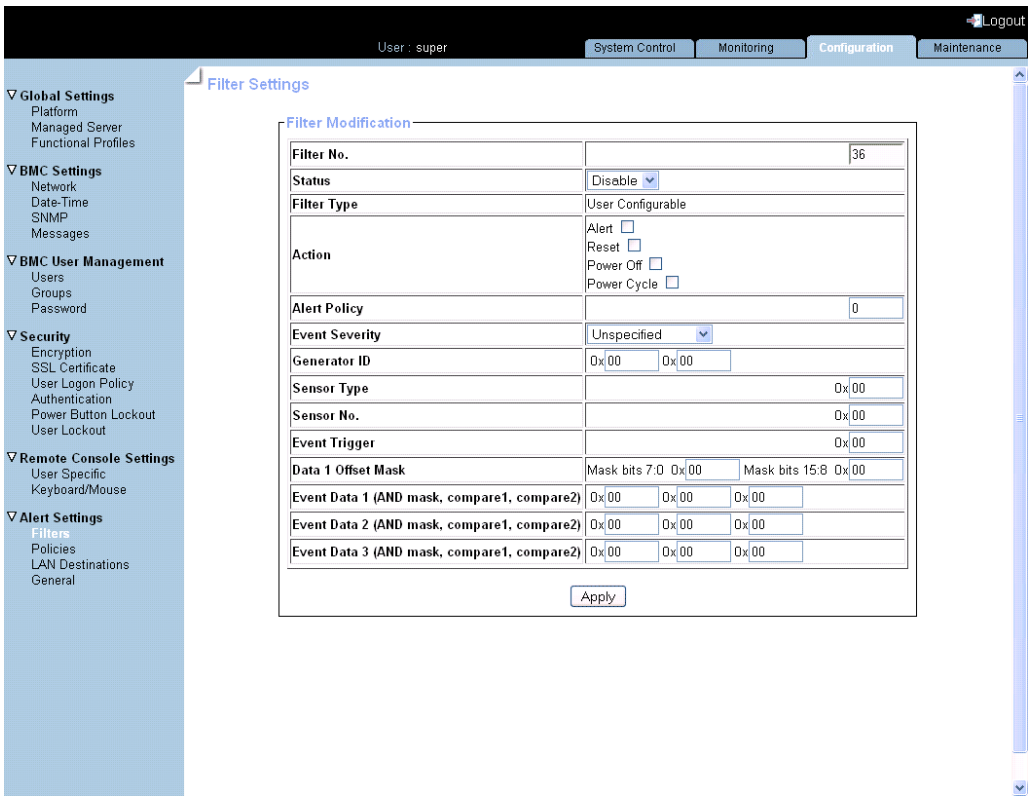


Figure 6-29. Customizing an event filter

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



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 LAN Destinations, on page 6-49) • Reset: the server is reset. • Power Off: the server is powered off. • Power Cycle: the server is powered off then powered on
Alert Policy	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*.

Filter Modification	
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 6-30. Configurable Filters - Modification

3. Complete the required fields and click **Apply**.
4. Use the **KiraTool** utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

Chapter 7. Using Maintenance Features

This chapter explains the maintenance operations you can perform from the Hardware Console and how to use the utilities provided on the *Resource and Documentation CD*. It includes the following topics:

Note The Hardware Console can be used to perform firmware updates. These operations may only be performed by qualified support personnel and are not documented in this guide. Please contact your Customer Service Representative for further information.

7.1. Getting Management Controller Information

You can display and/or save to an XML file embedded management controller 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 Controller** to display the **Management Controller Information** page.

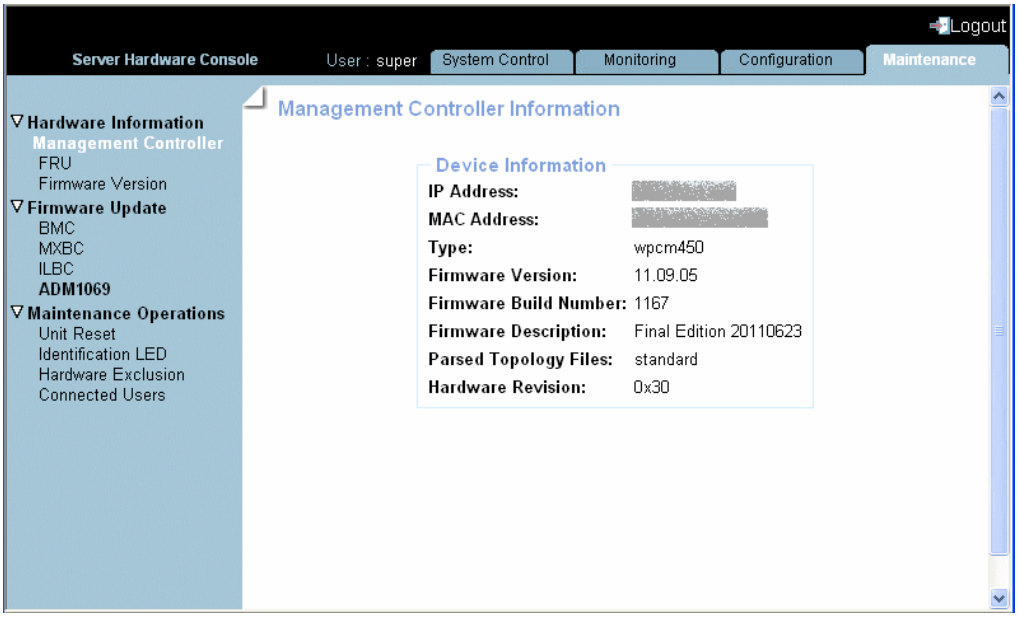


Figure 7-1. Management Controller Information

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

7.2. Getting 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.

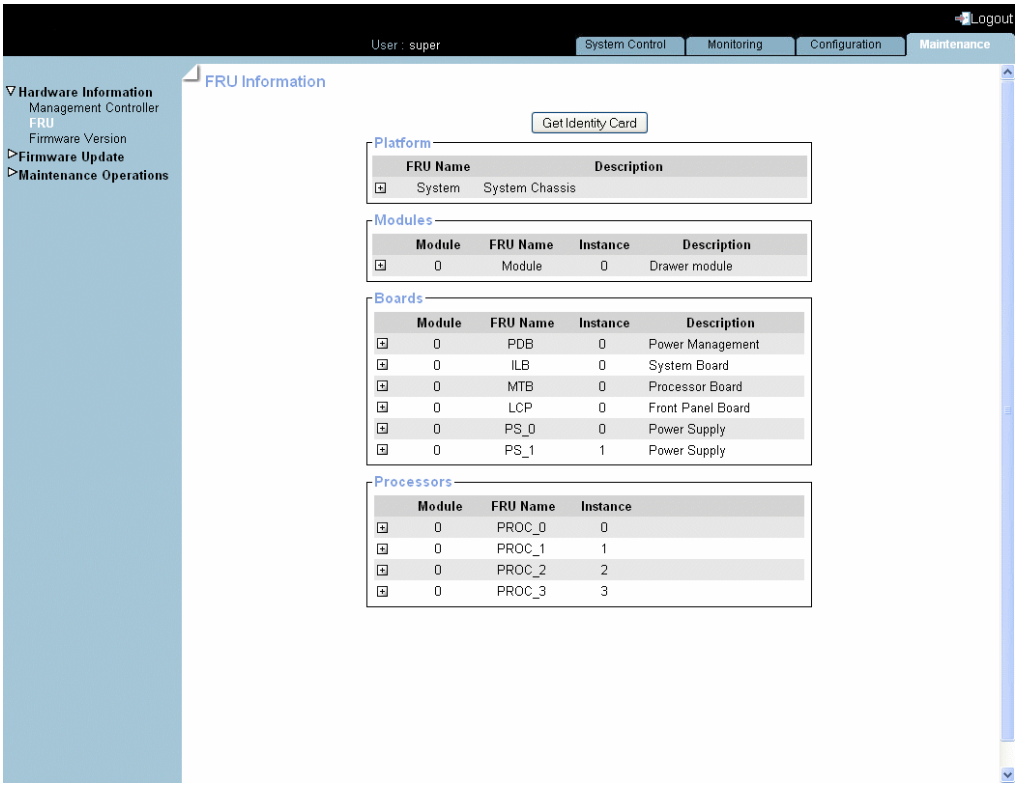


Figure 7-2. FRU Information

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 FRU information in XML format, click **Get Identity Card** and follow the instructions on the screen.

7.3. Displaying Firmware Versions

This feature is particularly useful for maintenance and troubleshooting (checking the 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.

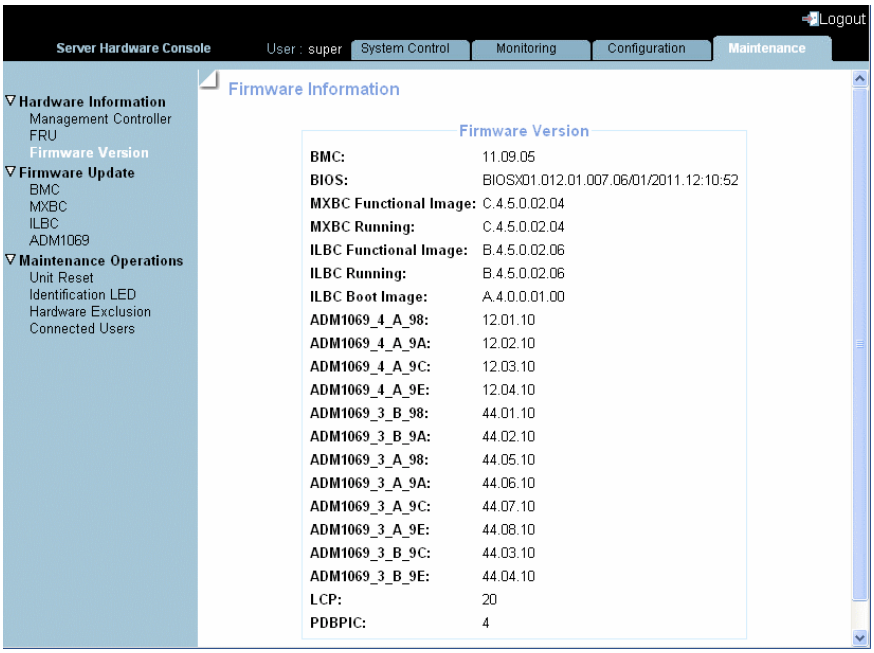


Figure 7-3. Viewing Firmware Information - Server Example

Note According to server model, other firmware image types may be displayed.

