bullx blade system Chassis Hardware Console

User's Guide

extreme computing

BULL

extreme computing

bullx blade system
Chassis Hardware Console
User's Guide

Hardware

October 2010

Trademarks and Acknowledgements

We acknowledge the rights of the proprietors of the 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

bullx blade system Chassis Hardware Console - - User's Guide

Preface

This guide explains how to use the Chassis Hardware Console (CHC) to manage your bullx blade system.

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

Intended readers

This guide is intended for use by blade 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

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.

- *bullx blade system Installation Guide*, 86 A1 48FB 03

  explains how to install the *bullx blade system*. This guide is intended for use by the qualified support personnel.

- *bullx blade system Maintenance and Troubleshooting Guide*, 86 A7 51FB 03

  explains how to maintain, service, and upgrade the bullx blade system. This guide is intended for use by qualified support personnel.

- *bullx B500 Blade Hardware Console User's Guide*, 86 A1 49FB 03

  explains how to use the bullx B500 compute blades. This guide is intended for use by Customer Administrators and Operators.

- *bullx B505 Blade Hardware Console User's Guide*, 86 A1 49FE 01

  explains how to use the bullx B505 accelerator blades. This guide is intended for use by Customer Administrators and Operators.

The illustrations in this document may differ slightly from the hardware received.

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 60950-1 USA
- EN 60950-1 international
- CSA 60950-1 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 is responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

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

An FCC regulatory label is affixed to the equipment.

Canadian compliance statement (Industry Canada)

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

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

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

- ICES-003
    - NMB-003

Laser compliance notice

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

For Your Safety, this manual contains important information, required to operate the server safely. Thoroughly review the information in this manual before using the server.

Use the following safety guidelines to ensure your personal safety and to help protect your server from potential damage. Throughout this guide, blocks of text may be accompanied by an icon which needs to be followed for your safety.

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 an action that could cause damage to a program, device, system, or data. A Caution notice may also indicate the presence of a hazard that has the potential of causing moderate or minor personal injury.

Read the installation instructions before connecting the system to the power source. Hazardous current and energy levels are present in areas indicated by this label. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact service technician.

CAUTION

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key or other means of security. Only trained and qualified personnel should be allowed to install, replace, or service this equipment.

- This equipment must be grounded. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available

- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating

- Use only power cables that are approved for use in the respective country. The power cable must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product

- If any of the following conditions occur, unplug the equipment from the electrical outlet and replace the part or contact your trained service technician:

  – The power cable, extension cable, or plug is damaged

  – An object has fallen into the equipment

  – The equipment has been exposed to water

  – The equipment does not operate correctly when you follow the operating instructions

- Allow the equipment to cool before removing covers or touching internal components

- Suitable disconnect device must be provided as part of the building installation. The purpose of the disconnect device is to provide an easy and accessible means for removing power from the product for servicing

- Opening or removing covers that are marked with the triangle symbol with a caution mark may expose you to risk of electrical shock. Components inside these compartments should be serviced only by a trained service technician

- Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label

- Hazardous energy is present when the blade is connected to the power source. Always replace the blade cover before installing the blade

- When removing the accelerator blade / compute blade power supply, dummy blade, filler covers, do not insert your hand into the open slots. Doing so may cause electric shock

- Do not operate your equipment with any filler covers removed

- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components

- Do not use top blade handle to lift the blade chassis. These are used only to install and remove the blade only

- Do not restrict airflow into the equipment by blocking any vents or air intakes

- Cleaning: Unplug your system from wall outlet before cleaning

- Do not spill food or liquids on your system components. Never operate the product in a wet environment

⚠️ **CAUTION**
When connecting or disconnecting power to hot-pluggable power supplies observe the following guidelines:

- **Install the power supply before connecting the power cable to the power supply**

- Unplug the power cable before removing the power supply

- If the equipment has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies to reduce shock hazard

- Never open the power supply module for any reason

- The power supplies in your system may produce high voltages and energy hazards. Only trained service technicians are authorized to remove the covers and access any of the components inside the system

⚠️ **CAUTION**
Incorrectly installing a battery or using an incompatible battery may increase the risk of fire or explosion. Replace the battery only with the same or equivalent type recommended by the manufacturer, carefully following installation instructions. Dispose of used batteries properly. Handle batteries carefully. Do not disassemble, crush, or puncture batteries.

Electrical safety

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.

CAUTION

For Europe, connect the plug through Pluggable type B inlet only.
Do not employ Pluggable type A type Plug in European market. Replacement of power cord shall be done only by Service person and the same type cord and plug configuration shall be utilized.

CAUTION

The following must be applied for, in end-system:
Pluggable Type A Equipment, is only accepted where the installation fuse is limited to 16 A; due to the mains fuse rating of 25 A, the following must be applied for:
- Connection through Pluggable Type B inlet
- Permanent Connection

CAUTION

The UCM installation and removal operation should be handled by a trained service technician. The module has to be completely discharged before removal.

Laser safety information

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 Electro technical 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

CAUTION

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.

Chapter 1. Getting to know the system

This chapter gives an overview of blade system architecture and a high-level description of each of the system components.

The bullx blade system is a high-density server system providing cluster architecture. It can be equipped with eighteen bullx B500 compute blades / nine bullx B505 accelerator blades, making it ideally suited for extreme computing cluster environments requiring a large number of high-performance servers in a small space. The bullx blade chassis provides common resources that are shared by the bullx B500 compute blades / bullx B505 accelerator blades, such as power, cooling, system management, network connections, and I/O switch. The use of common resources reduces blade size, minimizes cabling, and also reduces the time / likelihood of idle resources.

Performance, ease-of-use, reliability, and expansion capabilities were key considerations during the design of the bullx blade system. These design features make it possible for you to customize system hardware to meet the needs of today, while providing flexible expansion capabilities for the future.

This guide provides information on how to:

- install the system

- connect and test the system

Six bullx blade systems can be simultaneously housed in a 42U cabinet. Each bullx blade system comprises the following key hardware components, some of which are optional:

- Up to eighteen dual processor (DP) bullx B500 compute blades (NCB), with two processors, two fans for cooling, and an HDD/SDD disk.

- Up to nine bullx B505 accelerator blades (GPU), with two processors, two Nvidia cards and four fans for cooling.

- A Quad Switch Module (QSM).

- Optional Ultra Capacitor Module (UCM).

- A Chassis Management Module (CMM).

- An optional Ethernet Switch Module (ESM).

- A Local Control Panel (LCP) providing an LCD display and power and reset buttons.

- Up to four Power Supply Unit modules (PSU) providing N+1 power redundancy.

- Two fan blades to cool the QSM, CMM, and ESM modules.

Serial and part numbers are indicated on a label on the top of the chassis. The following table can be used to record system information.
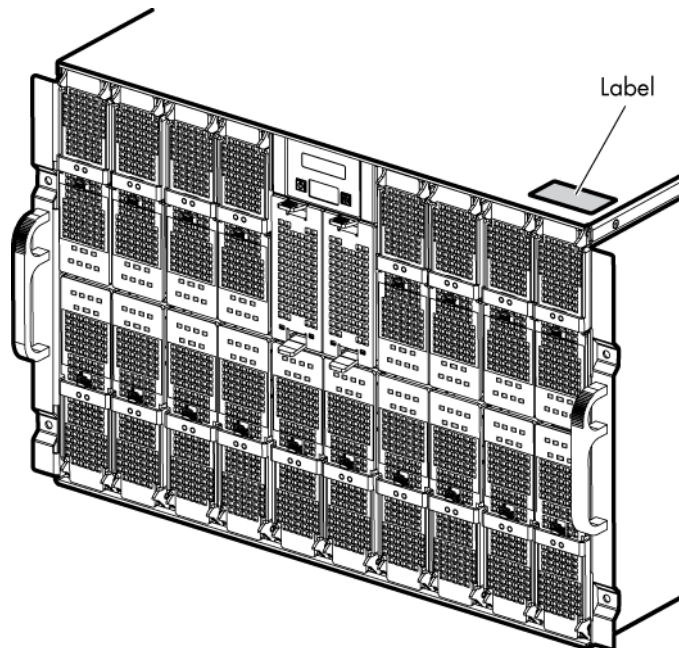
	bullx blade system
Product Name	
Model Type	
Serial Number (XAN)	

Figure 1-1.   System information record

1.1   What the blade system offers

The blade system design takes advantage of advancements in server technology. It houses up to eighteen functionally separate compute blades or nine accelerator blades and their shared resources in a single blade chassis. The blade system combines:

Innovative technology
Proven innovative technologies to build powerful, scalable and reliable Intel®-processor-based servers.

Expansion capabilities
Compute blades / accelerator blades can be added to the blade system as needed. The system can be equipped with a maximum of eighteen compute blades / nine accelerator blades.

Hot-swap / Hot-plug capabilities

The compute and accelerator blades, the fan blades, the Chassis Management Module (CMM), the Ethernet Switch Module (ESM), the Quad Switch Module (QSM) the Local Control Panel (LCP) and the Power Supply Units (PSU) are hot-pluggable / hot-swappable for optimum uptime and easy maintenance.

Redundancy capabilities
The redundant PSU modules and fan blades ensure continued operation even if a component fails.

Redundant network connection capabilities
The optional ESM provides a redundant Ethernet interface to the blades.

System management capabilities
The blade system Chassis Management Module (CMM) is equipped with a service processor, which in conjunction with the system-management firmware provided on the service processor in each compute or accelerator blade, allows remote management of system components and blades. The Chassis Management Module (CMM) also multiplexes access to the embedded management controllers on the compute blades / accelerator blades providing them with KVM and Virtual Media capabilities.
Each compute blade / accelerator blade is equipped with a service processor which provides blade system monitoring, event recording, and alert capabilities.

Network environment support
The blade system supports up to two Ethernet Switches, one in the Chassis Management Module (CMM) and the second in the Ethernet Switch Module (ESM). The Ethernet Switch Modules are used for compute blade / accelerator blade communication with the network. The Chassis Management Module (CMM) and Ethernet Switch Module (ESM) provide internal connections to each compute blade/ accelerator blade.

1.2 Reliability, Availability, and Serviceability (RAS)

The following is a list of RAS features that the blade system supports:

- Shared key components, such as power, cooling, and I/O
- All components serviced from the front or rear of the blade chassis
- Built-in monitoring for fan blade, power, temperature, and voltage
- Built-in monitoring for module redundancy
- Error codes and messages
- Fault-resistant startup
- Remote system management through the Chassis Management Module (CMM)
- Remote upgrade of Chassis Management Module (CMM) firmware
- Remote upgrade of compute blade/ accelerator blade service processor firmware
- Redundant components:
  - fan blades
  - Power Supply Unit modules
- Hot-plug / hot-swap components:
  - Compute blades (NCB) / accelerator blades (GPU)
  - Fan blades
  - Chassis Management Module (CMM)
  - Ethernet Switch Module (ESM)
  - Quad Switch Module (QSM)
  - Local Control Panel (LCP)
  - Power Supply Unit (PSU)
- Ultra Capacitor Module (UCM) (requires full system power down)

1.3 Features and specifications

The following is a summary of the features and specifications for the blade system:

- 7U rack-mountable system chassis with Midplane and LCP display
- bullx B500 compute blades (NCB)
- bullx B505 accelerator blades (GPU)
- AC power redundancy: N+1 (4 PSU modules redundant system, 3 PSU modules non-redundant system)
- Two fan blades cooling the QSM, CMM and ESM
- Rack-mountable system, using a standard cabinet

Further specifications are given in **Erreur ! Source du renvoi introuvable.**.

1.3.1 Chassis-level platform management

The following platform management features are available via the Chassis Hardware Console:

- Embedded web server, compliant with Microsoft Internet Explorer and Firefox browsers
- SNMP, SMASH/CLP, and IPMI Out of Band compliant interface
- Logistic control (thermal, cooling, global power control, and power distribution)
- Hardware health monitoring and alerting

1.3.2 Blade-level platform management

The following platform management features are available via the Blade Hardware Console:

- Embedded web server, compliant with Microsoft Internet Explorer and Firefox browsers
- IPMI v2.0, SMASH/CLP Out of Band compliant interface
- Logistic control (thermal, local power control, and power distribution)
- Hardware health monitoring and alerting

1.3.3 External connections, interfaces, indicators, buttons and switches

The following external connections, interfaces, indicators, buttons and switches are available:

- Eighteen IB QDR connections (QSFP connector with power) on the Quad Switch Module
- Three1Gb Ethernet ports -RJ45 connectors and a serial COM port for maintenance on the ESM
- Three1Gb Ethernet ports -RJ45 connectors and a serial COM port for maintenance on the CMM
- Local Control Panel (LCP)
- Chassis power On/Off switch
- Chassis power indicator LED
- Chassis blue ID indicator LEDs – front LCP indicator LED, rear CMM indicator LED
- Compute blade (NCB) / accelerator blade (GPU) indicator LEDs
- Quad Switch Module indicator LED
- Gbit Ethernet switch indicator LED
- Ultra Capacitor Module indicator LED
- CMM reset pushbutton (CMC reset)

1.4 System components, controls and LEDs

This section identifies the components, controls, and LEDs on the front and rear of the blade system.

1.4.1 Blade system with compute blades – exploded view
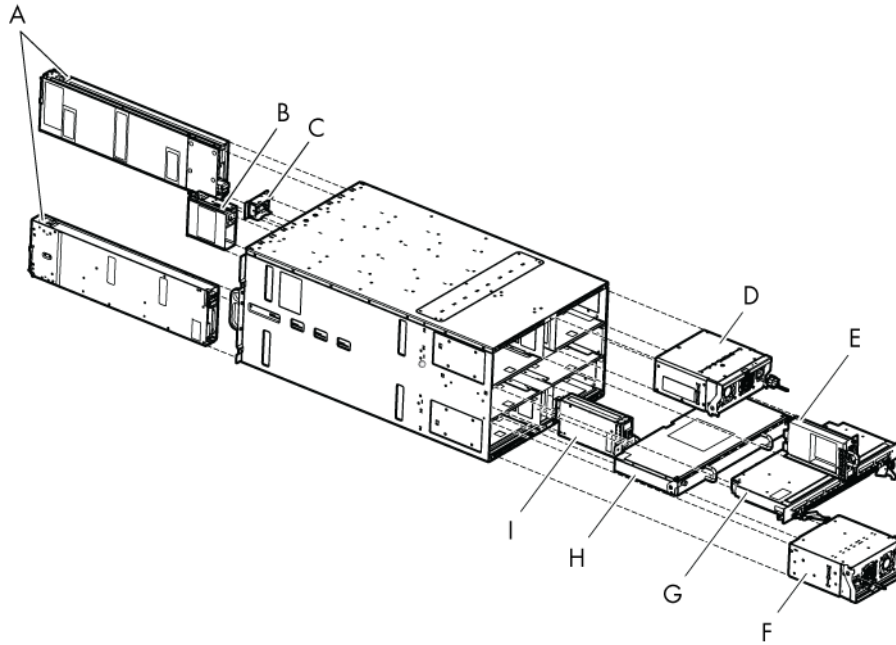
A Compute blades	B Fan blade
C Local Control Panel	D Power Supply Unit module
E Chassis Management Module	F Power Supply Unit module
G Quad Switch Module	H Ultra Capacitor Module
I Ethernet Switch Module	

Figure 1-2.   Blade system with compute blades – exploded view

1.4.2 Blade system with accelerator blades – exploded view
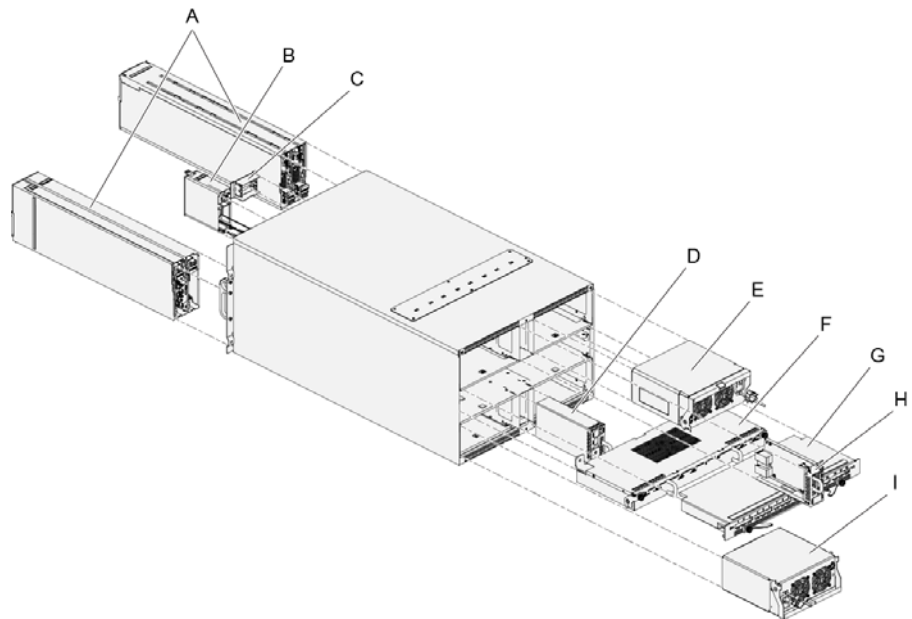
A Accelerator blades	B Fan blade
C Local Control Panel	D Ethernet Switch Module
E Power Supply Unit module	F Ultra Capacitor Module
G Quad Switch Module	H Chassis Management Module
I Power Supply Unit module	