Note For certain firmware, more than one type of image is displayed:

- MXBC Functional Image: MXBC image loaded in the SPI Flash EEPROM
- MXBC Running Image: MXBC image loaded in the associated FPGA RAM
- ILBC Functional Image: ILBC image loaded in the SPI Flash EEPROM
- ILBC Running Image: ILBC image loaded in the associated FPGA RAM
- ILBC Boot Image: ILBC boot image loaded in the SPI Flash EEPROM

7.4. Updating Firmware

The firmware on the boards listed below can be updated to install new features or to ensure system integrity after a maintenance operation.

- Embedded Management Controller (BMC)
- Memory and Xeon Board (MXBC)
- I/O Legacy Board (ILBC)
- ADM 1069
- FPGA PCIe Interface images(FPIF IMGA and FPIF IMGB)
- Local Control Panel (LCP)

WARNING
Qualified support personnel only is authorized to update server firmware. These operations are hazardous and are not documented in this guide.
Please contact your Customer Service Representative for further information.

7.5. Performing Reset Operations

The embedded management controller, the virtual keyboard/mouse, USB and video engine can be reset when needed, for example if the system hangs or if the virtual keyboard/mouse or screen no longer respond.

Note The embedded management controller is automatically reset after a BMC firmware update.

Prerequisites

Reset Management Controller: you have **Maintenance/Board Reset** permission

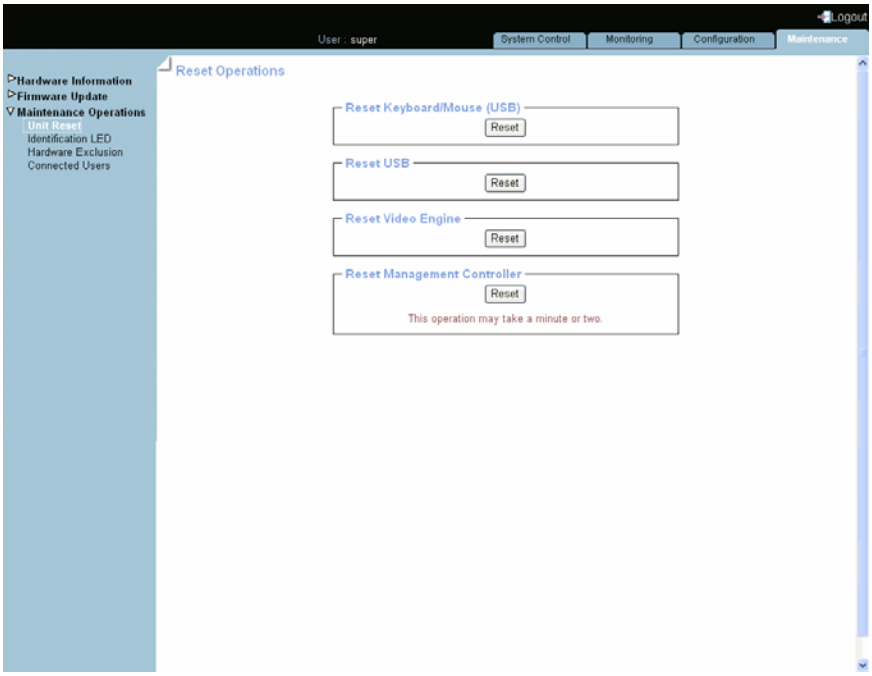
Reset Keyboard/Mouse, USB, Video Engine: you have **Remote Console Access** permission

All users have disconnected from the console

Procedure

Note The **Reset Management Controller** command will disconnect any connected users.

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



Feature	Explanation
Reset Keyboard/Mouse (USB) button	Resets the virtual keyboard/mouse.
Reset USB button	Resets the virtual USB.
Reset Video Engine button	Resets the virtual monitor.
Reset Management Controller button	Stops and restarts the embedded management controller.

Figure 7-4. Reset Operations

2. Click the required **Reset** button.

7.6. Enabling/Disabling the Identification LED

The server 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 the 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.

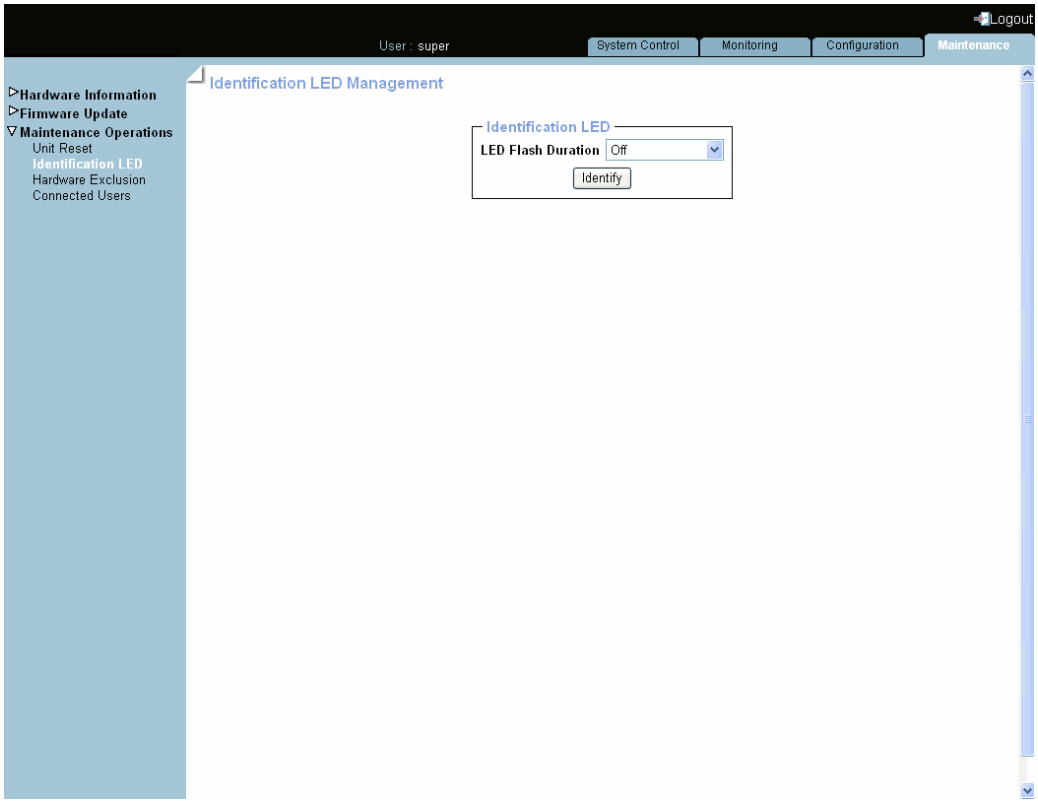


Figure 7-5. Identification LED Management

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

7.7. Excluding/Including Processors

The console allows you to exclude and include processors statically: the server must be powered off to select the processors to exclude/include and the modification is taken into account at the next power on.

Note Processors are only excluded logically. They remain powered on to ensure system operation.

Prerequisites

You have **Maintenance/Board Reset** permission

The server is powered off

Procedure

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

1. From the **System Control** tab, check that the server is powered down to the standby mode by selecting **Power Management** and 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 first and then proceed to Step 2.

2. From the **Maintenance** tab, click **Maintenance Operations > Hardware Exclusion** to display the **Hardware Exclusions** window.

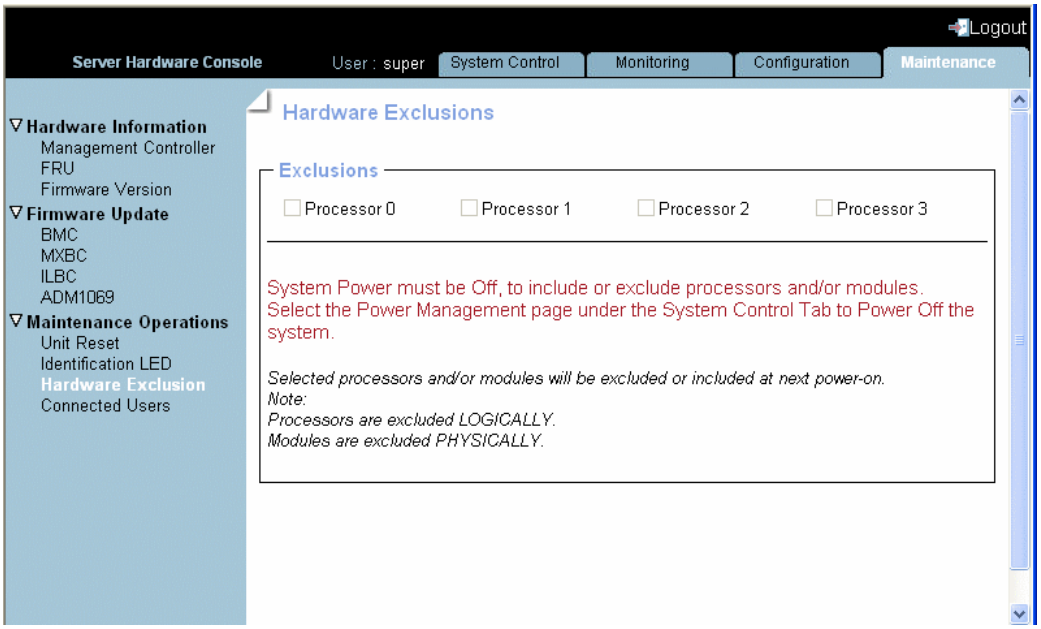


Figure 7-6. Hardware Exclusions

Important **If the server is not powered down to the standby mode, a message is displayed requesting you to do so. Go to Step 1.**

3. Either select the check box(es) corresponding to the processors to exclude or clear the check box(es) corresponding to the processors to include and click **Apply**.
4. Power on the server to apply the modification.

7.8. Excluding/Including a Server Module

The console allows you to exclude and include server modules statically: the server module must be powered off before selecting the components to exclude/include, and the modification is taken into account at the next power on.

Note Modules are excluded physically.

Prerequisites

You have **Maintenance/Board Reset** permission

The server is powered off

Procedure

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

1. From the **Power Control** tab, check that the server module is powered down to the standby mode by selecting **Power Management** and 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 first and then proceed to Step 2.

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

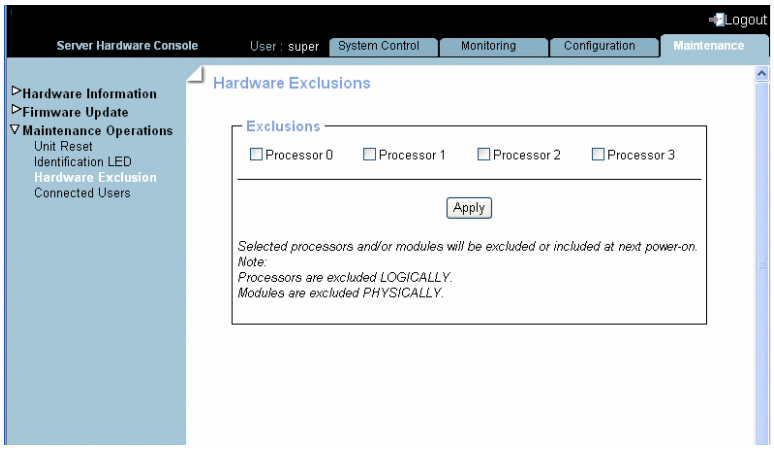


Figure 7-7. Excluding/Including Modules

Important **If the server module is not powered down to the standby mode, a message is displayed requesting you to do so. Go to Step 1.**

3. Either select the check box(es) corresponding to the server module to exclude or clear the check box(es) corresponding to the module to include and click **Apply**.
4. Power on the server module to apply the modification.

7.9. Displaying 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.

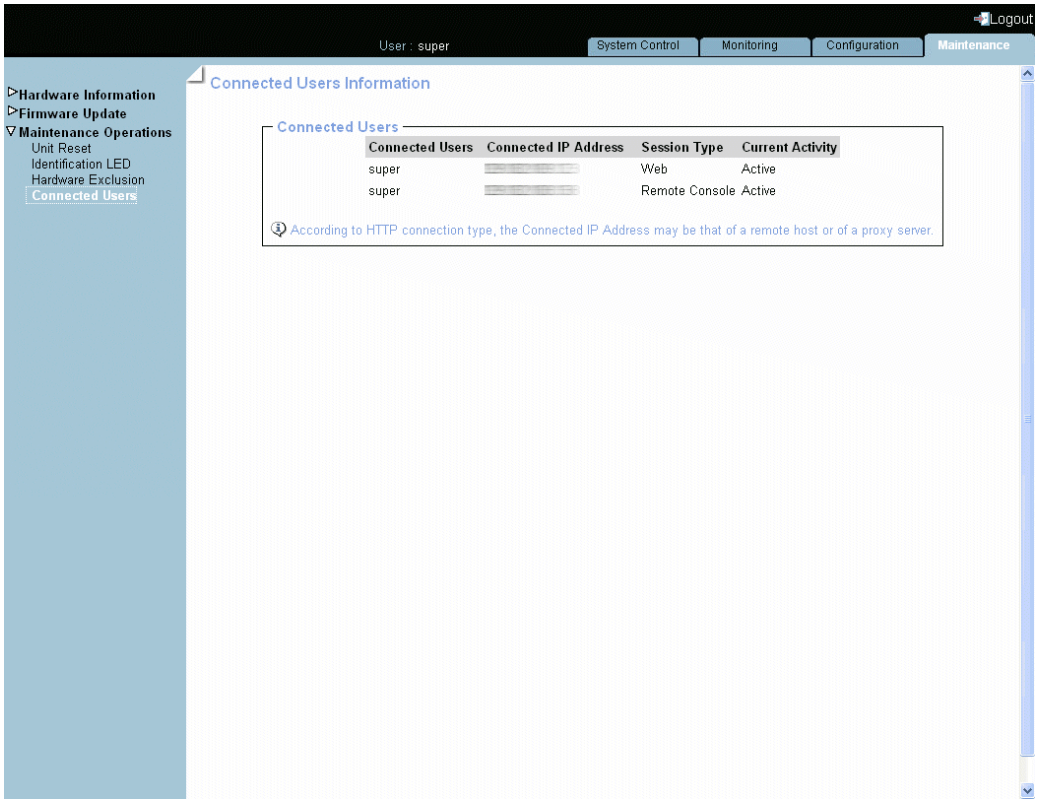


Figure 7-8. Connected Users Information

7.10. Backing Up Configuration Data

Note Backing up configuration data is an administrative task and requires extensive permissions. You are advised to use the default **super** user account.

Important **Follow the instructions set out in the *KiraTool* utility documentation provided on the *Resource and Documentation CD* to back up data.**

1. Check that the *KiraTool* utility is installed.
2. Refer to the *KiraTool* documentation available on the *Resource and Documentation CD*.
3. From the *KiraTool* utility, launch the backup command as described in the documentation.
4. Carefully note the backup file name and transmit it to the system administrator. The file will be used to restore configuration data when required.

Important **Two operations may be necessary to back up respectively:**

- configuration data (**`cfg backup conf`**)
- alert settings data **`(cfg backup pef)`**

7.11. Restoring Configuration Data

Note Restoring configuration data is an administrative task and requires extensive permissions. You are advised to use the default **super** user account.

Important **Follow the instructions set out in the *KiraTool* utility documentation provided on the *Resource and Documentation CD* to restore data.**

1. Check that the *KiraTool* utility is installed.
2. Request the backup file name and path from the system administrator.
3. Refer to the *KiraTool* documentation available on the *Resource and Documentation CD*.
4. From the *KiraTool* utility, launch the restore command as described in the documentation.

Important **Two operations may be necessary to restore respectively:**

- configuration data (**`cfg restore conf`**)
- alert settings data **`(cfg restore pef)`**

Appendix A. Troubleshooting the Server

This chapter describes how to troubleshoot the server. It includes the following topics:

A.1. 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.

Predefined Alert Filters Description

For guidance, the following sets of filters are available, according to component type and server model:

Component Type	Filter Index
Power system board	1
Sub-chassis	2, 35, 36
Power supply	3, 4, 5, 6, 7
Power unit	8, 9, 10, 40
System board (ILB)	11, 12, 23, 47
Processor board (MXB)	11, 12, 23, 47
Processor	11, 12, 13, 14, 15, 16, 44
Fan device / Cooling unit	17, 18, 19, 20, 21, 23, 47
Power distribution board (PDB)	23, 47
Ultra capacitor	23, 45, 46, 47, 48, 49, 50
Control panel (LCP)	23, 47
Embedded Management Controller (BMC)	24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 37, 39, 41, 42, 43
Memory	38
External Environment	22, 23, 47
All	51

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 Alerts, on page 6-47.

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	Information	The system is powered on.
1	Power system board	ACPI Pwr State	S4/S5: soft off	Information	The system is powered off.
2	Sub-chassis	Power button	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.
9	Power unit	Pwr Redundancy	Non redundant: Sufficient resources from Insufficient resources	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_X	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
11	Processor board (MTB)	MTB_X	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
11	Processor board (MXB)	MXB_X	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
11	Processor	PX_X	Limit exceeded	Non-recoverable	This voltage is out of the acceptable range.
12	System board (ILB)	ILB_X	Limit exceeded	Information	This voltage is now OK.
12	Processor board (MTB)	MTB_X	Limit exceeded	Information	This voltage is now OK.
12	Processor board (MXB)	MXB_X	Limit exceeded	Information	This voltage is now OK.
12	Processor	PX_X	Limit exceeded	Information	This voltage 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.
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.

N°	Component	Source	Event Description	Severity	Meaning
17	Cooling unit	FANPR_X Redund.	Fully redundant	Information	Both of the fans in the fan pair are up and running.
18	Cooling unit	FANPR_X Redund.	Redundancy lost	Non-critical	Only one fan in the fan pair is up and running.
19	Cooling unit	FANBX_X Redund.	Non redundant: Insufficient resources	Non-recoverable	No fans are working in the fan pair.
20	Cooling unit	FANUNIT_X Pres	Device removed / Device absent	Non-recoverable	The fan unit is not or no more present.
20	Fan device	FAN_X Presence	Device removed / Device absent	Non-recoverable	In the fan pair #X the fan#Y is not or no more present.
21	Cooling unit	FANUNIT_X Pres	Device inserted / Device present	Return to OK	The fan unit is (now) present.
21	Fan device	FAN_X Presence	Device inserted / Device present	Return to OK	In the fan pair #X the fan#Y is (now) present.
22	External Environment	Ambient Temp.	At or above upper critical threshold (going high)	Non-recoverable	The external temperature is above the defined threshold. By default a power off has been executed.
23	Cooling unit	ROTOR_XY Speed	At or below lower critical threshold (going low)	Return to OK	In the fan unit #X, the rotor #Y speed is now at normal speed.
23	Fan device	FAN_X Speed	At or below lower critical threshold (going low)	Return to OK	In the fan pair # X the fan #Y is now at normal speed.
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.
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.
23	Processor board (MXB)	MXB Temperature	At or below lower critical threshold (going low)	Return to OK	The MXB temperature is now OK.
23	Processor board (MXB)	MXB Temperature	At or above upper critical threshold (going high)	Return to OK	The MXB temperature is now OK.
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.
23	Ultra capacitor	Ultra Capa Temperature	At or below lower critical threshold (going low)	Return to OK	The UltraCapa temperature is now OK.
23	Ultra capacitor	Ultra Capa Temperature	At or above upper critical threshold (going high)	Return to OK	The UltraCapa temperature is now OK.
23	Ultra capacitor	UC XX V	At or below lower critical threshold (going low)	Return to OK	This voltage is now OK.

N°	Component	Source	Event Description	Severity	Meaning
23	Ultra capacitor	UC XX V	At or above upper critical threshold (going high)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VCAP	At or above upper critical threshold (going high)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VCAP	At or above upper critical threshold (going high)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VBOOST	At or below lower critical threshold (going low)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VBOOST	At or above upper critical threshold (going high)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VREF	At or below lower critical threshold (going low)	Return to OK	This voltage is now OK.
23	Ultra capacitor	UC VREF	At or above upper critical threshold (going high)	Return to OK	This voltage is now OK.
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.
23	External Environment	Ambient Temp.	At or above upper critical threshold (going high)	Return to OK	The external temperature is now OK.
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
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 fatal error has occurred.
26	BMC	Version Change	Management controller firmware change was successful.	Information	A version change event has occurred.
26	BMC	Version Change	System firmware change was successful	Information	A version change event has occurred.
26	BMC	Version Change	Programmable hardware change was successful	Information	A version change event has occurred.
27	BMC	Version Change	Management controller firmware change was unsuccessful	Non-critical	A version change event has occurred.
27	BMC	Version Change	System firmware change was unsuccessful	Non-critical	A version change event has occurred.