Figure 1-3.   Blade system with accelerator blades – exploded view

1.4.3 Blade system with compute blades – front view
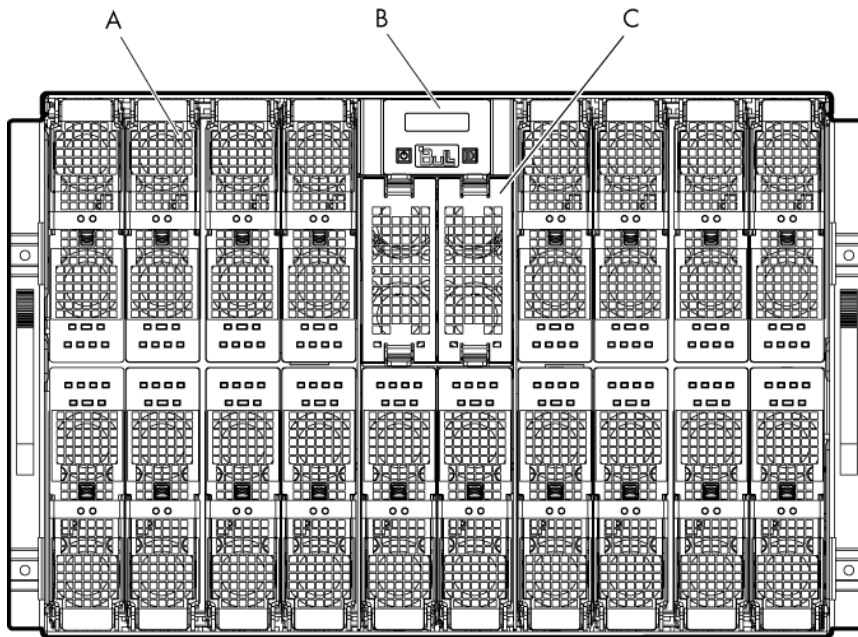
A Compute blade (NCB)	B Local Control Panel
C Fan blade	

Figure 1-4.   Blade system with compute blades – front view

1.4.4 Blade system with accelerator blades – front view
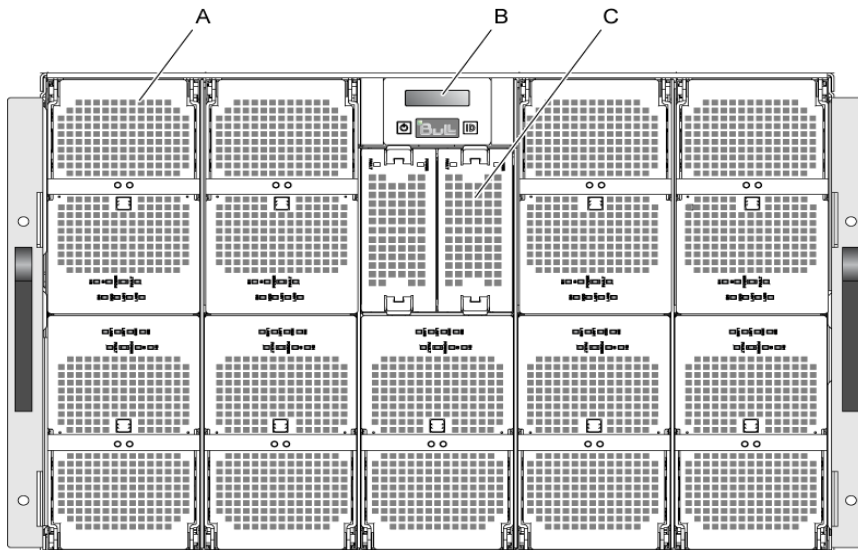
A Accelerator blade (GPU)	B Local Control Panel
C Fan blade	

Figure 1-5.   Blade system with accelerator blades – front view

1.4.5   Blade chassis

The front of the blade chassis is equipped with an LCP, eighteen bays to house compute blades/ nine bays to house accelerator blades and two bays to house fan blades. The blade chassis is also equipped with two handles for easy handling.

The Midplane, in the center of the blade chassis, provides interconnectivity between blades and the various modules located at the rear of the blade chassis.

1.4.6   Compute blades (NCB)

The eighteen compute blades are distributed in two rows, eight on the top row and ten on the bottom row. All the blades are inserted from the front of the blade system and plugged into the Midplane.

The compute blades provide the server motherboard functionality based on dual Nehalem-EP / Westmere-EP processors from Intel® and ensure maximum performance/watt for datacenter infrastructures and highly dense deployments. Each processor interconnects with the other processors through the Intel Quick Path Interconnect (QPI) feature. Each compute blade interconnects with the other compute blades through an embedded ConnectX QDR component and the Quad Switch Module.
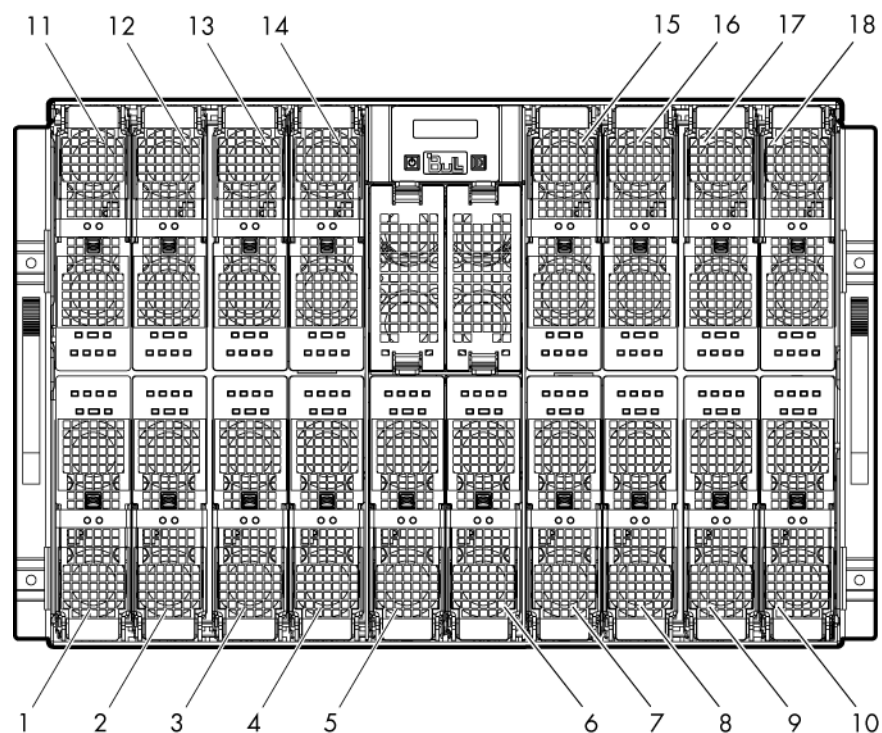
Figure 1-6.   Compute blades (NCB)

Note   Compute blades (NCB) and accelerator blades (GPU) can be installed in the same chassis.

The compute blades present the following features:

- Hot-plug / hot-swap supported

- Dual-processor sockets for up to two processors

- All processor SKUs supported up to 95W

- Twelve DDR3 DIMM slots (6 per socket) at 800, 1066, 1333 MHz

- SATA drive (HDD or SSD) form factor 1.8 inch

- Sleep state four (Suspend to disk) supported on HDD/SSD where available

- Front status LEDs

1.4.6.1 Compute blade (NCB) LEDs

Each compute blade is equipped with the following LEDs:
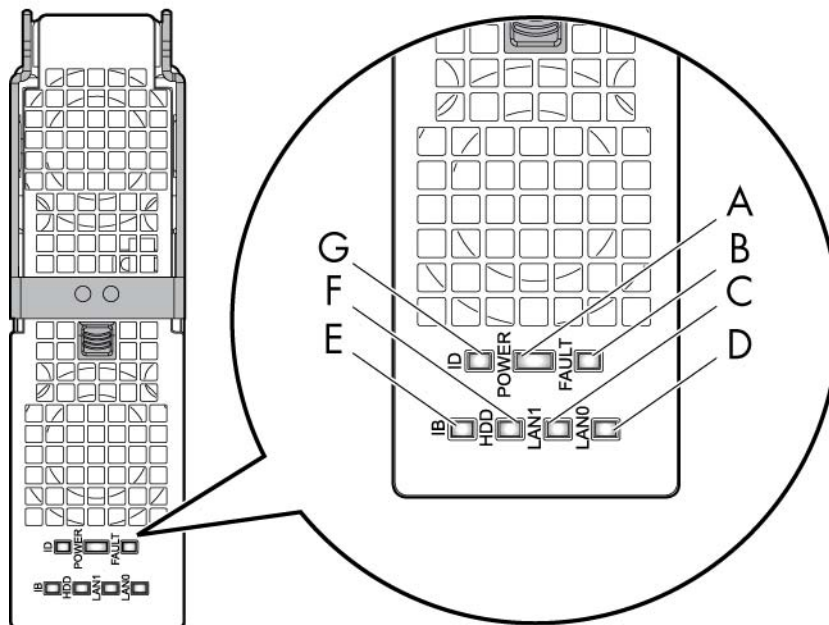
A Power LED	B Fault LED
C LAN1 LED	D LAN0 LED
E IB activity LED	F HDD activity LED
G Identification LED	

Figure 1-7.   Compute blade (NCB) LEDs

⚠ **DANGER**
Hazardous energy is present when the blades are connected to the power source. Never insert a blade into the chassis with its cover removed.

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated to maintenance operations and used to physically localize a compute blade.

This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface.

Power LED

The power LED indicator is bicolor: **amber/green**.

This indicator provides the compute blade power state:

–   **Amber**: 3.3V stand-by power presence (the blade is in stand-by/off power mode)

–   **Green**: 12V main power presence (the blade is in main power mode)

This indicator is managed by the hardware.

Fault LED

The fault LED indicator is **red**.

This indicator displays faults detected by the integrated Baseboard Management Controller (iBMC) firmware.

This indicator is managed by the iBMC firmware.

LAN 0 activity LED

The LAN 0 activity LED indicator is **green**.

This indicator flashes On and Off to indicate compute blade traffic (Tx and Rx data) on the Ethernet network channel 0 (to/from CMM).

This indicator is managed by the hardware.

LAN 1 activity LED

The LAN 1 activity LED indicator is **green**.

This indicator flashes On and Off to indicate compute blade traffic (Tx and Rx data) over the Ethernet network channel 1 (to/from ESM) through the Ethernet component.

This indicator is managed by the hardware.

IB activity LED

The IB activity LED indicator is **amber**.

This indicator flashes On and Off to indicate compute blade traffic over the IB network channel 0 for through the ConnectX component.

This indicator is managed by the hardware

HDD activity LED

The HDD activity LED indicator is **amber**

This indicator flashes On and Off to indicate traffic over the SATA link.

This indicator is managed by the hardware.

1.4.7 Accelerator blades (GPU)

The nine accelerator blades are distributed in two rows, four on the top row and five on the bottom row. All the blades are inserted from the front of the blade system and plugged vertically into the Midplane.

The accelerator blades provide the server motherboard functionality based on dual Nehalem-EP / Westmere-EP processors from Intel® and two Nvidia graphic cards and ensure maximum performance/watt for datacenter infrastructures and highly dense deployments. Each processor interconnects with the other processors through the Intel Quick Path Interconnect (QPI) feature. Each accelerator blade interconnects with the other accelerator blades through an embedded ConnectX QDR component and the Quad Switch Module.

The main accelerator blade components are the SSUPs (SSUP0 and SSUP1) with their processors, IOH and DIMMs, the Planar and two Nvidia graphic cards.
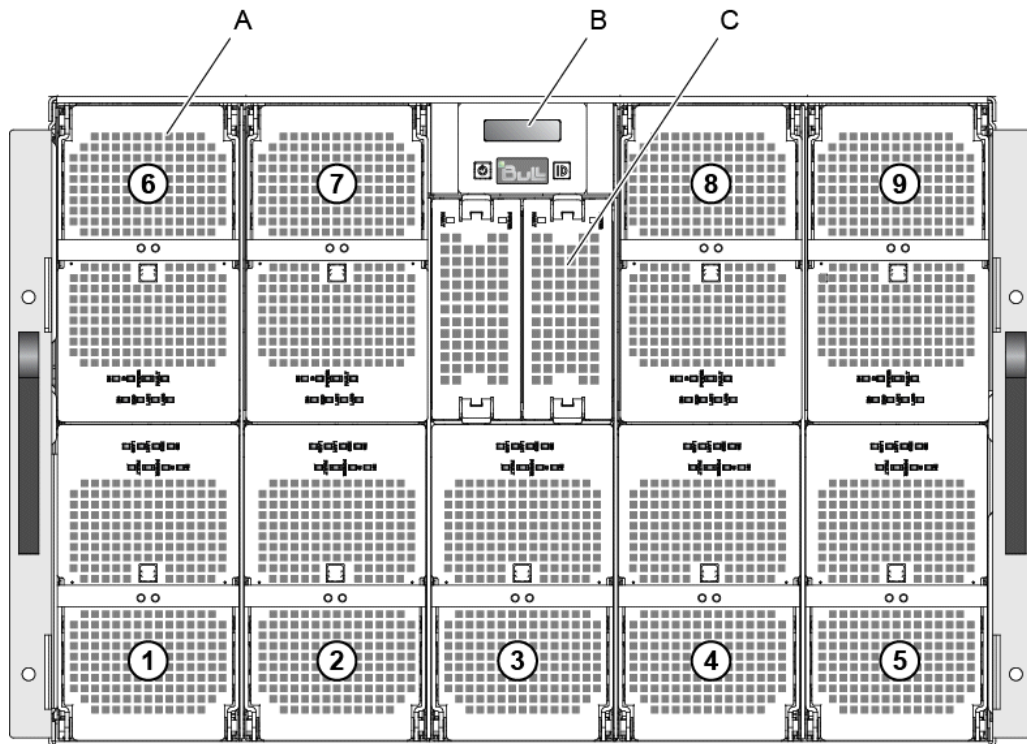
A Accelerator blade	B Local Control Panel
C Fan Blade	

Figure 1-8   Accelerator blades (GPU)

Note   Compute blades (NCB) and accelerator blades (GPU) can be installed in the same chassis.

The accelerator blades present the following features:

- Hot-plug / hot-swap supported

- Dual-processor sockets for up to two processors

- All processor SKUs supported up to 80W

- Six DDR3 DIMM slots (3 per socket) at 800, 1066, 1333 MHz

- Two PCI Express Gen2x16 slots

- SATA drive (HDD or SSD) form factor 1.8 inch

- Sleep state four (Suspend to disk) supported on HDD/SSD when available

- Front status LEDs

1.4.7.1   Accelerator blade (GPU) LEDs

Each accelerator blade is equipped with the following LEDs:
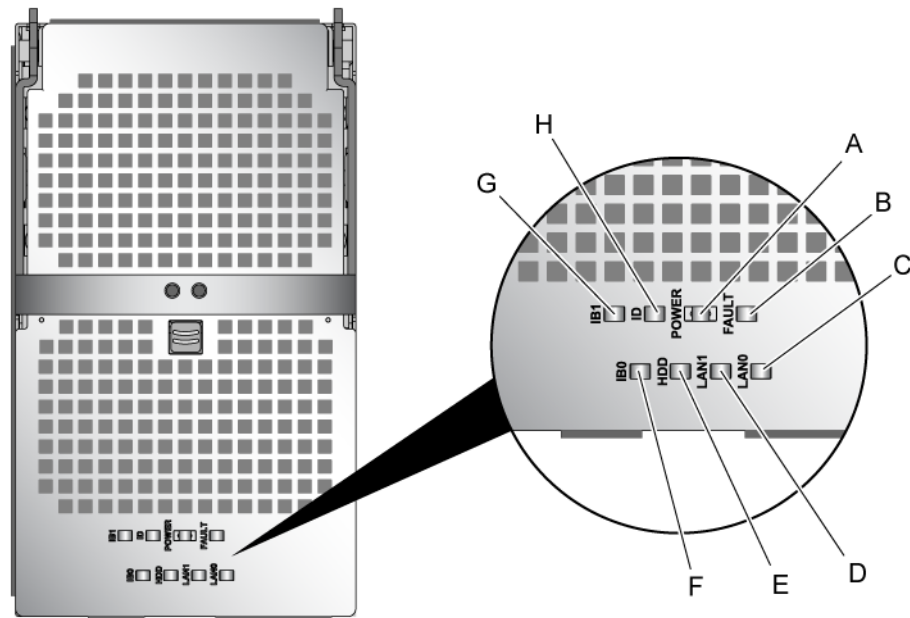
A Power LED	B Fault LED
C LAN0 LED	D LAN1 LED
E HDD activity LED	F IB0 activity LED
G IB1 activity LED	H Identification LED

Figure 1-9   Accelerator blade (GPU) LEDs

DANGER
Hazardous energy is present when the blades are connected to the power source. Never insert a blade into the chassis with its cover removed.

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated to maintenance operations and used to physically localize an accelerator blade.

The LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface.

Power LED

The power LED indicator is bicolor: **amber/green**.

This indicator provides the accelerator blade power state:

- **Amber**: 3.3V stand-by power presence (the blade is in the stand-by/off mode)
- **Green**: 12V main power presence

This indicator is managed by the hardware.

Fault LED

The fault LED indicator is **red**.

This indicator displays faults detected by the integrated Baseboard Management Controller (iBMC) firmware.

This indicator is managed by the iBMC firmware.

LAN 0 activity LED

The LAN 0 activity LED indicator is **green**.

This indicator flashes On and Off to indicate accelerator blade traffic (Tx and Rx data) on the Ethernet network channel 0 (to/from CMM).

This indicator is managed by the hardware.

LAN 1 activity LED

The LAN 1 activity LED indicator is **green**.

This indicator flashes On and Off to indicate accelerator blade traffic (Tx and Rx data) over the Ethernet network channel 1 (to/from ESM) through the Ethernet component.

This indicator is managed by the hardware.

IB0 activity LED

The IB0 activity LED indicator is **amber**.

This indicator flashes On and Off to indicate accelerator blade traffic over the IB0 network channel 0 through the SSUP0 ConnectX component.

This indicator is managed by the hardware

IB1 activity LED

The IB1 activity LED indicator is **amber**.

This indicator flashes On and Off to indicate accelerator blade traffic over the IB1 network channel 1 through the SSUP1 ConnectX component.

This indicator is managed by the hardware

HDD activity LED

The HDD activity LED indicator is **amber**.

This indicator flashes On and Off to indicate traffic over the SATA link.

This indicator is managed by the hardware.