N°	Component	Source	Event Description	Severity	Meaning
27	BMC	Version Change	Programmable hardware change was unsuccessful	Non-critical	A version change event has occurred.
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	See SEL Messages: BMC.
30	BMC	Watchdog	Timeout - no specific action	Critical	Timeout during BIOS init step which causes the configured action.
30	BMC	Watchdog	Timeout followed by hard reset	Critical	Timeout during BIOS init step which causes the configured action.
30	BMC	Watchdog	Timeout followed by Power Down	Critical	Timeout during BIOS init step which causes the configured action.
30	BMC	Watchdog	Timeout followed by Power Cycle	Critical	Timeout during BIOS init step which causes the configured action.
31	BMC	Platform Security Violation Attempt	Out-of-band access password violation	Non-critical	An out of band IPMI access failed due to password violation.
32	BMC	System Event	Entry added to auxiliary log	Information	A corrected machine error has been logged by BIOS in the non-volatile area.
33	BMC	System Event	Entry added to auxiliary log	Critical	An uncorrected machine error has been logged by BIOS in the non-volatile area.
34	BMC	System Event	Entry added to auxiliary log	Non-recoverable	A fatal machine error has been logged by BIOS in the non-volatile area.
35	Sub-chassis	Mod. Intrusion	General chassis intrusion	Critical	The enclosure is opened.
36	Sub-chassis	Mod. Intrusion	General chassis intrusion	Return to OK	The enclosure is now closed.
37	BMC	Chipset Error	Transition to OK	Return to OK	Return to normal temperature.
38	Memory	DIMM_XX	Correctable ECC threshold reached	Warning	Correctable ECC threshold reached on DIMM_XX.
39	BMC	Chipset Error	Informational	Information	A chipset correctable error has occured.
40	Power unit	Pwr Consumption	Power Consumption Level	Information	This event does not appear in the System Event Log (SEL)
41	BMC	Version Change	Firmware or software change	Information	BIOS recovery
42	BMC	System Boot Init	Initiated by hard reset	Information	System Boot Init
42	BMC	System Boot Init	OS / run-time software initiated hard (warm)reset	Information	System Boot Init
42	BMC	System Boot Init	System restart	Information	System Boot Init
43	BMC	OS Stop	OS graceful stop	Information	OS Stop
43	BMC	OS Stop	OS graceful shutdown	Information	OS Stop
44	Processor	Proc_X	Processor automatically throttled	Critical	PROC_X runs slowly to limit temperature or power consumption.
45	Ultra Capacitor	UC VCAP	At or above upper non recoverable threshold (going high)	Non recoverable	This voltage is out of the acceptable range. The module is powered off and disabled.

N°	Component	Source	Event Description	Severity	Meaning
46	Ultra Capacitor	UC VCAP	At or above upper non recoverable threshold (going high).	Return to OK	This voltage is now OK
47	Cooling unit	ROTOR_XY Speed	At or below lower critical threshold (going low)	Critical	In the fan unit #X, the rotor #Y speed is lesser than the minimum required.
47	Fan device	FAN_X Speed	At or below lower critical threshold (going low)	Critical	In the fan pair # X the fan #Y speed is lower than the minimum required.
47	System board (ILB)	ILB Temperature	At or below lower critical threshold (going low)	Critical	The ILB temperature is lower than the minimum.
47	System board (ILB)	ILB Temperature	At or above upper critical threshold (going high)	Critical	The ILB temperature is above the maximum.
47	Processor board (MXB)	MXB Temperature	At or below lower critical threshold (going low)	Critical	The MXB temperature is lower than the minimum.
47	Processor board (MXB)	MXB Temperature	At or above upper critical threshold (going high)	Critical	The MXB temperature is above the maximum.
47	Power distribution board (PDB)	PDB Temperature	At or below lower critical threshold (going low)	Critical	The PDB temperature is lower than the minimum.
47	Power distribution board (PDB)	PDB Temperature	At or above upper critical threshold (going high)	Critical	The PDB temperature is above the maximum.
47	Power distribution board (PDB)	UltraCapa Temp.	At or below lower critical threshold (going low)	Critical	The Ultra Capa temperature is lower than the minimum.
47	Power distribution board (PDB)	UltraCapa Temp.	At or above upper critical threshold (going high)	Critical	The Ultra Capa temperature is above the maximum.
47	Control panel (LCP)	LCP Temperature	At or below lower critical threshold (going low)	Critical	The LCP temperature is lower than the minimum.
47	Control panel (LCP)	LCP Temperature	At or above upper critical threshold (going high)	Critical	The LCP temperature is above the maximum.
47	External Environment	Ambient Temp.	At or above upper non-critical threshold (going high)	Critical	The external temperature is above the non critical threshold.
47	Ultra Capacitor	Ultra Capa Temperature	At or below lower critical threshold (going high)	Critical	The UltraCapa temperature is lower than the minimum.
47	Ultra Capacitor	Ultra Capa Temperature	At or above upper critical threshold (going high)	Critical	The UltraCapa temperature is higher than the maximum.
47	Ultra Capacitor	UC XX V	At or below lower critical threshold (going high)	Critical	This voltage is out of the acceptable range.
47	Ultra Capacitor	UC XX V	At or above upper critical threshold (going high)	Critical	This voltage is out of the acceptable range.
47	Ultra Capacitor	UC VCAP	At or above upper critical threshold (going high)	Critical	This voltage is out of the acceptable range. The UltraCapa has been disabled.

N°	Component	Source	Event Description	Severity	Meaning
47	Ultra Capacitor	UC VBOOST	At or below lower critical threshold (going high)	Critical	This voltage is out of the acceptable range.
47	Ultra Capacitor	UC VBOOST	At or above upper critical threshold (going high)	Critical	This voltage is out of the acceptable range.
47	Ultra Capacitor	UC VREF	At or below lower critical threshold (going high)	Critical	This voltage is out of the acceptable range.
47	Ultra Capacitor	UC VREF	At or above upper critical threshold (going high)	Critical	This voltage is out of the acceptable range.
48	Ultra capacitor	UC Failure	Battery failed	Critical	A fault has been detected on the UltraCapa (overvoltage, UVLO or charger timeout)
49	Ultra Capacitor	UC Failure	Battery failed	Return to OK	The Ultra Capacitor is now OK
50	Ultra capacitor	UC Power Outage	State asserted	Information	A Power Outage occurs
51	All	All	All	Unspecified	All events are picked up

Table A-1. Predefined Event Filters

A.2. System Event Log (SEL) Messages

This appendix lists System Event Log (SEL) messages and explains actions to recover, where applicable. It includes the following topics:

Note The following topics list the entirety of the messages that can be recorded in the SEL, regardless of the server model. Entries may not be relevant to your system.

A.2.1. SEL Messages: External Environment

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

Description	The external temperature is above the defined threshold. By default a power off has been executed.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	22.
Actions	Check environmental conditions (fan, air conditioning).
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The external temperature is now OK
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Ambient Temperature: At or above upper non-critical threshold (going high)

Description	The external temperature is above the non-critical threshold.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning).
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Ambient Temperature: At or above upper non-critical threshold (going high)

Description	The external temperature is now OK
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.2. SEL Messages: Power System Board

ACPI Pwr State: S0/G0 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 Alerts, on page 6-47.

ACPI Pwr State: S4/S5 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 Alerts, on page 6-47.

A.2.3. SEL Messages: Sub-chassis

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 Alerts, on page 6-47.

Sub-Chassis: General chassis intrusion

Description	The enclosure is opened.
Severity	Critical.
Direction	Assertion.
Filter Number	35.
Actions	Close the enclosure.
Comments	Notice that there is no deassertion event. For more information about filters, see Configuring Alerts, on page 6-47.

Sub-Chassis: General chassis intrusion

Description	The enclosure is now closed.
Severity	Return to OK.
Direction	Assertion.
Filter Number	36.
Actions	None.
Comments	Notice that there is no deassertion event. For more information about filters, see Configuring Alerts, on page 6-47.

A.2.4. SEL Messages: Power Supply

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

A.2.5. SEL Messages: Power Unit

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 Alerts, on page 6-47.

Pwr Redundancy: Redundancy lost

Description	Two power supplies are 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 Alerts, on page 6-47.

Pwr Redundancy: Non redundant. Sufficient resources from insufficient resources

Description	Two power supplies are 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

Pwr Consumption: Power Consumption Level

Description	This event does not appear in the System Event Log (SEL)
Severity	Information.
Direction	Assertion.
Filter Number	40.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.6. SEL Messages: ILB

ILB 0.9V 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 Alerts, on page 6-47.

ILB 0.9V 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

ILB 0.9V S MNG: 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 Alerts, on page 6-47.

ILB 0.9V S MNG: 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 Alerts, on page 6-47.

ILB 0.9V XDP: 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 Alerts, on page 6-47.

ILB 0.9V XDP: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

ILB 1.1V 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 Alerts, on page 6-47.

ILB 1.2V IB: 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 Alerts, on page 6-47.

ILB 1.2V IB: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

ILB 1.8V XDP: 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 Alerts, on page 6-47.

ILB 1.8V XDP: 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 Alerts, on page 6-47.

ILB 2.5V IB: 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 Alerts, on page 6-47.

ILB 2.5V IB: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

ILB 5V S 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 Alerts, on page 6-47.

ILB 5V S 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The ILB temperature is higher than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

ILB Temperature: At or above higher 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 Alerts, on page 6-47.

A.2.7. SEL Messages: MTB/MXB

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

MTB/MXB 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 Alerts, on page 6-47.

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

Description	The MTB/MXB temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The MTB/MXB temperature is higher than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The MTB/MXB temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The MTB/MXB temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.8. SEL Messages: Processor

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

Proc_X: Processor automatically throttled

Description	PROC_X runs slowly to limit temperature or power consumption.
Severity	Critical.
Direction	Assertion.
Filter Number	44.
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 Alerts, on page 6-47.

Proc_X: Processor automatically throttled

Description	PROC_X runs normally.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	16.
Actions	None.
Comments	X=0 to 3. For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

PX 1.8V: 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 Alerts, on page 6-47.

PX 1.8V MB0: 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 Alerts, on page 6-47.

PX 1.8V MB0: 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 Alerts, on page 6-47.

PX 1.8V MB1: 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 Alerts, on page 6-47.

PX 1.8V MB1: 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 Alerts, on page 6-47.

PX 3.3V CHAB: 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 Alerts, on page 6-47.

PX 3.3V CHAB: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

PX 3.3V CPU: 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 Alerts, on page 6-47.

PX 3.3V CPU: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

PX VCACHE: 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 Alerts, on page 6-47.

PX VCACHE: 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 Alerts, on page 6-47.

PX VCORE: 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 Alerts, on page 6-47.

PX VCORE: 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 Alerts, on page 6-47.

PX VIO: 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 Alerts, on page 6-47.

PX VIO: 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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

A.2.9. SEL Messages: Fan Device / Cooling Unit

FANPR_X Redund: Fan pair_X Fully redundant

Description	Both of the fans in the fan pair are up and running.
Severity	Information.
Direction	Assertion.
Filter Number	17.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

FANPR_X Redund: Fanpair_X Redundancy lost

Description	Only one fan in the fan pair is up and running.
Severity	Non-critical.
Direction	Assertion.
Filter Number	18.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

FANPR_X Redund: Fanpair_X Non redundant: Insufficient resources

Description	No fans are working in the fan pair.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	19.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

FAN_Y Presence: Device removed / Device absent

Description	In the fan pair #X, the fan #Y 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	For more information about filters, see Configuring Alerts, on page 6-47.

FAN_Y Presence: Device inserted / Device present

Description	In the fan pair #X, the fan #Y is (now) present.
Severity	Return to OK.
Direction	Assertion.
Filter Number	21.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	In the fan pair #X, the fan #Y speed is lesser than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	In the fan pair #X, the fan #Y speed is now at normal speed.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

FANUNIT_X Presence: Device removed / Device absent

Description	The fan unit #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	For more information about filters, see Configuring Alerts, on page 6-47.

FANUNIT_X Presence: Device inserted / Device present

Description	The fan unit #X is (now) present.
Severity	Return to OK.
Direction	Assertion.
Filter Number	21.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	In the fan unit# X, the rotor #Y speed is lesser than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	In the fan unit #X, the rotor#Y speed is now at normal speed.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.10. SEL Messages: PDB

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	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The PDB temperature is higher than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

PDB Temperature: At or above higher 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 Alerts, on page 6-47.

A.2.11. SEL Messages: Ultra Capacitor

UC Failure: Battery failed

Description	A fault has been detected on the UltraCapa (overvoltage, UVLO or charger timeout).
Severity	Critical.
Direction	Assertion.
Filter Number	48.
Actions	Change the Ultra Capa device and the PDBL board.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC Failure: Battery failed

Description	The UltraCapa is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	49.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC Availability: Device Disabled

Description	The UltraCapa has been disabled due to other error or operator request.
Severity	Information.
Direction	Assertion.
Filter Number	50.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC Availability: Device Enabled

Description	The UltraCapa is now available.
Severity	Information.
Direction	Assertion.
Filter Number	50.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The ultra capa temperature is lower than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Ultra Capa Temperature: At or above higher critical threshold (going high)

Description	The ultra capa temperature is higher than the minimum required.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The ultra capa temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Ultra Capa Temperature: At or above higher critical threshold (going high)

Description	The ultra capa temperature is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC Power Outage: State asserted

Description	A Power Outage occurs.
Severity	Information.
Direction	Assertion.
Filter Number	50.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 3.3V At or below lower critical threshold (going low)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 3.3V : At or above higher critical threshold (going high)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 3.3V : At or below lower critical threshold (going low)

Description	This voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 3.3V: At or above higher critical threshold (going high)

Description	This voltage is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 5V At or below lower critical threshold (going low)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 5V : At or above higher critical threshold (going high)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 5V : At or below lower critical threshold (going low)

Description	This voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 5V: At or above higher critical threshold (going high)

Description	This voltage is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 12V At or below lower critical threshold (going low)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 12V : At or above higher critical threshold (going high)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 12V : At or below lower critical threshold (going low)

Description	This voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC 12V: At or above higher critical threshold (going high)

Description	This voltage is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VCAP: At or above upper non-recoverable threshold (going high)

Description	Over voltage on the ultra capa VCAP voltage.
Severity	Non recoverable.
Direction	Assertion.
Filter Number	45.
Actions	The Module has been powered off and excluded. The power on will be refused. For safety reasons, disconnect AC power.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VCAP: At or above upper critical threshold (going high)

Description	Over voltage on the ultra capa VCAP voltage.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	The Module has been powered off and excluded. The power on will be refused. For safety reasons, disconnect AC power.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VCAP: At or above upper non-recoverable threshold (going high)

Description	The UltraCapa VCAP voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	46.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VCAP: At or above upper critical threshold (going high)

Description	The Ultra Capa VCAP voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VBOOST : At or below lower critical threshold (going low)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VBOOST : At or above higher critical threshold (going high)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VBOOST : At or below lower critical threshold (going low)

Description	This voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VBOOST : At or above higher critical threshold (going high)

Description	This voltage is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VREF : At or below lower critical threshold (going low)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VREF : At or above higher critical threshold (going high)

Description	This voltage is out of the acceptable range.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VREF : At or below lower critical threshold (going low)

Description	This voltage is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

UC VREF : At or above higher critical threshold (going high)

Description	This voltage is now OK.
Severity	Return to OK
Direction	Deassertion.
Filter Number	23.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.12. SEL Messages: LCP

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	47.
Actions	Check environmental conditions (fan, air conditioning).If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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

Description	The LCP temperature is higher than the maximum allowed.
Severity	Critical.
Direction	Assertion.
Filter Number	47.
Actions	Check environmental conditions (fan, air conditioning).If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

LCP Temperature: At or above higher 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 Alerts, on page 6-47.

A.2.13. 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	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Chipset Error: Transition to Non-Recoverable

Description	A chipset uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	24.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Chipset Error: Transition to OK

Description	Return to normal temperature.
Severity	Return to OK.
Direction	Assertion.
Filter Number	37.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Chipset Error: Informational

Description	A chipset correctable error has occurred.
Severity	Information.
Direction	Assertion.
Filter Number	39.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Processor Error: Transition to Critical from less severe

Description	A processor uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	25.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

Processor Error: Transition to Non-Recoverable

Description	A processor uncorrectable error has occurred.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	25.
Actions	If the problem persists, contact your Customer Service Engineer.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

Version Change: Firmware or software change

Description	BIOS recovery.
Severity	Information.
Direction	Assertion.
Filter Number	41.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

System Event

Description	A system boot event has occurred Event data 2 [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 Power Steps: BMC, on page A-58 and Power Steps: SMC, on page A-60 Event data 3 [7:6] Sequence nb 0 Power OFF sequence 1 Power ON sequence 2 Reset sequence 3 RFU [5:0] Error nb : 0-63 see Operation to Recover in the *bullx S6030 Service Guide* or *bullx S6010 Service Guide*.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	29.
Actions	See Operation to Recover in the *bullx S6030 Service Guide* or *bullx S6010 Service Guide*.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Event: Undetermined system hardware failure

Description	Overvoltage on the UltraCapa VCAP voltage. The Module has been powered off and excluded. The power on will be refused.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	29.
Actions	For safety reasons, disconnect AC power.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

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 Alerts, on page 6-47.

Platform Security Violation Attempt: Out-of-band access password violation

Description	An out of band IPMI access failed due to password violation.
Severity	Non-critical.
Direction	Assertion.
Filter Number	31.
Actions	Information.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Event: Entry added to Auxiliary Log

Description	A corrected machine error has been logged by BIOS in the non-volatile area.
Severity	Information.
Direction	Assertion.
Filter Number	32.
Actions	Analyze the log with the iCare Console.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Event: Entry added to Auxiliary Log

Description	An uncorrected machine error has been logged by BIOS in the non-volatile area.
Severity	Critical.
Direction	Assertion.
Filter Number	33.
Actions	Analyze the log with the iCare Console.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Event: Entry added to Auxiliary Log

Description	A fatal machine error has been logged by BIOS in the non-volatile area.
Severity	Non-recoverable.
Direction	Assertion.
Filter Number	34.
Actions	Analyze the log with the iCare Console.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Boot Init: Initiated by Hard Reset

Description	System Boot init.
Severity	Information.
Direction	Assertion.
Filter Number	42.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Boot Init: OS / Run-time Software Initiated (Hard/Warm) Reset

Description	System boot init.
Severity	Information.
Direction	Assertion.
Filter Number	42.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

System Boot Init: System Restart

Description	System boot init.
Severity	Information.
Direction	Assertion.
Filter Number	42.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

OS Stop: OS Graceful Stop

Description	OS stop.
Severity	Information.
Direction	Assertion.
Filter Number	43.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

OS Stop: OS Graceful Shutdown

Description	OS stop.
Severity	Information.
Direction	Assertion.
Filter Number	43.
Actions	None.
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.14. SEL Messages: Memory

DIMM_X: Correctable ECC threshold reached

Description	Correctable ECC threshold reached on DIMM_X
Severity	Warning.
Direction	Assertion.
Filter Number	38.
Actions	If the problem persists, contact your Customer Service Engineer
Comments	For more information about filters, see Configuring Alerts, on page 6-47.

A.2.15. Power Steps: BMC

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
Power ON in normal mode	0	[BMC PWR] Build partition composition structure	[BMC PWR] Build partition composition structure
	1	[BMC PWR] Powering on drawer	[BMC PWR] Powering on drawer
	2	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	3	[BMC PWR] Update hw presence in SMC	[BMC PWR] Update hw presence in SMC
	4	[BMC PWR] Init scratchpad registers	[BMC PWR] Init scratchpad registers
	5	[BMC PWR] Start IPMI watchdog timer	[BMC PWR] Start IPMI watchdog timer
	6	[BMC PWR] Resume BIOS initialization	[BMC PWR] Resume BIOS initialization
	7	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Power ON light standby	0	[BMC PWR] Powering on light standby	[BMC PWR] Powering on light standby
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Power ON deep standby	0	[BMC PWR] Powering on deep standby	[BMC PWR] Powering on deep standby
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
Power ON in north bios mode	0	[BMC PWR] Build partition composition structure	[BMC PWR] Build partition composition structure
	1	[BMC PWR] Powering on drawer in BIOS north mode	[BMC PWR] Powering on drawer in BIOS north mode
	2	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	3	[BMC PWR] Set ACPI legacy on state	[BMC PWR] Set ACPI legacy on state
	4		[BMC PWR] Init scratchpad registers
	5		[BMC PWR] Start IPMI watchdog timer
	6		[BMC PWR] Resume BIOS initialization
	7		[BMC PWR] Set ACPI legacy on state