1.4.8   Fan blades

Two fan blades provide cooling to the QSM, CMM, and ESM. The fan blades are hot-swappable/hot-pluggable.

A Latch	B Fault LED
C Power LED	
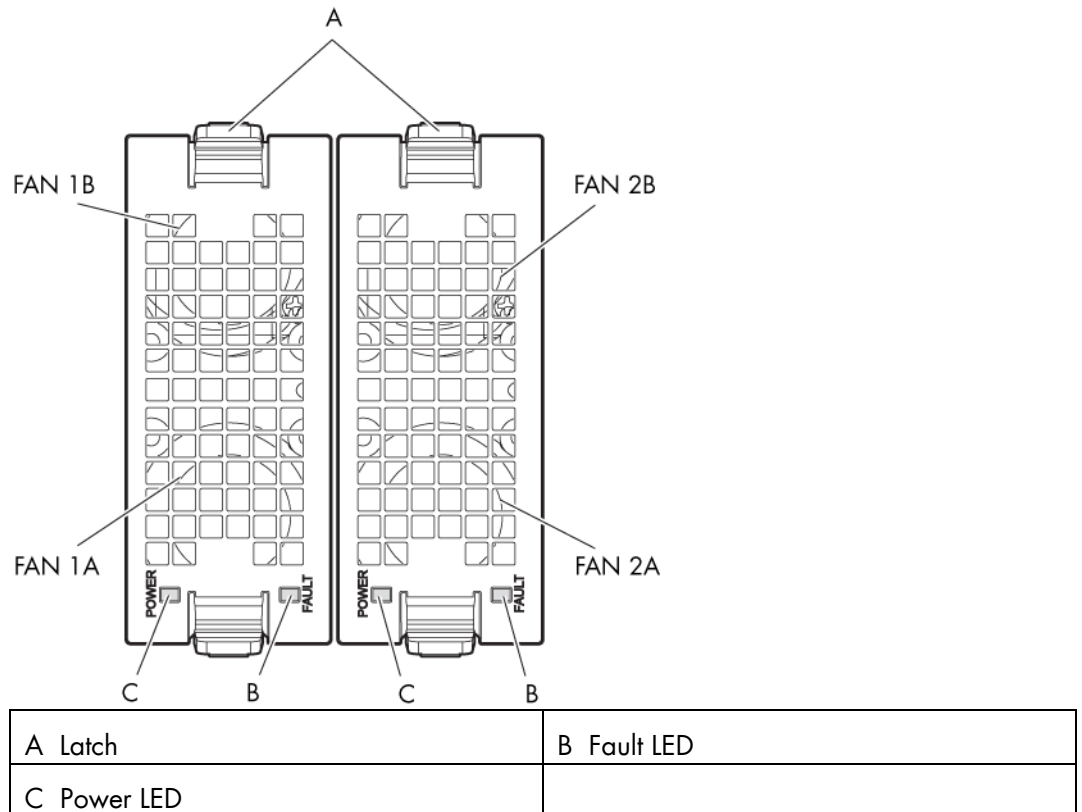
Figure 1-10 Fan blades

1.4.8.1   Fan blade LEDs

Each fan blade is equipped with the following LEDs:

Fault LED

The fault LED indicator is **red**.

When the fans do not rotate as per the expected speed, the fault LED switches On.

Power LED

The power LED indicator is **green**.

When the fans are rotating as per the expected speed, the power LED switches On.

---

important   Replace a failed fan blade as soon as possible to restore cooling redundancy. See the *bullx blade system Maintenance and Troubleshooting Guide* on the *bullx blade system Resource and Documentation CD* for instructions.

1.4.9   Local Control Panel

The Local Control Panel (LCP) is on the front of the blade chassis. The Local Control Panel is hot-swappable / hot-pluggable.
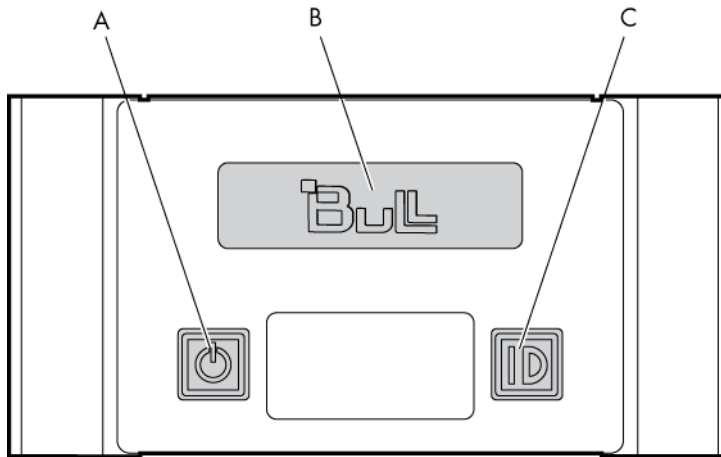
A Power On/Off button	B Display screen
C Identification button	

Figure 1-11. Local Control Panel

1.4.9.1   Local Control Panel LEDs

The Local Control Panel is equipped with the following LEDs:

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated to maintenance operations and used to physically localize a blade chassis from the front of the chassis. This LED turns On simultaneously with the CMM identification LED indicator on the rear of the chassis.

This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface or locally from the LCP ID button (providing this option is enabled from the Chassis Hardware Console web interface).

Power LED

The power LED indicator is **green**.

This indicator indicates 12V main power presence within the blade chassis.

This indicator is managed by the CMC firmware.

1.4.10   Blade system – rear view

This section identifies the components and LEDs on the rear of the blade system.
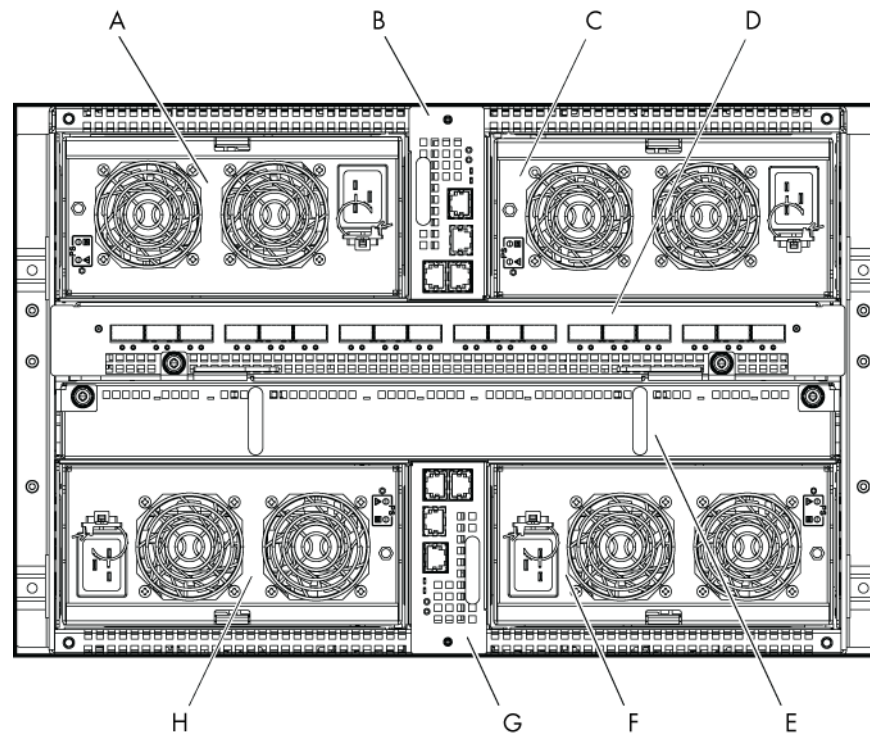
A PSU3	B CMM
C PSU4	D QSM
E UCM	F PSU2
G ESM	H PSU1

Figure 1-12. Blade system – rear view

1.4.11   Blade chassis

The rear of the blade chassis provides bays for blade system PSU, CMM, QSM, UCM, and ESM modules.

The Midplane, in the center of the blade chassis, provides interconnectivity between these modules and the blades located at the front of the blade chassis.

1.4.12   Power Supply Unit (PSU) module

There are four x 2900W PSU modules at the rear of the blade system, providing 12V main and 3.3V stand-by outputs. When four PSU modules equip the blade system, they provide N+1 redundancy. Typical system power dissipation is approximately 7900W according to configuration and running applications. High-level PSU module features are:

- Hot-plug / hot swap supported, up to four parallel supplies

- 2900W power supply

- 12V main and 3.3V stand-by outputs

- 210 VAC to 240 VAC corrected AC input power factor

- PSMI compliant
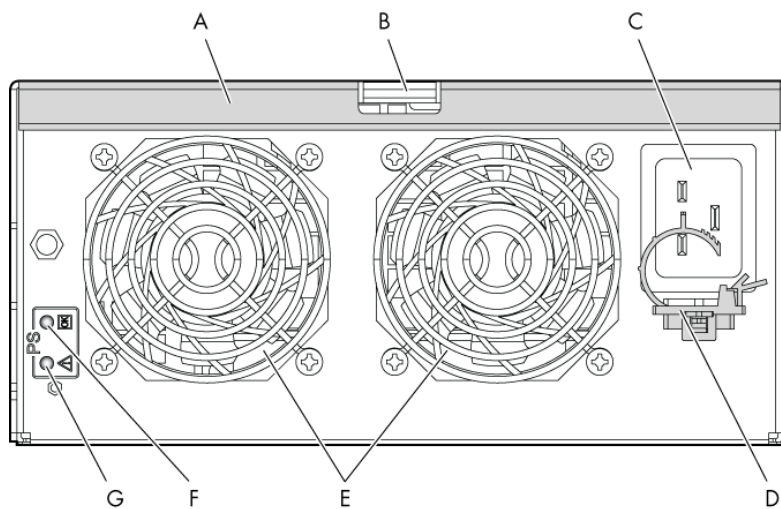
A Handle	B Latch
C Power socket	D Cable retention
E Fans	F Power LED
G Fault LED	

Figure 1-13. Power Supply Unit (PSU) module

1.4.12.1   Power Supply Unit module LEDs

The Power Supply Unit module is equipped with the following LEDs:

Fault LED

The Fault LED indicator is **amber**.

A slow blinking or solid On state indicates that the PSU module has failed or reached a critical state warranting its replacement.

Power LED

The Power LED indicator is **green**.

Slow **blinking green** indicates that AC is being applied to the PSU module and that the 3.3V stand-by voltage is available. Once 12V is enabled this LED becomes **steady**.

1.4.13　Chassis Management Module (CMM)

The primary function of the CMM is to provide the blade chassis-level management functionality for the blade system, including detection, power On/Off, hardware status monitoring for the compute blades / accelerator blades and other hardware modules within the blade chassis, PSU status monitoring and system fan control. The CMM is also used to manage and display LCP messages.

The CMM is a hot-swappable module which includes of a 24-port 1GbE Ethernet switch and an OPMA daughter card, which is used as a service processor.

The Ethernet logical connections are:

- One Ethernet port to the service processor (internal)

- Eighteen Ethernet ports to the compute blades / accelerator blades through the backplane connector (internal)

- Three Ethernet ports to RJ45 connectors on the rear (external)
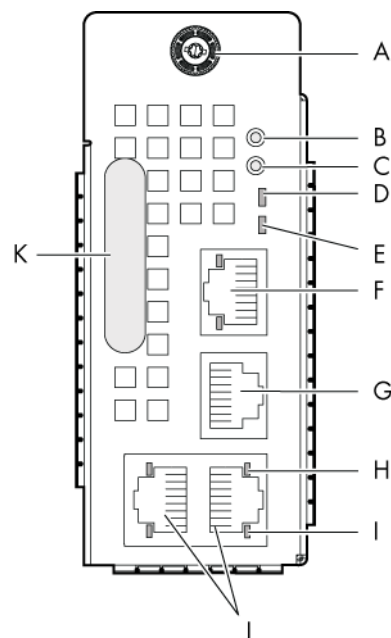
A Thumb screw	B Default button
C Reset button	D Power and health status LED
E Identification LED	F Dynamically configurable stacking or Ethernet port
G Serial port	H Activity LED
I Link LED	J Dynamically configurable stacking or Ethernet port
K Handle	

Figure 1-14. Chassis Management Module (CMM)

The CMM presents the following features:

- Hot-plug / hot-swap supported
- Compute blades / accelerator blades can run even when the CMM is down
- Ethernet switch supports VLANs
- Three dynamically configurable stacking or Ethernet ports
- External COM port
- Status LEDs
- Status information displayed on the LCP
- Ethernet switch firmware can be loaded in-band over the Ethernet links

1.4.13.1 Chassis Management Module LEDs

The Chassis Management Module is equipped with the following LEDs:

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated maintenance operations and used to physically localize the blade chassis from the rear of the chassis. This LED turns On simultaneously with the LCP identification LED indicator on the front of the chassis.

This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface or locally from the LCP ID button.

Power LED

The power LED indicator is **amber**.

This indicator provides the blade chassis power state and CMC activity:

- **Solid amber**: CMM is initializing
- **Blinking amber**: CMC firmware is alive

LAN activity and status LED

Two LEDs are integrated in each of the three Ethernet connectors:

- Link status LED
- Link activity LED

1.4.14　Quad Switch Module (QSM)

The blade system supports a QSM, based on a 36 port QDR switch Board (QSB) to provide the quad switching function between the compute blades / accelerator blades and the external QSFP ports. The QSM plugs into the Midplane from the rear of the blade chassis. This module is also known as InfiniBand Switch.
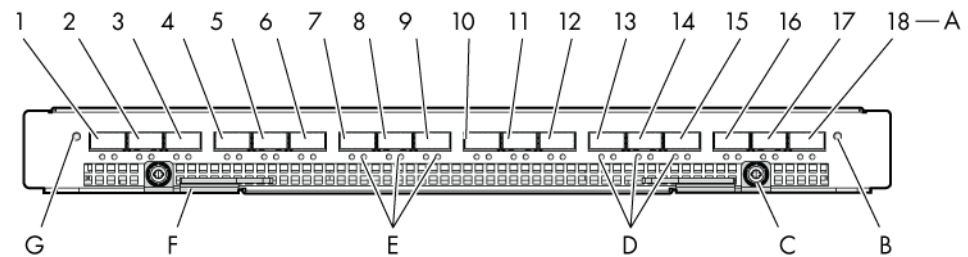
A QSFP ports (1-18)	B Power On/AUX Power LED
C Thumb screw	D Logical link LED
E Physical link LED	F Latch
G Identification LED	

Figure 1-15. Quad Switch Module

The QSM presents the following features:

- Hot-plug / hot-swap supported
- 36 InfiniBand Switch ports:
    - 18 internal ports
    - 18 external ports
- QDR IB support
- Passive and active cable support per IB standard
- Status indication LEDs
- In-band IB connection switch management

1.4.14.1 Quad Switch Module LEDs

The Quad Switch Module is equipped with the following LEDs:

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated maintenance operations and used to physically localize the module. This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface.

Power LED

The power LED status indicator is bicolor:

- **Amber**: 3.3V stand-by power presence
- **Green**: 12V main power presence

IB link activity LEDs

There are two IB link activity LEDs:

- **Physical link**: -**still green** indicates a good physical link; **blinking green** indicates a physical link problem.
- **Logical link**: **blinking amber** indicates data transfer.

1.4.15 Ultra Capacitor Module (UCM)

The UCM is an optional module that can ride through AC outages of up to 250ms. The UCM connects to the Midplane through bus bars and during normal operation the UCM charges power from the Midplane 12V. This power is stored in the module's Ultra capacitors. During outage, the capacitors discharge to provide the required power to the other components, such as the blades and the Quad Switch Module (QSB). Hold-time under 3V3 stand-by voltage is 1000ms. The UCM is also controlled/monitored by the CMM under 3V3 stand-by voltage.
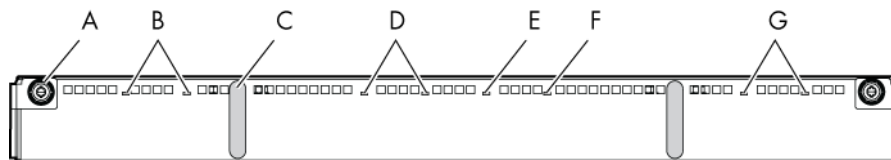
A Thumb screw	B Discharging LEDs
C Handle	D Charging LEDs
E Identification LED	F Fault LED
G Charge / Discharge LEDs	

Figure 1-16. Ultra Capacitor Module (UCM)

The UCM presents the following features:

- 250 ms power outage offset ability
- 480 ms maximum hold-up time
- Status indication LEDs

1.4.15.1 Ultra Capacitor Module LEDs

DANGER

The UCM must be fully discharged, i.e. CHARGE / DISCHARGE LEDs OFF (G), before servicing the module. DO NOT TOUCH the module until FULLY DISCHARGED.

The Ultra Capacitor Module is equipped with the following LEDs:

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated to maintenance operations and used to physically localize the module. This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface.

Charging LEDs

There are two charging LEDs, one per Ultra Capacitor stack.

Charging LEDs are **amber** when the UCM is charging.

These indicators are managed by the hardware.

Discharging LEDs

There are two discharging LEDs, one per Ultra Capacitor stack.

Discharging LEDs are **red** when the UCM is charged.

These indicators are managed by the hardware.

Charge LEDs

There are two charge LEDs, one per Ultra Capacitor stack.

Charge LEDs are **green** when the UCM is charged.

Charge LEDs are **Off** when the UCM is fully discharged.

These indicators are managed by the hardware.

Fault LED

The fault power LED indicator is **amber**.

This indicator displays UCM failure.

This indicator is managed by the CMC firmware.

1.4.16   Ethernet Switch Module (ESM)

The ESM is an optional module which provides the Ethernet switching function through the three external Ethernet ports.
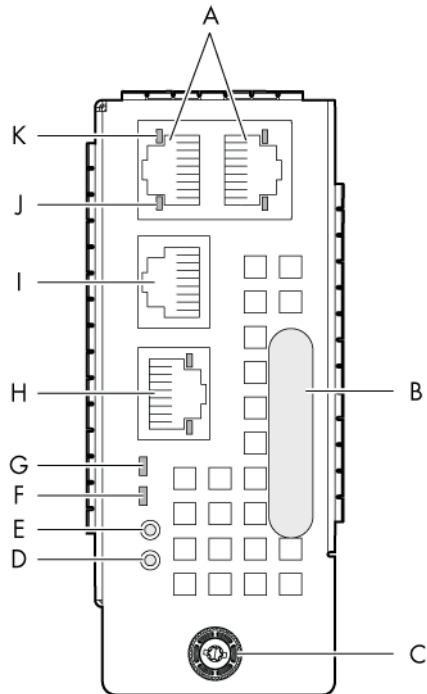
A Dynamically configurable stacking or Ethernet ports	B Handle
C Thumb screw	D Default button
E Reset button	F Power and health status LED
G Identification LED	H Dynamically configurable stacking or Ethernet port
I Serial port	J Activity LED
K Link LED	

Figure 1-17. Ethernet Switch Module

The ESM presents the following features:

- Hot-plug / hot-swap supported
- Ethernet switch supports VLANs
- Ethernet has two stacking ports and a switching Ethernet port by default. Ports can be dynamically configured either as stacking ports or as GbE ports
- Status indication LEDs
- Ethernet switch firmware can be loaded in-band over the Ethernet links

1.4.16.1　Ethernet Switch Module LEDs

The Ethernet Switch Module is equipped with the following LEDs:

Identification LED

The identification LED indicator is **blue**.

This indicator is a unit identifier dedicated to maintenance operations and used to physically localize the module. This LED is switched On/Off by the maintenance operator from the Chassis Hardware Console web interface.

Power LED

The power LED indicator is **amber**.

This indicator provides module 3.3V stand-by power status.

This indicator is managed by the hardware.

LAN activity and status LED

Two LEDs are integrated in each of the three Ethernet connectors:

- Link status LED

- Link activity LED

Note	LAN activity for the embedded Ethernet switch links (i.e. between the Ethernet switch and each compute blade / accelerator blade) are displayed on a LED on the front of each compute blade / accelerator blade.

Chapter 2. Introducing the Chassis Hardware Console

This chapter describes Chassis Hardware Console (CHC) features and explains how to start and stop the console from a Web browser.

2.1 Starting the console

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

Prerequisites

- The drawer is connected to the site power supply and also to the enterprise LAN
- Your web browser is configured to accept cookies

Procedure

1. Launch your web browser and enter the standard or secure IP address or host name (example: https://myconsole.mydomain), as per settings. The authentication page opens.
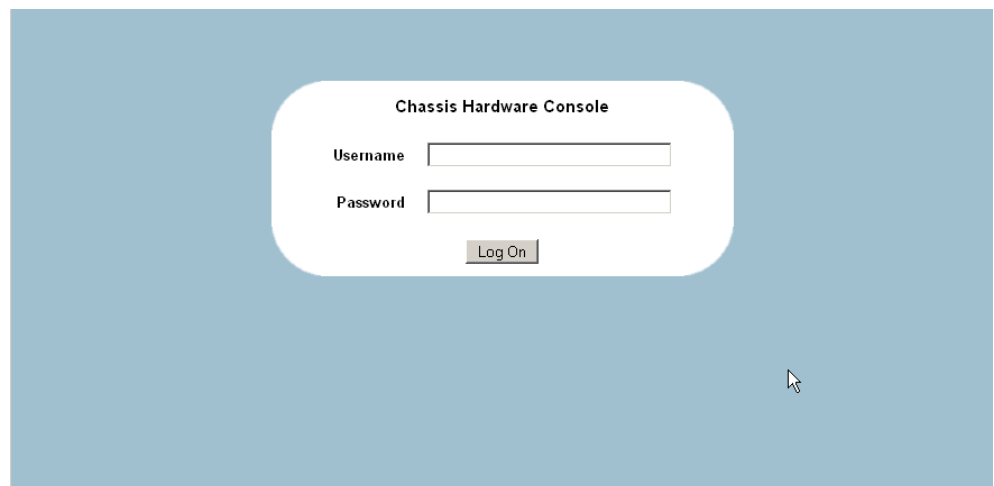
| Username | Factory-default username: super |
| Password | Factory-default password: bull |

Figure 2-1.   Authentication page

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

> **Important**
>
> You are advised to change factory-default authentication settings once initial setup is completed, taking care to record your new account details for subsequent connections. If you lose your account details, contact your Customer Service Representative.

If you cannot connect to the console or if the web pages are displayed incorrectly, it may be due to network failure or incorrect network or browser settings.

2.2　Console overview

The Chassis Hardware Console is a web-based administration application embedded on the Chassis Management Module (CMM). It allows you to remotely operate, monitor, configure and maintain the blade system. The Chassis Hardware Console can be accessed via the Ethernet network using a Microsoft Internet Explorer or a Mozilla Firefox browser.
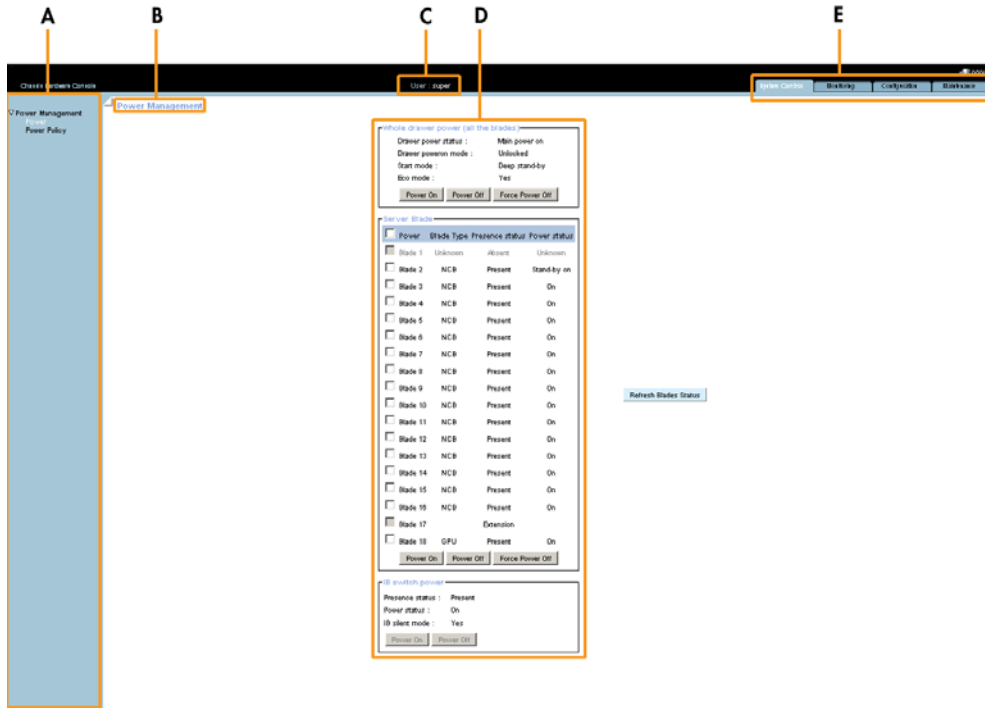
Console overview	
A	The navigation tree provides access to console features. Note that displayed features differ according to the tab selected.
B	Current feature name and description.
C	User logon name.
D	The control pane displays the commands and information associated with the item selected in the navigation tree.
E	Four tabs allow access to families of features accessible from the associated navigation trees: System Control, Monitoring, Configuration, and Maintenance.

Figure 2-2.　Chassis Hardware Console overview

2.3   Console features and permissions

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

Tab	Tree node	Features	Permission
System Control	Power Management	Power	Viewing: all users Operations: root users
		Power Policy	Viewing: all users Operations: root users
Monitoring	Cabinet Status & Logs	Sensor Status	Viewing: all users
		System Event Log	Viewing: all users Operations: root users
		Messages	Viewing: all users Operations: root users
Configuration	General Settings	Chassis	Viewing: all users Operations: root users
		CMC Network	Viewing: all users Operations: root users
		BMC Network	Viewing: all users Operations: root users
		Date-time	Viewing: all users Operations: root users
		SNMP	Viewing: all users Operations: root users
		Messages	Viewing: all users Operations: root users
	User Management	Users	Viewing: all users Operations: root users
		Groups	Viewing: all users Operations: root users
		Password	Viewing: all users Operations: root users

Tab	Tree node	Features	Permission
Configuration	Security Management	Encryption	Viewing: all users Operations: root users
		SSL Certificate	Viewing: all users Operations: root users
		Access Control	Viewing: all users Operations: root users
		User Logon Policy	Viewing: all users Operations: root users
		Authentication	Viewing: all users Operations: root users
		Power Button Lockout	Viewing: all users Operations: root users
		User Lockout	Viewing: all users Operations: root users
	Alert Settings	Filters	Viewing: all users Operations: root users
		Policies	Viewing: all users Operations: root users
		LAN Destination	Viewing: all users Operations: root users
		General	Viewing: all users Operations: root users
Maintenance	Hardware Information	Management Board	Viewing: all users Operations: root users
		FRU	Viewing: all users Operation: root users
		Firmware	Viewing: all users
		Drawer Information	Viewing: all users Viewing: new drawer

Tab	Tree node	Features	Permission
Maintenance	Firmware Updates	CMC	Viewing: all users Operations: root users
	Maintenance Operations	Unit reset	Viewing: all users Operations: root users
		Identification LED	Viewing: all users Operations: root users
		Hardware Exclusion	Viewing: all users Operations: root users
		Server Blade Change	Viewing: all users Operations: root users
		CMM Change	Viewing: all users Operations: root users
		ESM Change	Viewing: all users Operations: root users
		IBSW Change	Viewing: all users Operations: root users
		LCP Change	Viewing: all users Operations: root users
		Power Management	Viewing: all users Operations: root users
		Connected Users	Viewing: all users Operations: root users
		UCM Management	Viewing: all users Operations: root users

Table 2-1.   Console features and permissions

2.4   Stopping the Console

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

Chapter 3. Using chassis power controls

This chapter explains how to use power controls and check power status.

3.1   Viewing power features and checking status

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System Control** tab and select **Power Management > Power** to display the **Power Management** page.
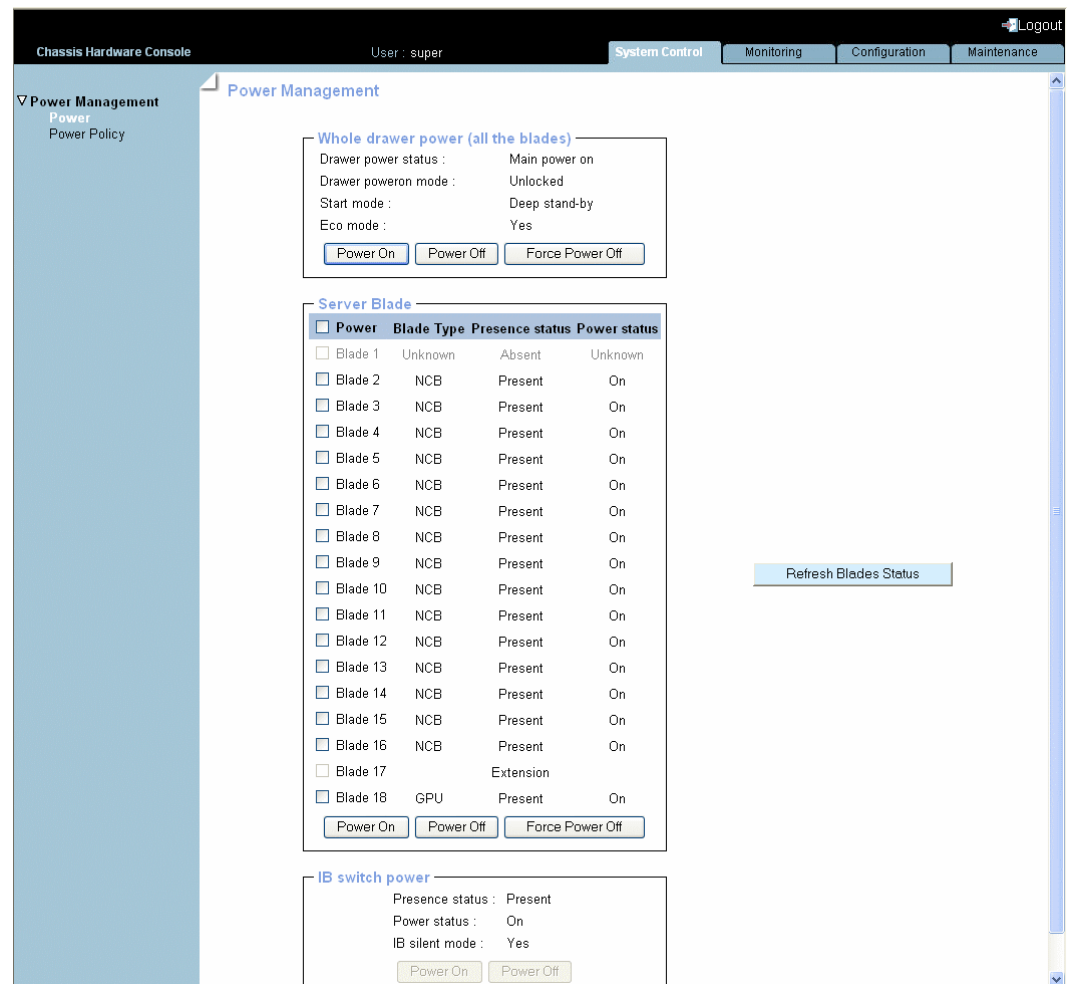
Figure 3-1.   Power management page

The Power Management page is divided into three areas:

- Whole drawer power

- Server blade

- IB switch power

Whole drawer power		
Drawer power status	Deep stand-by	Lowest drawer power consumption waking state
	Light stand-by	Moderate drawer consumption working state
	Unlocked	Drawer functional state
Drawer power on mode	Full power on	All the blades and other boards powered
	Unlocked	All the blades and other boards unlocked (12V enabled)
Start mode	Deep stand-by	Blade remains in stand-by off state (i.e. BMC is not running)
	Light stand-by	Blade turns to stand-by on state (i.e. BMC is running)
	Unlocked power	Blade turns to off state (i.e. BMC is running and 12V power enabled)
Eco mode	Yes	Forces drawer to silent mode. (The drawer can be configured to save energy when the blades are not extensively used. The drawer is in deep stand-by state when blade inactivity is detected
	No	Forces drawer to off
Server blade		
Power		Blade number.
Blade Type		GPU (accelerator blade) NCB (compute blade)
Presence status	Present	Corresponding blade is present
	Absent	Corresponding blade is absent
Power status	Off	Corresponding blade is powered off
	On	Corresponding blade is powered on
	Unknown	Corresponding blade is absent
IB switch power		
Presence status	Absent	Quad Switch Module is absent
	Present	Quad Switch Module is present
Power status	Unknown	Quad Switch Module is absent
	Stand-by off	Quad Switch Module is powered off
	On	Quad Switch Module is powered on
IB switch silent mode	Yes	Switch set to silent
	No	Switch can be powered off

Table 3-1.   Power Management page features

3.2 Powering on the complete blade system

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System Control** tab and select **Power Management > Power** to display the **Whole drawer power** box.

Power on modes		
Power on	Full power on	All the blades are powered on and the OS is booted.
	Unlocked	All the blades are turned to the Off state

Figure 3-2.   Powering on the blade system

2. Click **Power On** to launch the power up sequence, which may take a few minutes to complete.

   Once the power up sequence is completed, the **Power State** value switches from **Off** to **On** and the **Power Off** button is enabled.

   If required, connect to the **Remote System Console** to follow the power on sequence.

3.3 Powering off the complete blade system

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System Control** tab and select **Power Management > Power** to display the **Whole drawer power** box.
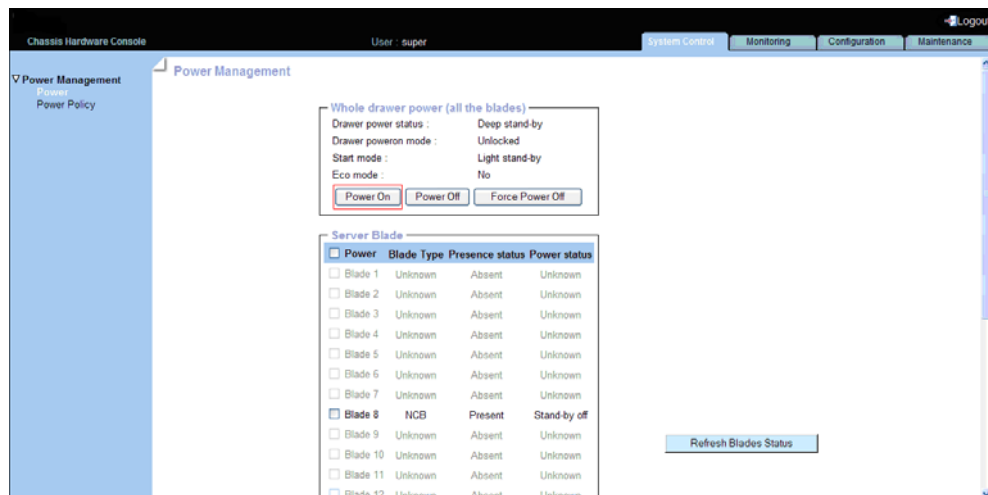
Figure 3-3. Powering off the blade system

2. Click **Power Off** to launch the routine power down sequence, which may take a few minutes to complete. Operating systems are shut down gracefully and hardware is powered down from the main power mode to the Power Off (Unlocked) mode.
   Once the power down sequence is completed, the **Power State** value switches from **On** to **Off**.
   If required, connect to the **Remote System Console** to follow the power off sequence.

Note   If the system does not power off correctly, this may be due to a system crash or freeze and you may need to forcibly power down the system using the **Force Power Off** button.