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
Power OFF in normal mode	0	[BMC PWR] Stop IPMI watchdog timer	[BMC PWR] Stop IPMI watchdog timer
	1	[BMC PWR] Powering off drawer	[BMC PWR] Powering off drawer
	2	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	3	[BMC PWR] Set ACPI legacy off state	[BMC PWR] Set ACPI legacy off state
Power OFF light standby	0	[BMC PWR] Powering off drawer	[BMC PWR] Powering off drawer
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Set ACPI legacy off state	[BMC PWR] Set ACPI legacy off state
Power OFF deep standby	0	[BMC PWR] Powering off deep standby	[BMC PWR] Powering off deep standby
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Set ACPI legacy off state	[BMC PWR] Set ACPI legacy off state
Power OFF in north bios mode	0	[BMC PWR] Powering off drawer in BIOS north mode	[BMC PWR] Powering off drawer in BIOS north mode
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Set ACPI legacy off state	[BMC PWR] Set ACPI legacy off state

Sequence nb = 2	Step	Action (MTB board)	Action (MXB board)
Warm reset	0	[BMC PWR] Reset drawer	[BMC PWR] Reset drawer
	1	[BMC PWR] Receiving SMC answer	[BMC PWR] Receiving SMC answer
	2	[BMC PWR] Start IPMI watchdog timer	[BMC PWR] Start IPMI watchdog timer
	3	[BMC PWR] Resume BIOS initialization	[BMC PWR] Resume BIOS initialization

A.2.16. Power Steps: SMC

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
Power ON in normal mode	0	[SMC PWR] LCP Display powering on	[SMC PWR] LCP Display powering on
	1	[SMC PWR] Check ILBC is loaded	[SMC PWR] Check ILBC is loaded
	2	[SMC PWR] Check power redundancy	[SMC PWR] Power on 12v power supplies
	3	[SMC PWR] Power on 12v power supplies	[SMC PWR] Power on fans
	4	[SMC PWR] Power on fans	[SMC PWR] Check ADM1069 firmwares
	5	[SMC PWR] Check ADM1069 firmwares	[SMC PWR] Load MXBC FPGA
	6	[SMC PWR] Load MTBC FPGA	[SMC PWR] Check MXBC is loaded
	7	[SMC PWR] Check MTBC is loaded	[SMC PWR] Get module configuration
	8	[SMC PWR] Set FPGA reset mode	[SMC PWR] Set FPGA reset mode
	9	[SMC PWR] Power on light standby voltages	[SMC PWR] Set FPGA CPU modes
	10	[SMC PWR] Light standby condition is true	[SMC PWR] Enable clock drivers
	11	[SMC PWR] Pulse PWRBTN signal	[SMC PWR] Power on light standby voltages
	12	[SMC PWR] Get module configuration	[SMC PWR] Light standby condition is true
	13	[SMC PWR] Set FPGA CPU modes	[SMC PWR] Pulse PWRBTN signal
	14	[SMC PWR] Power on ILBC main voltages	[SMC PWR] Power on main voltages
	15	[SMC PWR] Power on MTBC main voltages	[SMC PWR] Main power condition is true
	16	[SMC PWR] Main power condition is true	[SMC PWR] LCP Display BIOS init
	17	[SMC PWR] Enable clock drivers	[SMC PWR] Check PLTRST signal deasserted
	18	[SMC PWR] Assert XDP power good	[SMC PWR] Chipset access condition is true
	19	[SMC PWR] Chipset access condition is true	[SMC PWR] Check processor boot mode
	20	[SMC PWR] Assert IOH power good	[SMC PWR] Light on LCP green led
	21	[SMC PWR] LCP Display BIOS init	[SMC PWR] Drawer is powered on
	22	[SMC PWR] Assert ICH power good	[SMC PWR] Monitoring condition is true

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
	23	[SMC PWR] Check PLTRST signal deasserted	[SMC PWR] Set OS running
	24	[SMC PWR] Chipset access condition is true	
	25	[SMC PWR] Check processor boot mode	
	26	[SMC PWR] Light on LCP green led	
	27	[SMC PWR] Drawer is powered on	
	28	[SMC PWR] Monitoring condition is true	
	29	[SMC PWR] Set OS running	

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
Power ON deep standby	0	[SMC PWR] Drawer is powered on	[SMC PWR] Drawer is powered on

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
Power ON light standby	0	[SMC PWR] LCP Display powering on	[SMC PWR] LCP Display powering on
	1	[SMC PWR] Check ILBC is loaded	[SMC PWR] Check ILBC is loaded
	2	[SMC PWR] Power on 12v power supplies	[SMC PWR] Power on 12v power supplies
	3	[SMC PWR] Power on fans	[SMC PWR] Power on fans
	4	[SMC PWR] Load MTBC FPGA	[SMC PWR] Load MXBC FPGA
	5	[SMC PWR] Check MTBC is loaded	[SMC PWR] Check MXBC is loaded
	6	[SMC PWR] Set FPGA reset mode	[SMC PWR] Set FPGA reset mode
	7	[SMC PWR] Power on light standby voltages	[SMC PWR] Power on light standby voltages
	8	[SMC PWR] Light standby condition is true	[SMC PWR] Light standby condition is true
	9	[SMC PWR] Light on LCP green led	[SMC PWR] Light on LCP green led
	10	[SMC PWR] LCP Display light standby	[SMC PWR] LCP Display light standby
	11	[SMC PWR] Drawer is powered on	[SMC PWR] Drawer is powered on

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
Power ON in north bios mode	0	[SMC PWR] LCP Display powering on	[SMC PWR] LCP Display powering on
	1	[SMC PWR] Check ILBC is loaded	[SMC PWR] Check ILBC is loaded
	2	[SMC PWR] Power on 12v power supplies	[SMC PWR] Power on 12v power supplies
	3	[SMC PWR] Power on fans	[SMC PWR] Power on fans
	4	[SMC PWR] Check ADM1069 firmwares	[SMC PWR] Check ADM1069 firmwares
	5	[SMC PWR] Load MTBC FPGA	[SMC PWR] Load MXBC FPGA
	6	[SMC PWR] Check MTBC is loaded	[SMC PWR] Check MXBC is loaded
	7	[SMC PWR] Set FPGA reset mode	[SMC PWR] Get module configuration
	8	[SMC PWR] Power on light standby voltages	[SMC PWR] Set FPGA reset mode
	9	[SMC PWR] Light standby condition is true	[SMC PWR] Set FPGA CPU modes
	10	[SMC PWR] Pulse PWRBTN signal	[SMC PWR] Enable clock drivers
	11	[SMC PWR] Get module configuration	[SMC PWR] Power on light standby voltages
	12	[SMC PWR] Set FPGA CPU modes	[SMC PWR] Light standby condition is true
	13	[SMC PWR] Power on ILBC main voltages	[SMC PWR] Pulse PWRBTN signal
	14	[SMC PWR] Power on MTBC main voltages	[SMC PWR] Power on main voltages
	15	[SMC PWR] Main power condition is true	[SMC PWR] Main power condition is true
	16	[SMC PWR] Enable clock drivers	[SMC PWR] LCP Display BIOS init
	17	[SMC PWR] Assert XDP power good	[SMC PWR] Check PLTRST signal deasserted
	18	[SMC PWR] Assert processors power good	[SMC PWR] Chipset access condition is true
	19	[SMC PWR] Assert IOH power good	[SMC PWR] Check processor boot mode
	20	[SMC PWR] LCP Display BIOS update	[SMC PWR] Light on LCP green led
	21	[SMC PWR] Assert ICH power good	[SMC PWR] Drawer is powered on
	22	[SMC PWR] Check PLTRST signal deasserted	[SMC PWR] Monitoring condition is true
	23	[SMC PWR] Chipset access condition is true	[SMC PWR] Set OS running

Sequence nb = 1	Step	Action (MTB board)	Action (MXB board)
	24	[SMC PWR] Check processor boot mode	
	25	[SMC PWR] Light on LCP green led	
	26	[SMC PWR] Drawer is powered on	

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
Power OFF in normal mode	0	[SMC PWR] LCP Display powering off	[SMC PWR] LCP Display powering off
	1	[SMC PWR] Reset OS running	[SMC PWR] Reset OS running
	2	[SMC PWR] Monitoring condition is false	[SMC PWR] Monitoring condition is false
	3	[SMC PWR] Chipset access condition is false	[SMC PWR] Chipset access condition is false
	4	[SMC PWR] Deassert ICH power good	[SMC PWR] Main power condition is false
	5	[SMC PWR] Deassert IOH power good	[SMC PWR] Power off main voltages
	6	[SMC PWR] Deassert processors power good	[SMC PWR] Light standby condition is false
	7	[SMC PWR] Deassert XDP power good	[SMC PWR] Power off light standby voltages
	8	[SMC PWR] Disable clock drivers	[SMC PWR] Disable clock drivers
	9	[SMC PWR] Main power condition is false	[SMC PWR] Reset FPGA reset mode
	10	[SMC PWR] Power off MTBC main voltages	[SMC PWR] Power off fans
	11	[SMC PWR] Power off ILBC main voltages	[SMC PWR] Power off 12V power supplies
	12	[SMC PWR] Light standby condition is false	[SMC PWR] Blink LCP green led
	13	[SMC PWR] Power off light standby voltages	[SMC PWR] Drawer is powered off
	14	[SMC PWR] Reset FPGA reset mode	
	15	[SMC PWR] Power off fans	
	16	[SMC PWR] Power off 12v power supplies	
	17	[SMC PWR] Blink LCP green led	
	18	[SMC PWR] Drawer is powered off	

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
Power OFF light standby	0	[SMC PWR] LCP Display powering off	[SMC PWR] LCP Display powering off
	1	[SMC PWR] Light standby condition is false	[SMC PWR] Light standby condition is false
	2	[SMC PWR] Power off light standby voltages	[SMC PWR] Power off light standby voltages
	3	[SMC PWR] Reset FPGA reset mode	[SMC PWR] Reset FPGA reset mode
	4	[SMC PWR] Power off fans	[SMC PWR] Power off fans
	5	[SMC PWR] Power off 12v power supplies	[SMC PWR] Power off 12v power supplies
	6	[SMC PWR] Blink LCP green led	[SMC PWR] Blink LCP green led
	7	[SMC PWR] Drawer is powered off	[SMC PWR] Drawer is powered off

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
Power OFF deep standby	0	[SMC PWR] Drawer is powered off	[SMC PWR] Drawer is powered off

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
Power OFF in north bios mode	0	[SMC PWR] LCP Display powering off	[SMC PWR] LCP Display powering off
	1	[SMC PWR] Chipset access condition is false	[SMC PWR] Reset OS running
	2	[SMC PWR] Deassert ICH power good	[SMC PWR] Monitoring condition is false
	3	[SMC PWR] Deassert IOH power good	[SMC PWR] Chipset access condition is false
	4	[SMC PWR] Deassert processors power good	[SMC PWR] Main power condition is false
	5	[SMC PWR] Deassert XDP power good	[SMC PWR] Power off main voltages
	6	[SMC PWR] Disable clock drivers	[SMC PWR] Light standby condition is false
	7	[SMC PWR] Main power condition is false	[SMC PWR] Power on light standby voltages
	8	[SMC PWR] Power off MTBC main voltages	[SMC PWR] Disable clock drivers
	9	[SMC PWR] Power off ILBC main voltages	[SMC PWR] Reset FPGA reset mode
	10	[SMC PWR] Light standby condition is false	[SMC PWR] Power off fans
	11	[SMC PWR] Power off light standby voltages	[SMC PWR] Power off 12v power supplies
	12	[SMC PWR] Reset FPGA reset mode	[SMC PWR] Blink LCP green led

Sequence nb = 0	Step	Action (MTB board)	Action (MXB board)
	13	[SMC PWR] Power off fans	[SMC PWR] Drawer is powered off
	14	[SMC PWR] Power off 12v power supplies	
	15	[SMC PWR] Blink LCP green led	
	16	[SMC PWR] Drawer is powered off	

Appendix B. Serial-Over-LAN Console

This appendix explains how to set up and use the Serial-Over-Lan (SOL) Console. It includes the following topics:

B.1. Introducing the SOL Console

The IPMI Serial-Over-Lan (SOL) tool provides access to the system over the management LAN, via the motherboard's embedded management controller (BMC), allowing you to remotely view the text-based console and perform diagnosis and repair tasks such as:

- reconfigure the Operating System or run utilities,
- remotely view boot sequences,
- receive alerts and view messages,
- remotely configure the BIOS.