3.4   Forcibly powering down the complete blade system

In the event of a system crash or freeze, the system can be forcibly powered down.

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

⚠️ CAUTION

The Force Power Off option 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. Open From the **System Control** tab and select **Power Management** to display the **Whole drawer power** box.
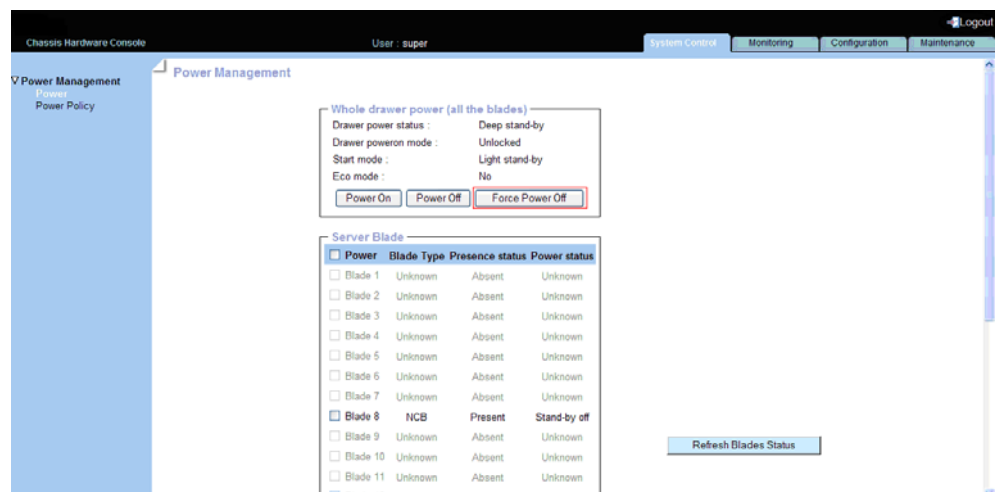
Figure 3-4.   Forcibly powering off the blade system

2. Click **Force Power Off** to forcibly power down the system, which may take a few minutes to complete.

3.5 Powering on / off individual blades and checking status

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System control** tab and select **Power Management > Power** to display the **Server blade** box.
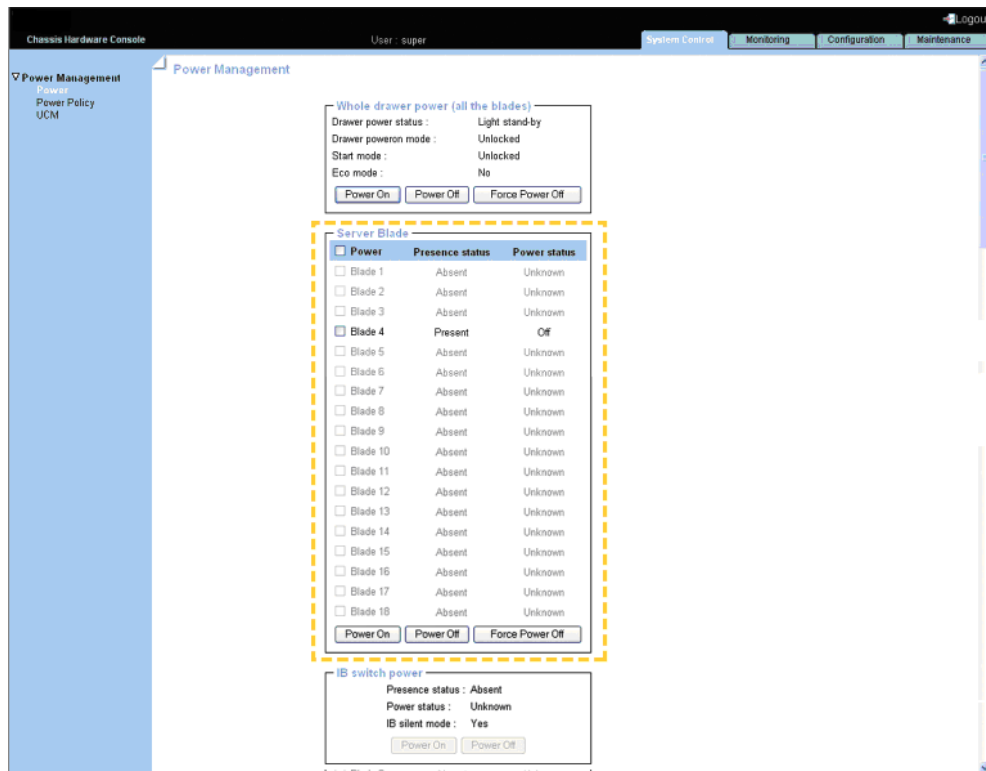
Server blade power options	
Power On	Accessible only when the system is powered Off. This button powers On the corresponding blade.
Power Off	Accessible only when the system is powered On. This button powers Off the corresponding blade.
Force Power Off	This button performs a power down sequence independently of the Operating System. If the **Power Off** operation fails, you can forcibly power Off by clicking **Force Power Off** button.

Figure 3-5.   Server blade power options

2. Select the required power sequence, as explained in the table above.

3.6 Viewing IB switch power status

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System control** tab and select **Power Management > Power** to display the **IB switch power** box.
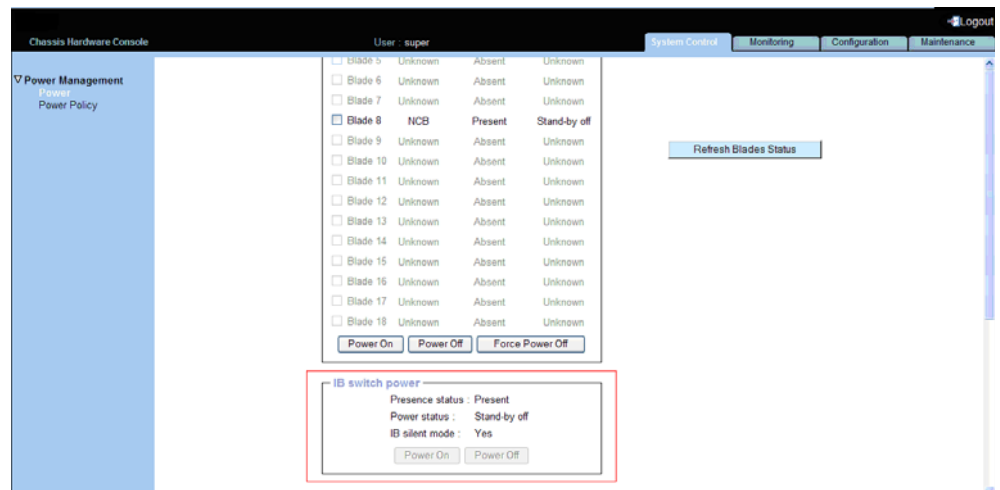
IB switch power status		
Presence status	Absent	Quad Switch Module is absent
	Present	Quad Switch Module is present
Power status	Unknown	Quad Switch Module is absent
	Stand-by off	Quad Switch Module is powered off
	On	Quad Switch Module is powered on
IB switch silent mode	Yes	Switch set to silent
	No	Switch can be powered off

Figure 3-6.   IB switch power status

3.7 Applying power policies

- Viewing: all users

- Operations: root users

Procedure

1. Open the **System Control** tab and select **Power Management > Power Policy** to open the **Power Policy** page.
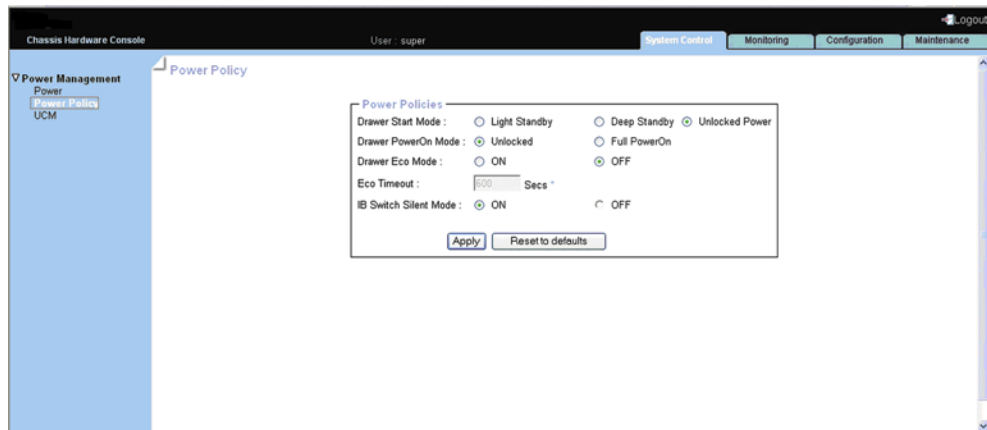
Figure 3-7. Power Policy page

2. Select the required power policy and click **Apply** to apply changes.
For more information about power policy options, refer to the following table.

Power policies		
Drawer start mode	Light stand-by	Moderate power consumption waking state. Blades turn to stand-by on state (i.e. BMC is running)
	Deep stand-by	Lowest power consumption waking state. Blades remain in stand-by off state (i.e. BMC is not running)
	Unlocked power	Blades turn to off state (i.e. BMC is running and 12V power enabled)
Drawer power on mode	Unlocked	All the blades and other boards are unlocked (12 V hot swap enabled) when the drawer is powered on
	Full power on	All the blades and other boards are powered on when the drawer is powered on
Drawer ECO mode	On	Forces drawer eco mode to On. The drawer is configured to save energy when the blades are not used extensively. This mode automatically forces the IB switch silent mode to On
	Off	Forces drawer eco mode to Off
Eco time out		Sets eco mode time in seconds
IB Switch Silent Mode	On	Forces IB switch silent mode to be silent. The IB switch is implicitly powered on when the blade is powered on and is implicitly powered off when the last blade is powered off
	Off	Forces IB switch silent mode not to be silent. The IB switch is explicitly powered on/off

Table 3-2.   Power policy options

3.8 Viewing Ultra Capacitor Module power status

⚠ **DANGER**
The UCM must be fully discharged, i.e. CHARGE / DISCHARGE LEDs OFF (G), before servicing the module. DO NOT TOUCH the module until FULLY DISCHARGED.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

Open the **Maintenance** tab and select **Maintenance Operations > UCM Management** to display the **Ultra Capacitor Module Management** page.
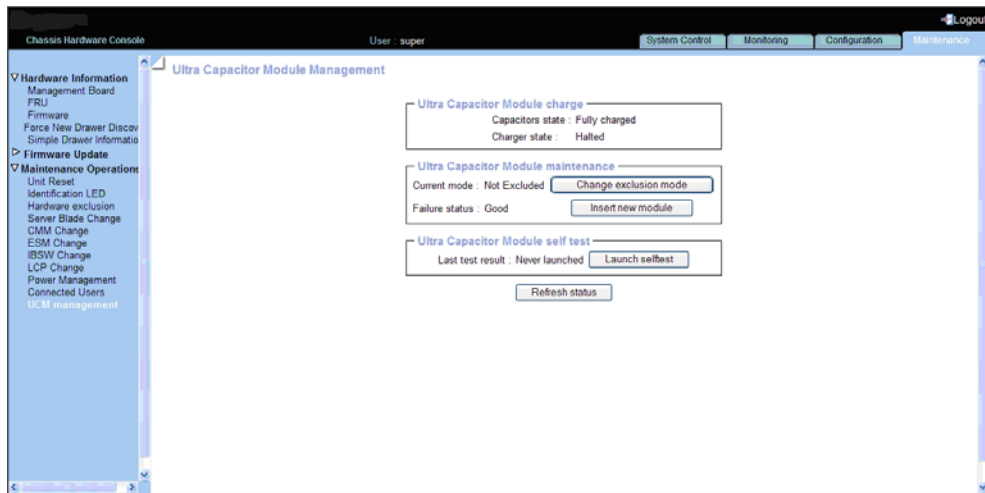
Ultra Capacitor Module Information	
Capacitor state	Depends upon charge level in the UCM capacitor stack
Charger State	Current UCM charging status
Current Mode	UCM exclusion / inclusion status
Failure Status	Values: Fail: a failure has been detected in the UCM Good: the UCM is operating correctly
Last test result	Last UCM self test result

Figure 3-8.   Ultra Capacitor Module power status

Chapter 4. Monitoring the blade system

This chapter explains how to monitor compute blade system activity and view and manage event logs.

4.1 Initial messaging and alert configuration

When the blade system is first delivered, you will need to perform a few basic configuration tasks to benefit from all the messaging and alert features available.

Please refer to Chapter 5. Configuring the , for instructions.

4.2 Viewing monitoring sensor readings

The blade system is equipped with sensors that monitor component status.

Procedure

1. Open the **Monitoring** tab and select **Cabinet Status & Logs > Sensor Status** to display the **Sensor Status** page.
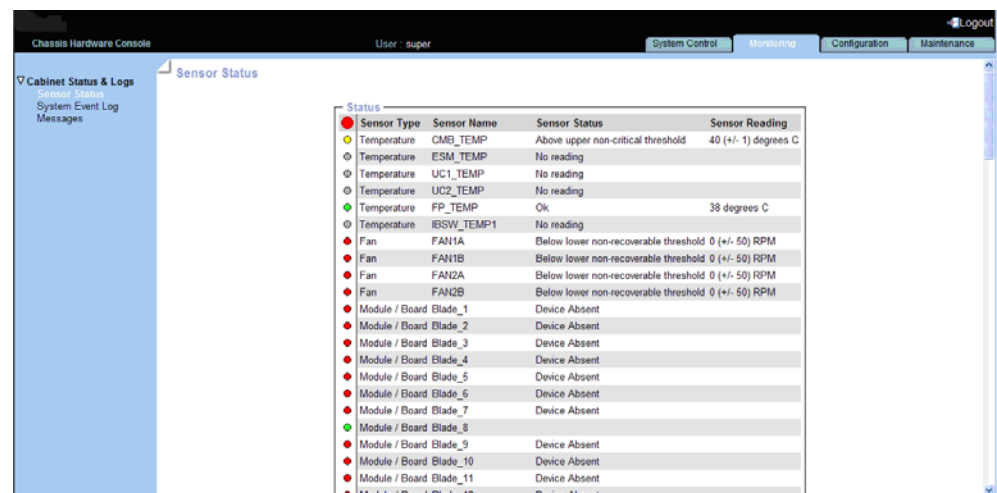
Status Icon Description	
Green	NORMAL This component is operating correctly.
Yellow	NON-CRITICAL A problem has been detected that may need preventive or corrective action.
Red	CRITICAL A problem has been detected. Immediate preventive or corrective action is required.
Gray	NOT-AVAILABLE
Global	The global status icon at the top of the page reflects overall system status.

Figure 4-1.   Sensor Status page

2. Click the **Refresh** button at the bottom of the page to refresh the display.
   If the blade system is operating correctly, all icons should be green.

For reference, the following table lists sensor reading values without thresholds.
Refer to Appendix AAppendix B Troubleshooting the blade system, for detailed
information.

Icon	Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Green Red	Power Supply	PSU_X	Device Present Device Absent	-
Green Red	Power Supply	PSU_X_Fail	No reading Ok	-
Green Red Yellow Gray	Power Supply	Drawer Power PSU_X_PWRIn	-	Value in Watts
Green Red Yellow Gray	Temperature	CMB_TEMP ESM_TEMP UC1_TEMP UC2_TEMP FP_TEMP IBSW_TEMP1	Above upper non- critical threshold No reading OK(normal)	Value in °C
Green Red Yellow Gray	Fan	FAN X	Below power non recoverable threshold Ok	Value in RPM
Green Red Yellow Gray	Module/Board	Blade_X IBSW UCM	Device Present Device Absent	
Green Red Yellow Gray	Voltage	PSU_X_12V_PG Blade_X_3v3_PG Blade_X_Sys_PG PSU_X_Vin PSU_X_VOut UCM_VCAP_X_SENS UCM_21V_SENS_X UCM_12V_SENS UCM_VREF_SENS UCM_X_SENS		Value in Voltage
Green Red Yellow Gray	Current	PSU_X_Iin PSU_X_3v3_Iout PSU_X_12v_Iout		Value in Amps

Table 4-1.   Sensor status page description

4.3   Viewing the System Event Log (SEL)

The System Event log (SEL) records hardware-related events, in particular those concerning:

- Power supplies
- Fans
- Temperature sensors

The events recorded in this log can also be transmitted via the event alerting system to a SNMP Manager or to offline personnel by email.

Note   Non-hardware-related events are recorded in the Board and Security Messages log.

⚠️ CAUTION

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Monitoring** tab and select **Cabinet Status & Logs > System Event Log** to display the **System Event Log** page.

Figure 4-2.   System Event Log page

2. Use the **Refresh** button to update the display at any time.

3. Use the **Clear** button to empty the log.

4.4 Viewing board and security messages
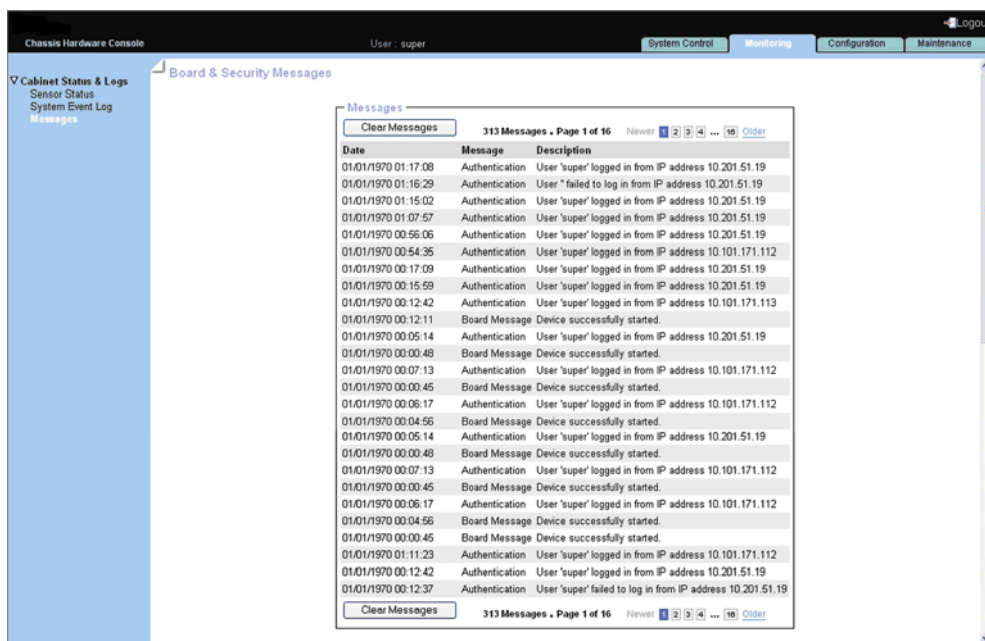
The Board and Security Messages record non-hardware-related events, such as user authentication, connection to the remote console, security violation, log deletion or firmware upgrade. However, hardware-related events are recorded in the SEL.

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Monitoring** tab and select **Cabinet Status & Logs > Messages** to display the **Board & Security Messages** page.

Figure 4-3.   Board & Security Messages page

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

Important

This log can record up to 1,000 events. Once this limit is reached, the arrival of new messages will automatically delete the oldest messages in the log.

Chapter 5. Configuring the blade chassis

- This chapter explains how you can configure the chassis to suit your working environment.

5.1 Configuring the blade chassis name

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **General Settings > Chassis** to display the **Chassis Settings** page.
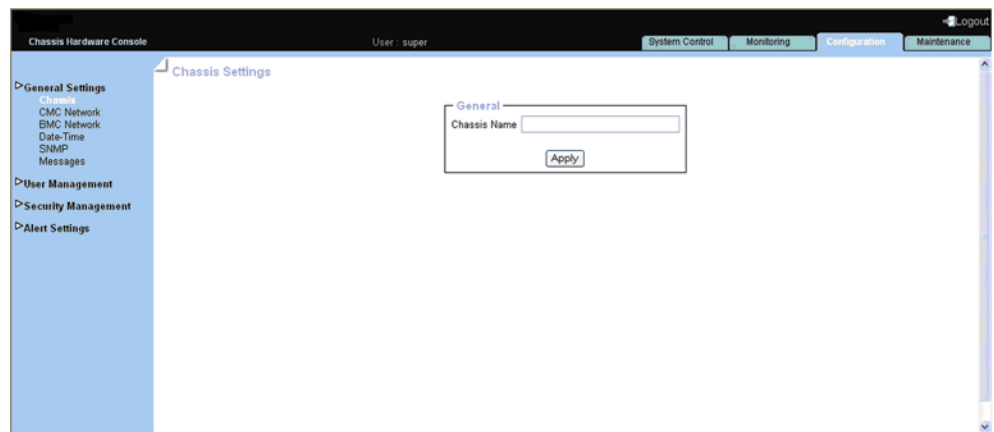
Figure 5-1.   Chassis Settings page

2. Complete the field with the required name and click **Apply**.

5.2   Configuring the CMC network

The CMC Network Settings page allows you to configure or modify network settings for remote access to the Chassis Hardware Console with a web browser.

Prerequisites

- Viewing: all users

- Operations: root users

⚠️   CAUTION
Good knowledge in network administration is required. If new network settings are incorrect, you may lose the connection to the console. You are advised to note current settings before entering new values so that you can restore the connection if needed.

Procedure

1. Open the **Configuration** tab and select **General Settings > CMC Network** to display the **CMC Network Settings** page.

Figure 5-2.   CMC Network Settings page

The following table explains how to complete network setting fields:

General box	
IP Auto-Configuration	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) **BOOTP**: Network settings are retrieved from a BOOTP server
Preferred Host Name	Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if auto-configuration is disabled. The static IP address you want to use (Factory-default value: 192.168.1.176).
Subnet Mask	Accessible only if auto-configuration is disabled. The subnet mask you want to use (Factory-default value: 255.255.255.0).
Gateway IP Address	Accessible only if auto-configuration is disabled. Your router IP address, if applicable.
Primary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your primary DNS server IP address, if applicable.
Secondary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your secondary DNS server IP address, if applicable.
Advanced Box	
Remote Console and HTTPs Ports	Port number used for secure HTTPS connections and for the remote console (Factory-default: 443).
HTTP Port	Port number used for standard HTTP connections (Factory-default: 80).
TELNET Port	Telnet port number (Factory-default: 23).
SSH Port	Secure Shell (SSH) port number (Factory-default: 22).
Enable TELNET Access	Select this option to connect using a Telnet client.
Enable SSH Access	Select this option to connect using an SSH client.
Disable Setup Protocol	Select this option to prevent blade system from being automatically detected or re-detected on the network when installing other devices.

Network Adapter Configuration Box	
Current Parameters	Displays current network adapter settings.
Speed	LAN interface speed. **Autodetect**: Automatically adjusts the interface speed (factory-default). **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.

Table 5-1.   CMC Network Settings page description

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

Note   You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

What to do if an incident occurs?

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

- The LAN cable may be detached

- Network settings are incorrect

- Your network may be down

CAUTION
Changing CMC network setting may result in a loss of remote connection to the console.

5.2.1 Configuring the BMC network

The BMC Network Settings page allows you to configure or modify network settings for remote access to the Blade Hardware Console with a web browser.

Prerequisites

- Viewing: all users
- Operations: root users

⚠️ **CAUTION**
Good knowledge in network administration is required. If new network settings are incorrect, you may lose the connection to the console. You are advised to note current settings before entering new values so that you can restore the connection if needed.

Procedure

1. Open the **Configuration** tab and select **General Settings**, and click **BMC Network** to display the BMC Network Settings page.

Figure 5-3.   BMC Network Settings page

The following table explains how to complete network setting fields:

General box	
Server Blade Slot Number	This drop-down lists all the bullx B500 compute blades/ bullx B505 accelerator blades. **Show Details**: Provides the information of the bullx B500 compute blade/ bullx B505 accelerator blades.
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.

General box	
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 auto-configuration is disabled. The static IP address you want to use (Factory-default value: 192.168.1.217).
Subnet Mask	Accessible only if auto-configuration is disabled. The subnet mask you want to use (Factory-default value: 255.255.255.0).
Gateway IP Address	Accessible only if auto-configuration is disabled. Your router IP address, if applicable.
Primary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your primary DNS server IP address, if applicable.
Secondary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your secondary DNS server IP address, if applicable.
Advanced Box	
Remote Console and HTTPs Ports	The port number that is used for secure HTTPS connections and for the remote console (Factory-default: 443).
HTTP Port	The port number that is used for standard HTTP connections (Factory-default: 80).
TELNET Port	The Telnet port number (Factory-default: 23).
SSH Port	The Secure Shell (SSH) port number (Factory-default: 22).

Table 5-2.   BMC Network Settings page description

2. Complete the above fields to comply with your network requirements and click **Apply**.

Note   You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

What to do if an incident occurs?

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

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

⚠ CAUTION
Changing BMC network settings may result in a loss of remote connections to the BMC.

5.2.2 Configuring date and time settings

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

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

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **General Settings > Date-Time** to display the **Date/Time Settings** page.

General	
UTC Offset	Allows you to set the difference between local and universal time, using the drop-down list.
User specified	Allows you to manually set the blade system internal clock. You can either manually enter the date and use the UTC Offset drop-down list or manually enter both the date and local time.
Synchronize with NTP Server	Allows you to enter the IP addresses of the NTP servers that you want to use.
View Defaults	Allows you to display factory-default values (Stored value is equal to the default).

Figure 5-4.   Date/Time Settings page

2. If required, change the **UTC Offset** value and select either **User Specified** or **Synchronize with NTP Server.**

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

Note   NTP Server configuration is obtained automatically. Ensure that the BOOTP/DHCP server used by this device provides correct time server information

5.2.3 Configuring SNMP settings

When enabled, the SNMP agent allows you to:

- Retrieve the following data from your SNMP manager:
  - Serial number
  - Firmware version
  - MAC address/IP address/Netmask/Gateway IP address
  - Power status
  - Post code

- Perform the following actions through your SNMP manager:
  - Reset to factory setting
  - Power on/off remotely

- Report the following event to your SNMP manager:
  - User logon
  - Access denied
  - Reset
  - Power on/off

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **General Settings > SNMP** to display the **SNMP Settings** page.

Figure 5-5.   SNMP Settings page

The following table explains how to complete SNMP settings fields:

General		
Area 1	**Enable SNMP Agent**: When selected, this option allows the SNMP agent to communicate with an SNMP manager.	
	System Location	blade system name.
	System Contact	blade system administrator's name or email address.
Area 2	**Use SNMPv3**: Select this option if required by your SNMP manager.	
	DES Encryption	Enables or disables the privacy provided by SNMPv3. Using privacy requires that both the SNMP manager and agent share a secret encryption key.
	Read Username	Name of an SNMP user who has read-only access to the blade system.
	Read Password	Read-only user authentication password.
	Write Username	Name of an SNMP user who has write access to the blade system.
	Write Password	Write user authentication password.
Area 3	**Use SNMPv1**: Select this option, if required by your SNMP manager.	
	Read Community	SNMP read-only community name for the blade system (example: public).
	Write Community	SNMP write community name for the blade system.
Area 4	**Download the SNMP MIB file:** This link allows you to save, as a .txt file, the blade system MIB file. This file is required by your SNMP manager to interpret trap messages.	

Table 5-3.   SNMP Settings page description

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

| **Note** | The Bull System Manager Add-on for the bullx blade system supplies the MIB file. |

3. Select Enable SNMP Agent.

4. Complete the System Location and System Contact fields.

5. Configure the SNMP agent depending on your SNMP manager:
    - If you select **Use SNMPv3**, complete the corresponding fields accordingly:
        - To allow data retrieval and event reporting only, complete the Read User Name and Read Password fields only.
        - To allow the performance of actions only, complete the Write User Name and Write Password fields only.
        - To allow data retrieval, event reporting and the performance of actions, complete the Reader User Name, Read Password, Write User Name and Write Password.

- If you select **Use SNMPv1**, complete the corresponding fields accordingly:
  - To allow data retrieval and event reporting only, complete the Read Community field only.
  - To allow the performance of actions only, complete the Write Community field only.

Important

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

---

6. Click **Apply**.

Note   You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.2.4   Setting up the messaging policy for Board and Security messages

This section describes how to set up the messaging policy for the Board and Security Messages log, which retrieves non-hardware-related events, such as user authentication, connection to the remote console, security violation, log deletion, or firmware upgrade.

Note   Hardware-related events are recorded in the System Event Log. You can set up SEL messaging policies through Alert Settings.

⚠ **CAUTION**
By default, only the Local Messaging policy is enabled for Board and Security messages. These messages will be lost if the blade chassis is powered down or if a hard reset is performed. You are strongly advised to configure and enable one or more external messaging policies (NFS, SMTP and/or SNMP).

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **General Settings > Messages** to display the **Board, Security & Remote Console Messages** Settings page.

Figure 5-6.   Board, Security & Remote Console Messages Settings page

The following table explains how to complete message settings fields:

	Messaging Policy	
Area 1	**Enable Local Messaging**	This option is selected by default and allows message entries to be displayed in the **Board & Security Messages** page (**Monitoring** tab).
	Entries per Page	Maximum number of lines displayed in each Board & Security Message page. Enter a value between 1 and 500.
Area 2	**Enable NFS Messaging**	This option allows board and security messages to be written to a file located on a Network File System (NFS) server. The size of the NFS message file is not limited: Each event is appended to the end of the file indefinitely. Depending on your hard disk space, you may have to empty or archive the file at regular intervals. **Do not use the same file name to write messages from more than a system using the same NFS shared directory**.
	NFS Server	NFS server hostname or IP address.
	NFS Share	Full pathname of the NFS shared directory. Note that the NFS shared directory is mounted immediately after you click the Apply button. To avoid error messages, use a valid NFS share value.
	NFS Message File	Name of the file used to save the board and security messages.
Area 3	**Enable SMTP Messaging**	This option allows board and security messages to be sent by email to specified recipients. Emails contain the same description strings as the local messages and the mail subject is filled with the corresponding message group (Board Message, Security, Remote Console or Authentication).
	SMTP Server	SMTP server IP address and port number. **The SMTP server must not require authentication.**
	Receiver Email Address	Example: administrator@mycompany.com
	Sender Email Address	Example: system@mycompany.com
Area 4	**Enable SNMP Messaging**	This option allows board and security messages to be sent by SNMP trap.
	Destination IP	SNMP manager IP address and port number.
	Community	(Optional) Example: public.
	Download the SNMP MIB File	Link allowing you to save, as a .txt file, the MIB file. This file is required by your SNMP manager to interpret trap messages.

Messaging Filters		
This box allows you to select message type and groups. The columns displayed in this box depend on the messaging policies enabled.		
Area 5	**Board Messages**	This group consists of the following messages: Device successfully started Board Reset performed by user… Firmware upload failed No firmware file uploaded Uploaded firmware file discarded Firmware validation failed Firmware file uploaded by user… Firmware updated by user… Internal log file cleared by user…
	Security	This group consists of the Security Violation message.
	Authentication	This group consists of the following messages: Login failed Login succeed

Table 5-4.   Board, security & Remote console Messages Settings page description

2.   Complete the **Messaging Policy** box.

3.   If necessary, modify the **Messaging Filter** box and click **Apply**.

Note   You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.3 Managing Users

Access to console features and data is based on users and privileges. You can use the **User Management** menu to implement a privilege-based user management policy that enables users to only access the features and data they require.

5.3.1 Creating a user account

The blade system is delivered with two predefined groups and one predefined user:

- Admin group with full permissions for full system access and a default super user

- User group with no permissions and no predefined users

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

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

Important

The blade 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

- Viewing: all users

- Operations: root users

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. Open the **Configuration** tab and select **User Management > Users** to display the **User Management** page.
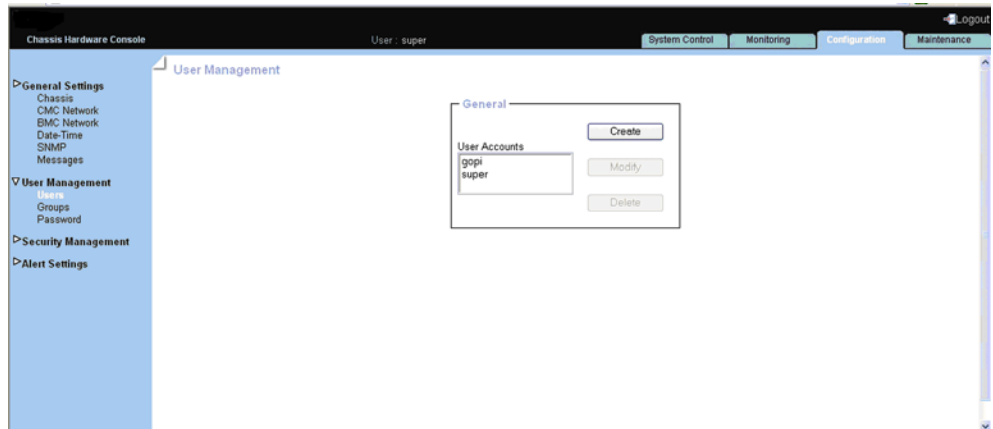
Figure 5-7.   User Management page

2. Click **Create** to open the **User Creation** box.
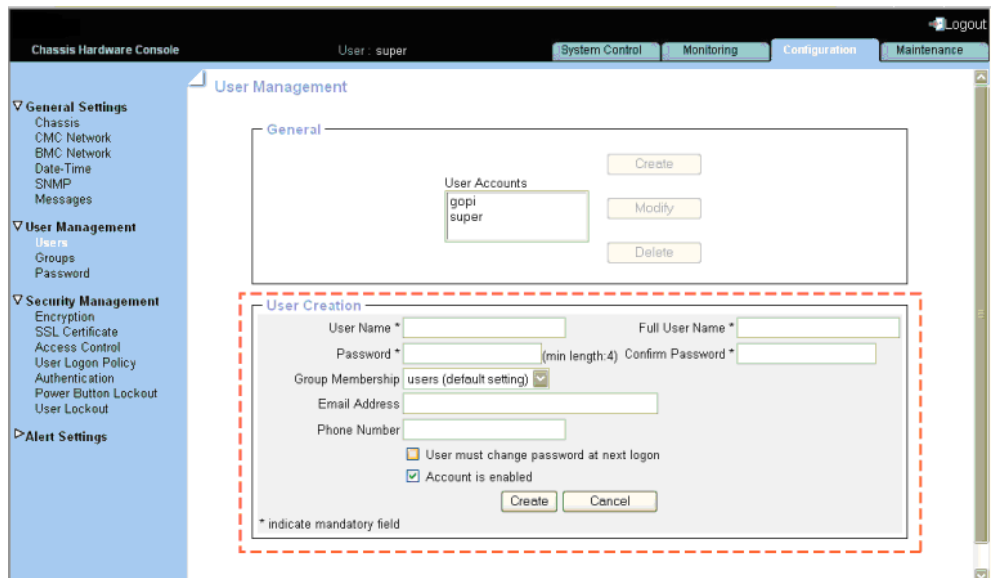
Figure 5-8.   User Creation dialog page

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

   The user is created and is displayed in the **User Accounts** box.