For further details about SOL Console options, refer to the *ipmitool Guide* delivered on the *Resource & Documentation CD* and the *telnet Guide* delivered with your Operating System.

Note Only one SOL Console can be opened at a time.

Important **SOL requires BIOS Version 01.003.00.014 or higher and Hardware Console Firmware Build Number 1033 or higher.**

There are two methods for accessing the SOL Console:

- **ipmitool** for Linux Operating Systems,
- **telnet** for Linux and Windows Operating Systems.

Important **To be able to use the SOL Console, you must:**

- configure the BIOS,
- set up the required network and SOL permissions from the embedded management controller's (BMC) Hardware Console,
- install the ipmitool / telnet packages (as applicable),
- perform the necessary Operating System configuration tasks. Refer to the documentation delivered with your Operating System for details.

B.2. Using the SOL Console with ipmitool

The **ipmitool command** can be used to connect the SOL Console using a Linux Operating System.

Prerequisites

The BIOS is configured

The required network and SOL permissions are configured on the Hardware Console

The **ipmitool** package is installed

The Operating System is configured

Procedure

This procedure explains how to open and close the SOL Console with the **ipmitool command**.

1. Open a Linux session.
2. Open the SOL Console by running the following command:

```
ipmitool -H <BMC IP address or host name> -I lanplus -U <user> -P <password> sol activate
```

A SOL session screen opens.

3. Press **Enter** to take control of the remote system.
4. Press **<~ ?>** to display **ipmi sol** help.

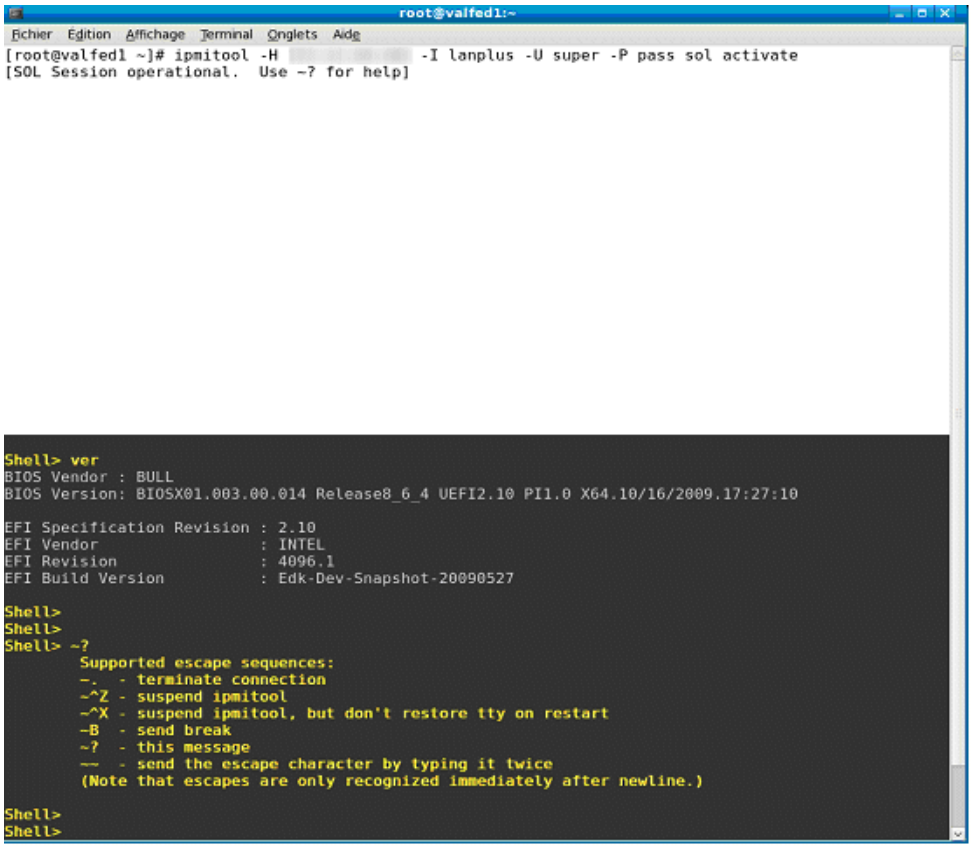


Figure B-1. SOL Console - Launching with ipmitool

5. Close the SOL Console by pressing <~.>.

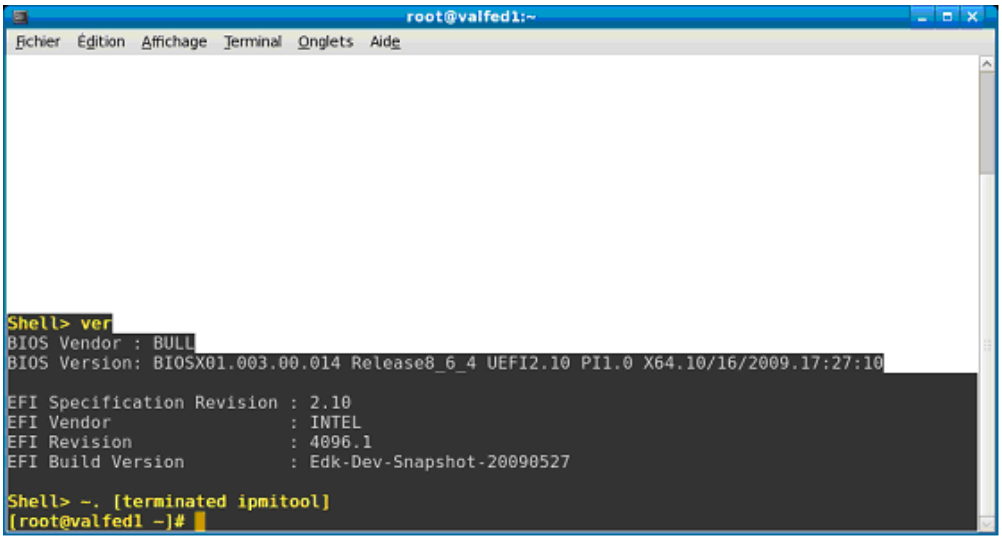


Figure B-2. SOL Console - Closing with ipmitool

B.3. Using the SOL Console with telnet

The **telnet command** can be used to connect the SOL Console using a Linux or Windows Operating System.

Prerequisites

The BIOS is configured

The required network and SOL permissions are configured on the Hardware Console

telnet is installed

The Operating System is configured

Procedure

This procedure explains how to open and close the SOL Console with the **telnet command**.

1. Open a Linux or Windows session.
2. Run the **telnet command** on **Port 23**.

   A telnet session screen opens.
3. Enter the embedded management controller's (BMC) login and password.

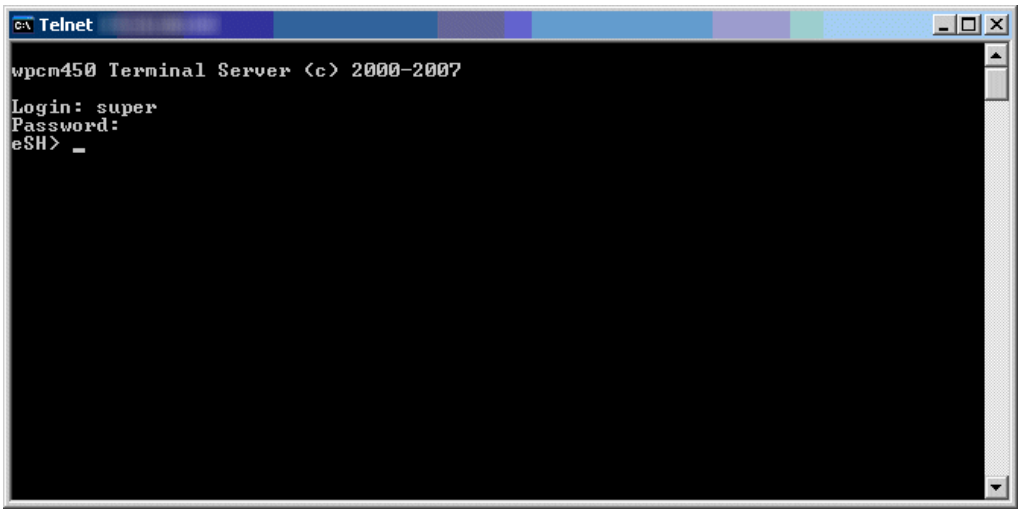


Figure B-3. Telnet session

4. Press <?> to display available commands

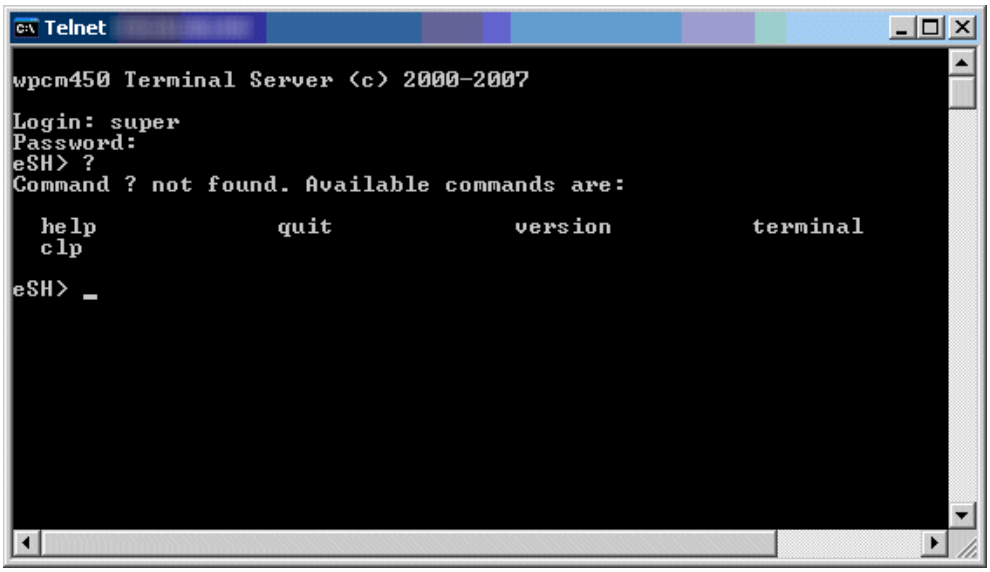


Figure B-4. Telnet commands

5. Type **terminal** and press **Enter** TWICE to open the SOL Console and take control of the remote system.

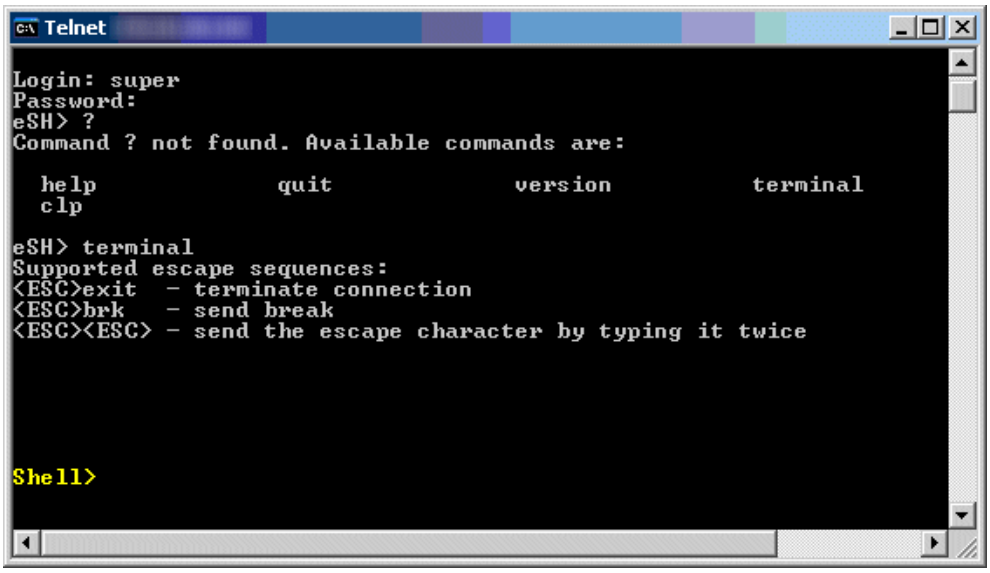


Figure B-5. SOL Console - Launching with telnet

6. _Close the SOL Console by pressing <Esc> and typing **exit** simultaneously.
7. Type **quit** to close the session.

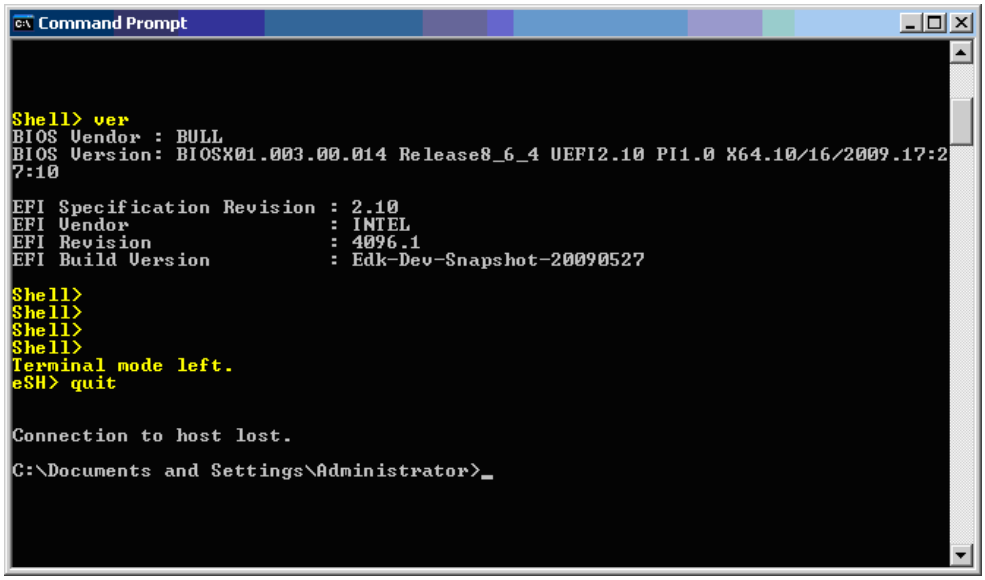


Figure B-6. SOL Console - Closing with telnet

Glossary

A

ABR
Automatic BIOS Recovery.

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.

ADM1069
The ADM1069 Super Sequencer® is a configurable supervisory/ sequencing device that offers a single-chip solution for supply monitoring and sequencing in multiple supply systems.

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. An ARU is also known as a PMU.

ASR
Automatic Server Restart.

ASIC
Application Specific Integrated Circuit.

B

Base Operating System
The Operating System that is booted at initialization.

BCE
Elementary calculation block.

BCEA
ASIC elementary calculation block.

BCEF
FPGA elementary calculation block.

BCS
Bull Coherence Switch. This is the Bull eXternal Node Controller providing 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.

BHC
See Blade Hardware Console.

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.

Blade Hardware Console
Graphical user interface used to access the management software embedded in the blade module.

BMC
Baseboard Management Controller. See Embedded Management Controller.

BOOTP
Network protocol used by a network client to obtain an IP address from a configuration server.

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).

C

Chassis Hardware Console
Graphical user interface used to access the management software embedded in the Chassis Management Module.

CHC
See Chassis Hardware Console.

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.

CMB
Chassis Management Board.

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

CMC
Chassis Management Controller.

CMM
Chassis Management Module.

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

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

CSE
Customer Service Engineer.

D

DES
Data Encryption Standard.

DHCP
Dynamic Host Configuration Protocol.

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.

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.

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.

ESB
Ethernet Switch Board.

ESM
Ethernet Switch Module.

F

FC-LGA
Flip-Chip Land Grid Array.

Flash EPROM
Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store 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.

FPGA
Field Programmable Gate Array.

FQDN
Fully Qualified Domain Name.

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.

G

GPU
Graphical Processing Unit.

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.

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

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.

HPC
High Performance Computing.

HPC Cluster
High Performance Computing Cluster. A group of computers linked together to form a single computer.

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.

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.

iBMC
Integrated Baseboard Management Controller. See Embedded Management Controller.

iCare
The 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 / ILBC
I/O Legacy Board / I/O Legacy Board Controller.

INCA
INtegrated Cluster Architecture.

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

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

JOEM
JTAG Over Ethernet Module.

JTAG
Joint Test Action Group.

K

No entries.

L

LAN
Local Area Network.

LCD
Liquid Crystal Display.

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.

LED
Light Emitting Diode.

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.

M

MAC
Media Access Control.

MCA
A Machine Check Abort exception occurs when an error condition has arisen that requires corrective action.

MESCA
Multiple Environments on a Scalable Csi-based Architecture.

MIB
Management Interface Base.

MIMD
Multiple Instruction Multiple Data

MMX
MultiMedia eXtensions.

MTB/MTBC
Memory and Tukwila Board / Memory and Tukwila Board Controller.

MTBF
Mean Time Between Failure.

Multicore
Presence of two or more processors on a single chip.

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.

MXB/MXBC
Memory and Xeon Board / Memory and Xeon Board Controller.

N

Nehalem
NEHALEM Intel Xeon Processor (8 cores per die).

NFS
Network File System.

NIC
Network Interface Controller.

NUMA
Non Uniform Memory Access.

NVRAM
Non-Volatile Random Access Memory.

O

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.

OPMA
Open Platform Management Architecture.

P

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.

Platform Event
A platform event is an event that originates directly from platform firmware (BIOS) or platform hardware, independently of the state of the Operating System or System Mangement Hardware.

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.

PET
The Platform Event Trap format is used for sending a platform event in an SNMP Trap. See Platform Event.

PIROM
The 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.

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.

POST
Power On Self Test.

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.

PSMI
Power Supply Management Interface.

PSU
Power Supply Unit. Sub-assembly of the Power Supply Module.

PSWB
PCI SWitch Board.

PSWM
PCI SWitch Module.

PWM
Pulse Width Modulation.

Q

QDR
Quad Data Rate. Communication signalling technique where data is transmitted at four points in the clock cycle.

QPI
Quick Path Interconnect. High-speed point-to-point Intel interface, used to interconnect processors and I/O Hubs, and optionally node controllers (BCS).

QSB
Quad Switch Board.

QSFP
Quad Small Form-factor Pluggable. Low-power interconnect technology.

QSMB
Quad Switch Module. InfiniBand Switch.

R

RADIUS
Remote Authentication Dial-In User Service.

RAS
Reliability, Availability, Serviceability.

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.

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.

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.

SHC
See Server 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.

SMTP
Simple Mail Transfer Protocol.

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.

SoC
System on Chip.

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.

SO-DIMM
Small Outline Dual In-line Memory.

SR
Scratch Register. Internal registers of both the Tukwila processor and the I/O Hub used as scratch area.

SSH
Secured Shell.

SSL
Secure Socket Layer.

T

TELNET
TELecommunication NETwork. Protocol used on the Internet or Local Area Networks to provide a bidirectional interactive communications facility.

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 socket).

U

UCM
Ultra Capacitor Module.

UVLO
Under Voltage Latch Output.

V

VMM
Virtual Machine Monitor.

W

WOL
Wake On Lan. 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).

XNC
External Node Controller. See BCS.

Y

No entries.

Z

No entries.

Index

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

Bull Cedoc
357 avenue Patton
BP 20845
49008 Angers Cedex 01
FRANCE

REFERENCE
86 A1 50FD 06