5.3.2 Modifying a user account

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 section 5.2.11 Modifying your Password.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Users** to display the **User Management** page.
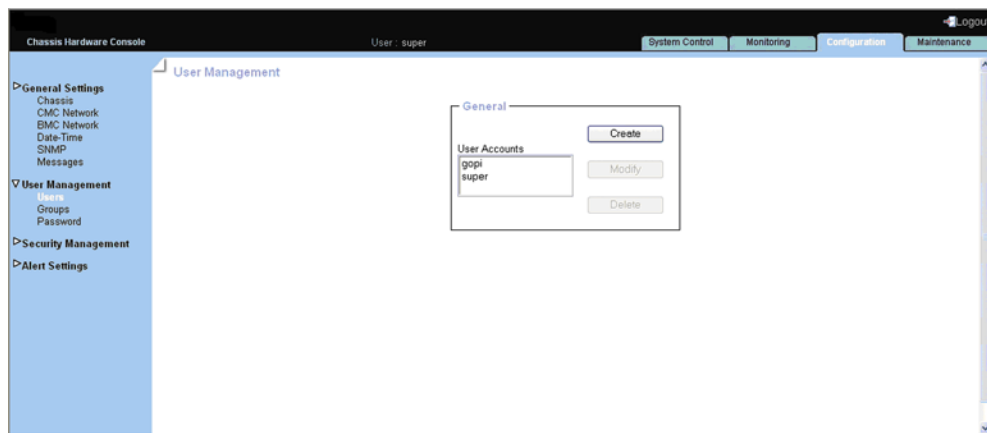
Figure 5-9.   User Management page

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.
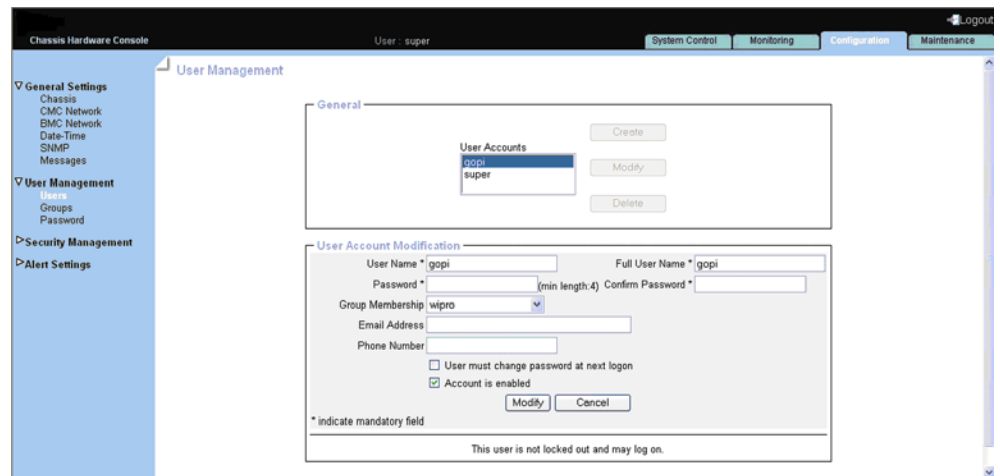
Figure 5-10. User Account Modification box

3. Modify the required fields and click **Modify**.
   User account details have been modified successfully.

5.3.3   Viewing a user account

For easy user management, you can display the basic details of any user account at any time. You may want to see 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

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Users**. The **User Management** page appears.
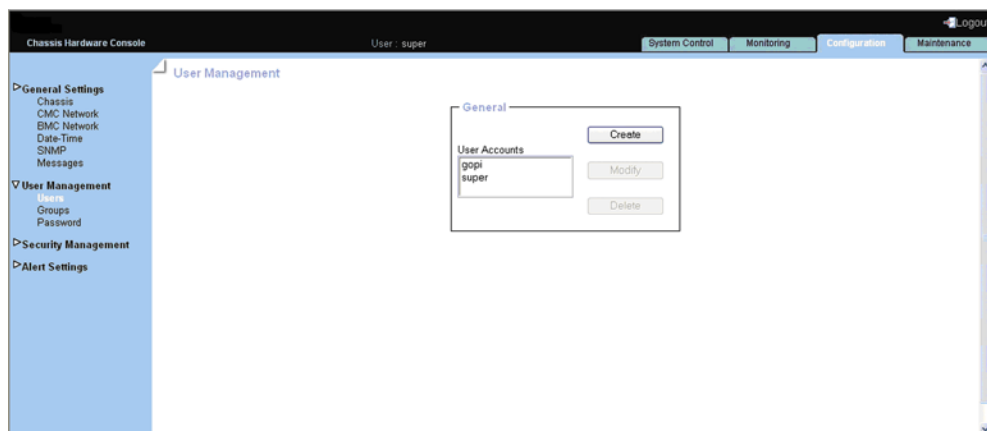
Figure 5-11. User Management page

2. In the **User Accounts** list, select a user to display the **Account Details** box.
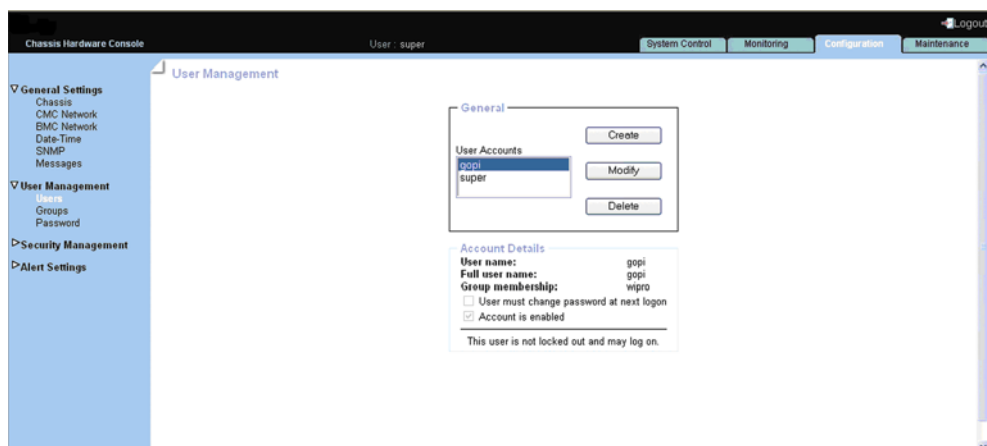
Figure 5-12. Account Details box

5.3.4   Deleting a user account

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Users** to display the **User Management** page.
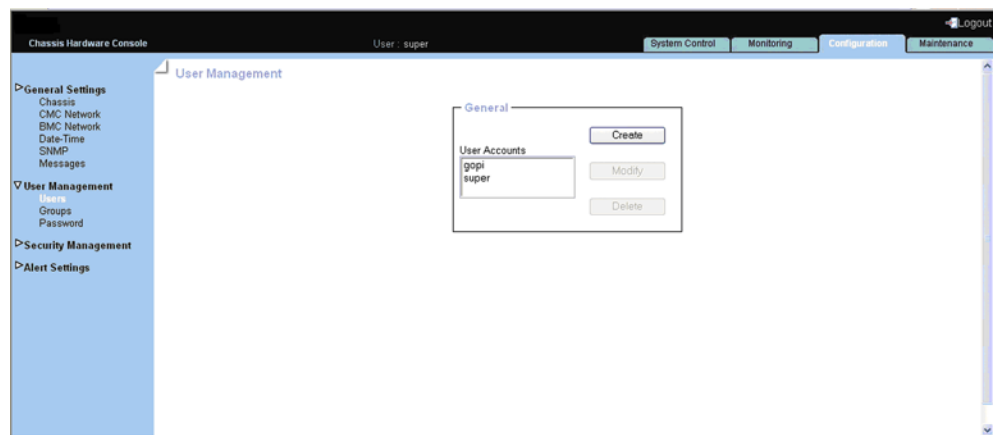
Figure 5-13. User Management page

2. Select a user in the **User Account** list box and click **Delete**.

The **User Account Deletion** box appears.
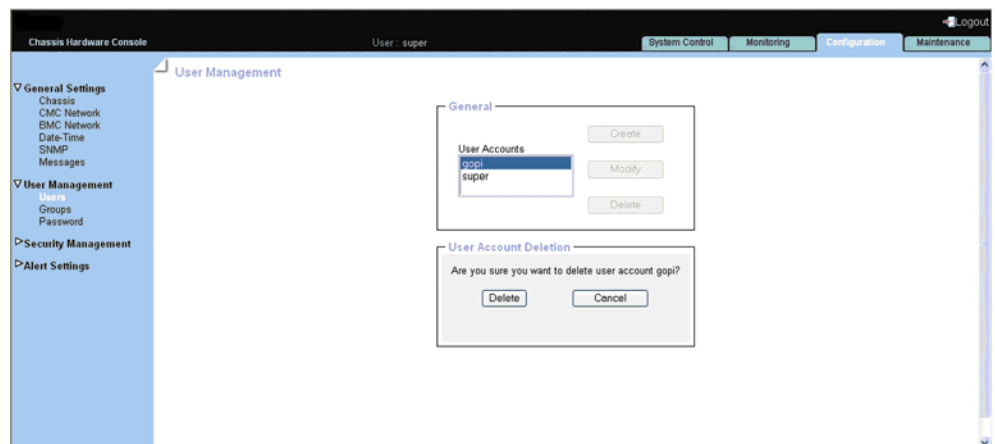
Figure 5-14. Deleting a User Account

3. Click **Delete** to confirm.

The user is removed from the list and from the associated group.

5.3.5 Disabling or enabling user accounts

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Users** to display the **User Management** page.
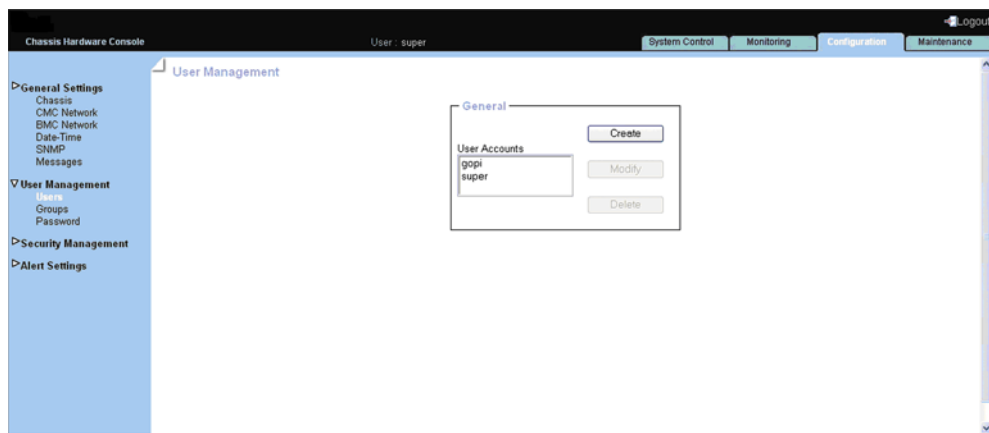
Figure 5-15. User Management page

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.
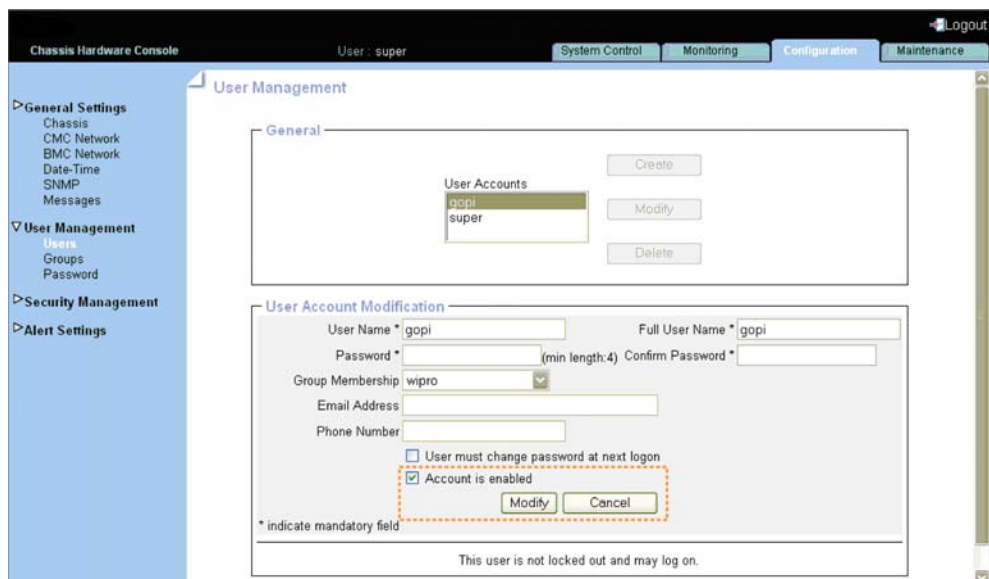
Figure 5-16. User Account Modification

3. To enable/disable the account, check/uncheck the **Account is enabled** box.

4. Click **Modify** to update the modification

5.3.6   Creating a group

The blade system is delivered with two predefined groups and one predefined user:

- Admin group with full permissions for full system access and one default super user

- User group with no permissions and no predefined users

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

Important

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

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management** > **Groups** to display the **Group Management** page.
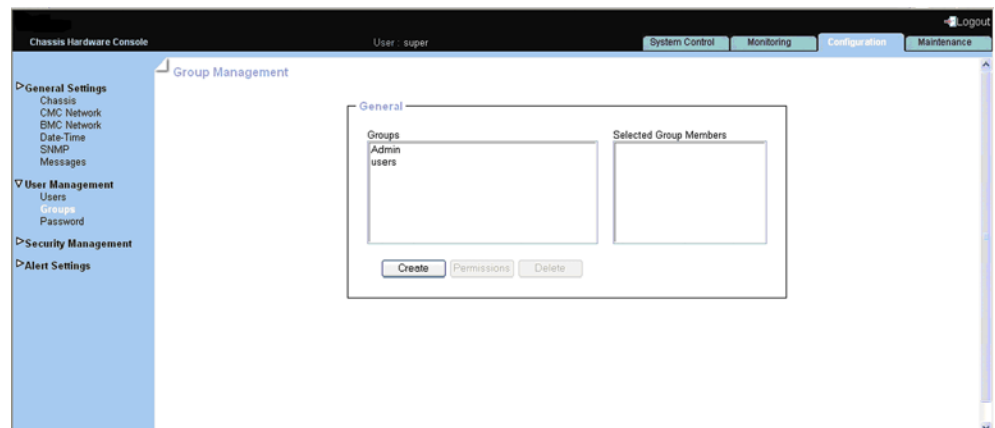
Figure 5-17. Creating a group

2. Click **Create** to open the **Group Creation** box.
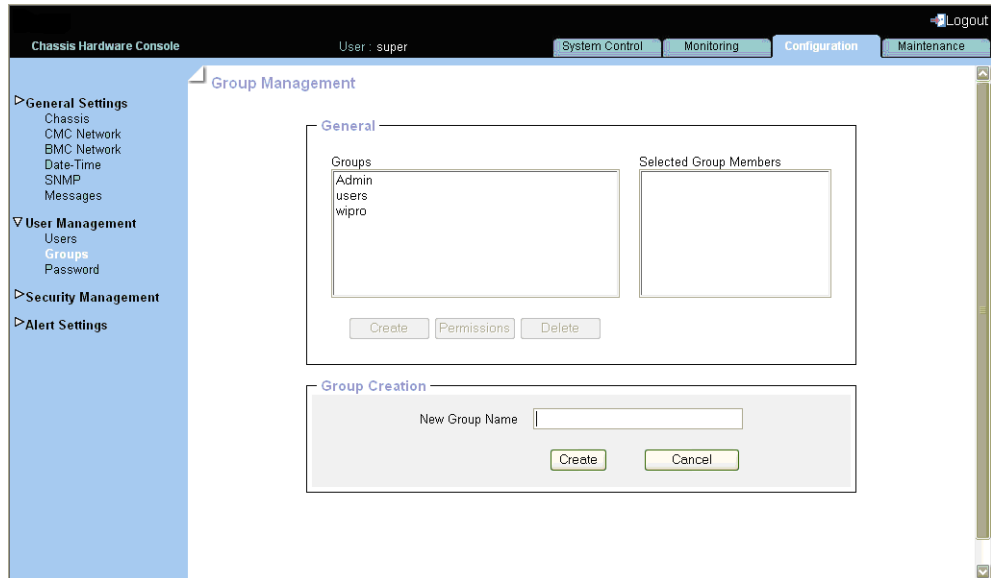
Figure 5-18. Group Creation box

3. Enter the group name in the **New Group Name** field and click **Create**. The group is created and appears in the **Groups** box. You can now proceed to define permissions and set up users for the group.

5.3.7   Viewing groups

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

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Groups** to display the **Group Management** page.
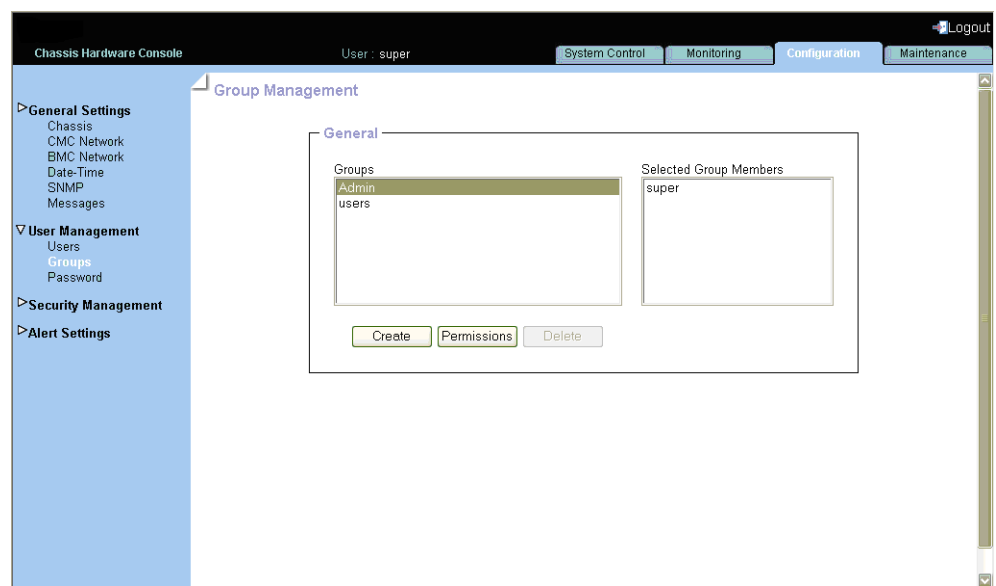
Figure 5-19. Group Management page

2. In the **Groups** list, select a group.
   The group members appear in the **Selected Group Members** box.

5.3.8 Deleting a group

You can delete an empty group when no longer needed.

---

important

Predefined groups and users cannot be deleted.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Groups** to display the **Group Management** page.
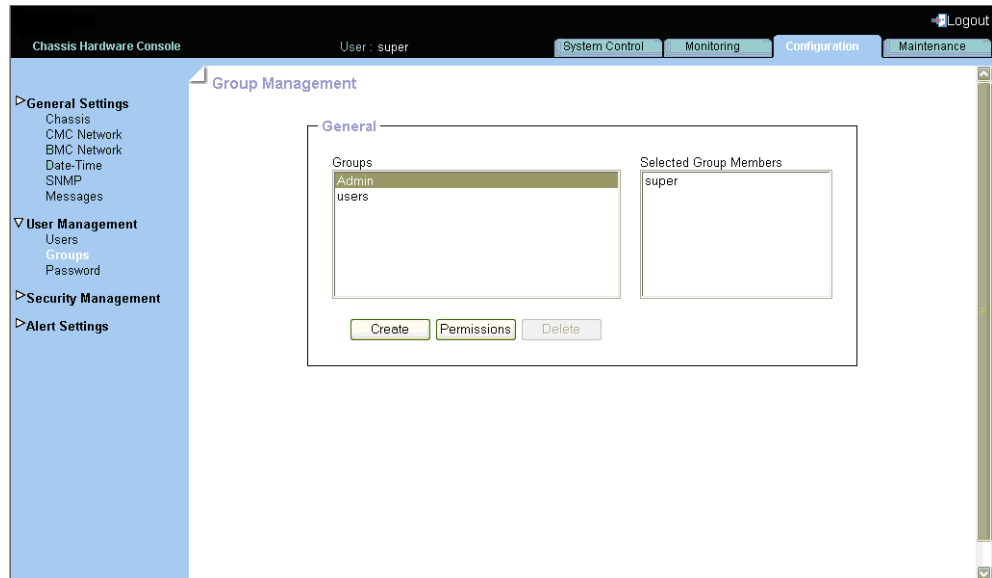
Figure 5-20. Group Management page

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.
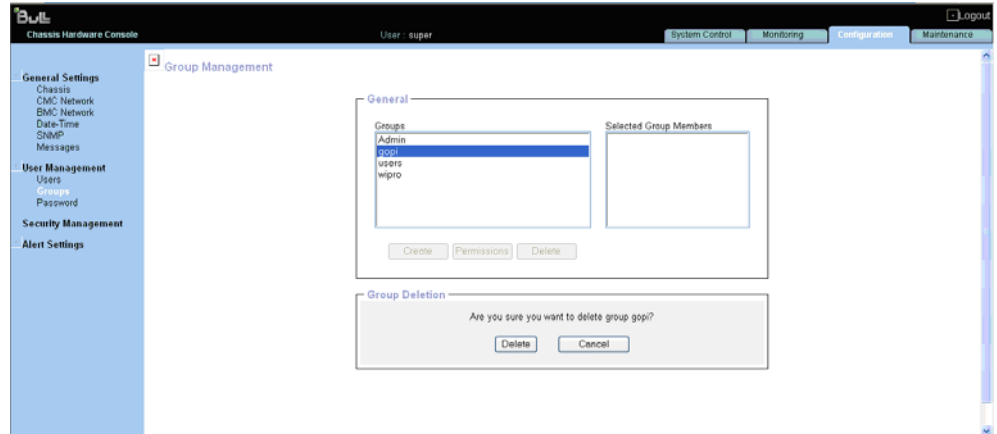
Figure 5-21. Deleting a Group

3. Click **Delete**.

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

5.3.9   Setting group permissions

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

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Groups** to display the **Group Management** page.
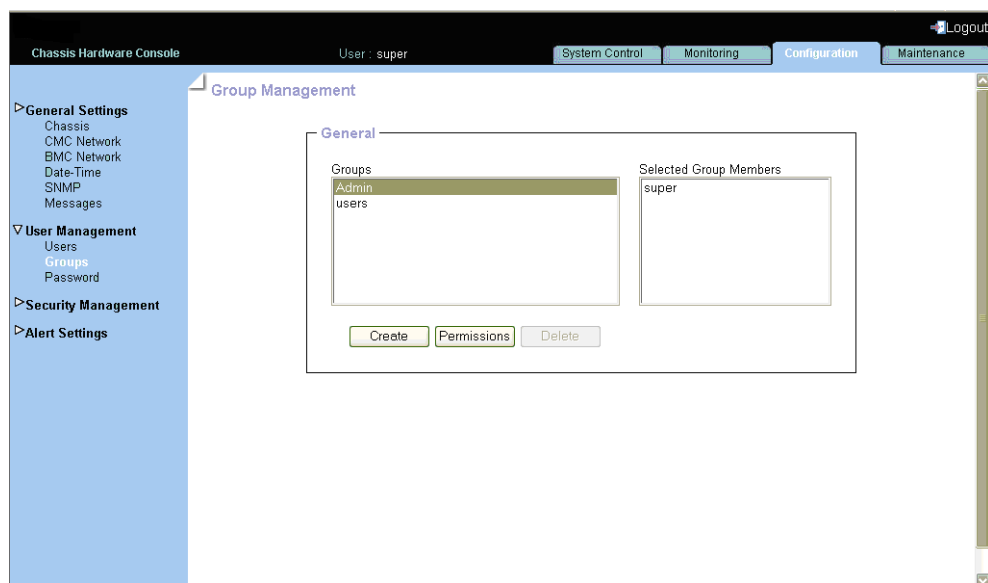
Figure 5-22. Group Management page

2. Select the group and click **Permissions** to display the **Group Permissions** page.
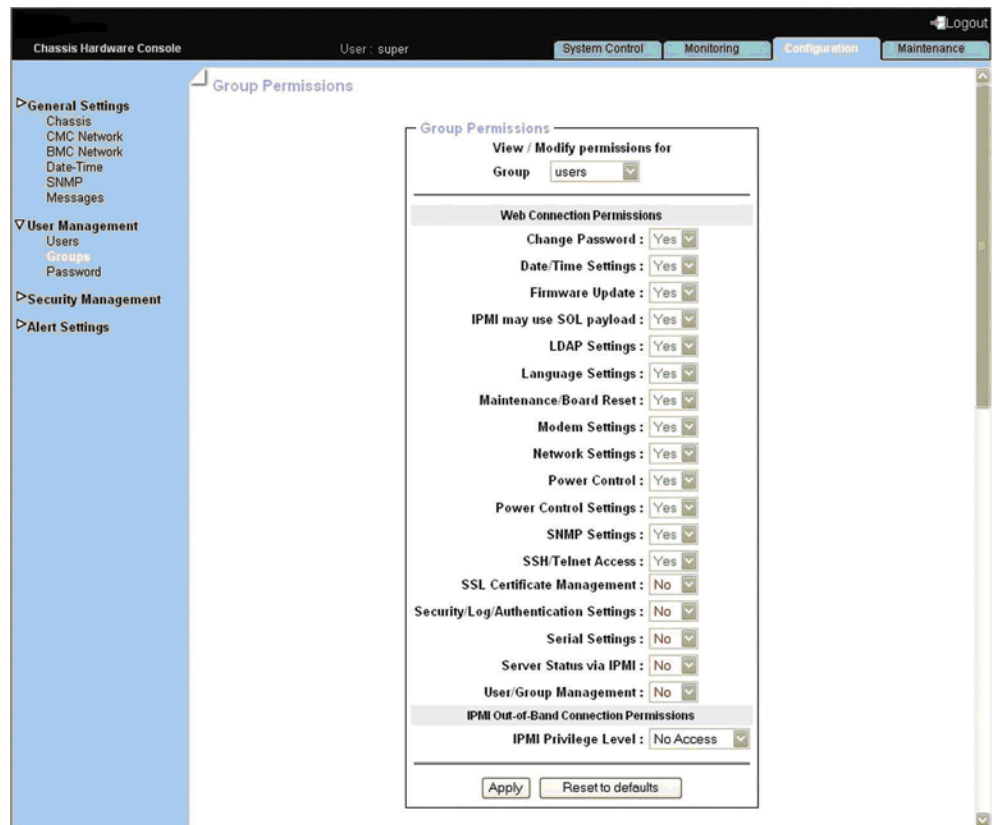
Figure 5-23. Group permission page

5.3.10   Changing group membership

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

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Users** to display the **User Management** page.
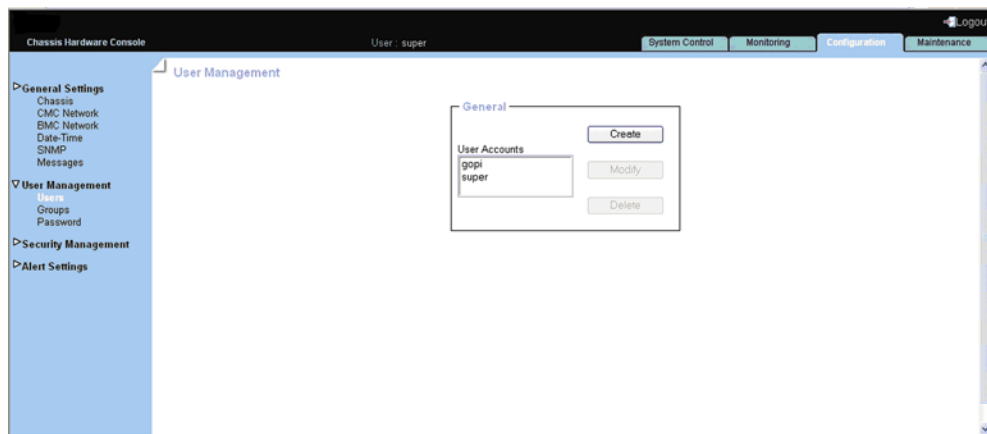
Figure 5-24. User Management page

2. Select the user account you want to modify in the **User Accounts** list 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.
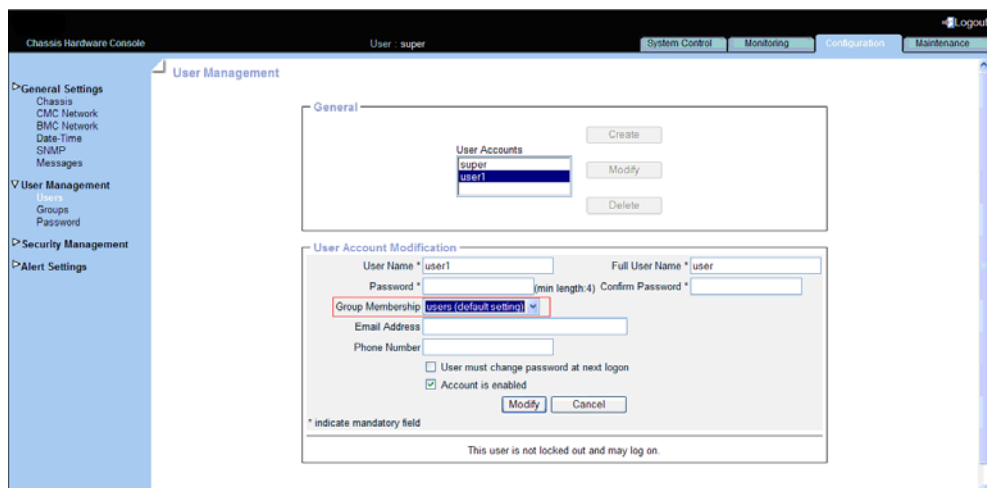
Figure 5-25. User Account Modification box

4. Click **Modify** to update the modification.

5.3.11 Modifying your password

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **User Management > Password** to open the **Password Management** page.
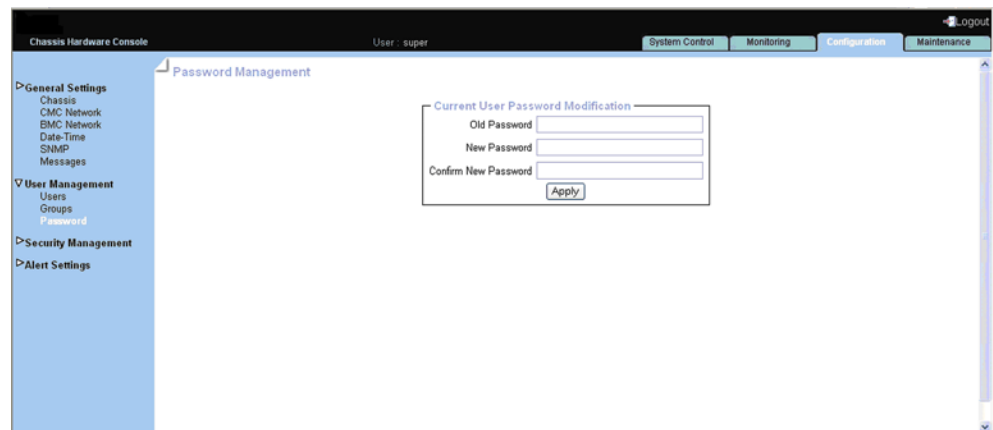
Figure 5-26. Password Management page

2. Complete all three fields.

Notes
- Minimum password length: Four characters
- Maximum password length: 32 characters
- The space character is forbidden

---

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

5.4 Configuring security management

The Configuring tab provides access to security management page, which further leads to other topics below.

5.4.1 Enabling encryption

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management > Encryption** to display the **Encryption Management** page.
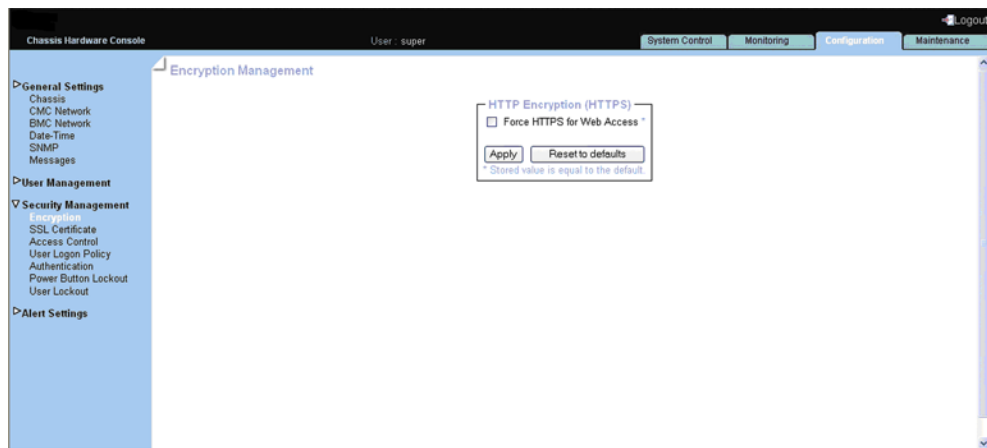
HTTP Encryption (HTTPS)	
Force HTTPS for Web Access	The HTTPS protocol requires the use of an URL in one of the following formats: https://<IP Address> https://<Hostname>

Figure 5-27. Encryption Management page

2. Select the **Force HTTPS for Web Access** check box and click **Apply**.

Note You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.4.2 Installing an SSL Certificate

You can secure Web connections by configuring the console to use the HTTPS protocol. A valid SSL certificate is required to use the HTTPS protocol. By default, a temporary certificate is delivered. For optimum security, you are advised to generate and install your own certificate.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management > SSL Certificate** to display the **SSL Certificate Management** page.

Certificate Signing Request(CSR)	
Common name	Fully Qualified Domain Name. This should be the same as the network name or a security warning will pop up when the blade system is accessed using HTTPS.
Organizational unit	Name of the department using the blade system.
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	Administrator's email address.
Certificate Signing Request(CSR)	
Challenge Password	Minimum password length: four characters.
Confirm Challenge Password	
Key length(bits)	Length of the generated key in bits, generally 1024 bits.

Figure 5-28. SSL Certificate Management page

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 checks your information, generates a signed Certificate and sends it back to you.

4. When you receive your signed certificate, use the **Certificate Upload** box to install the certificate.

5.4.3 Configuring the logon policy

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management > User Logon Policy** to display the **User Logon Policy Management** page.
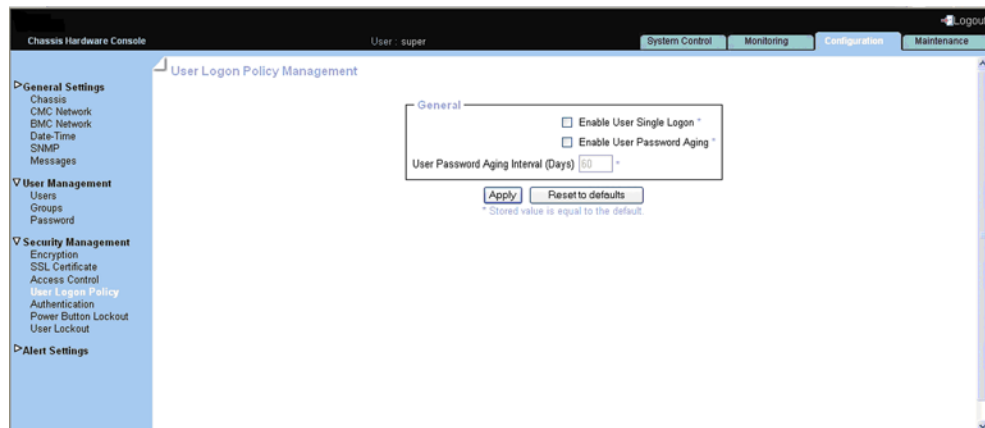
Figure 5-29. User Logon Policy Management page

2. Check/Uncheck as required and click **Apply**.

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.

Table 5-5.   User Logon Policy Management page description

Note   You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.4.4   Configuring authentication

By default, the console is configured to use its own Local Authentication mechanism to authenticate and connect users.

You can either use this mechanism and manually create groups and user accounts or use your organization's LDAP or RADIUS server to use existing user accounts.

Important

- **If you select LDAP authentication management, the LDAP database is used only 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

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management > Authentication** to display the **Authentication Management** page.
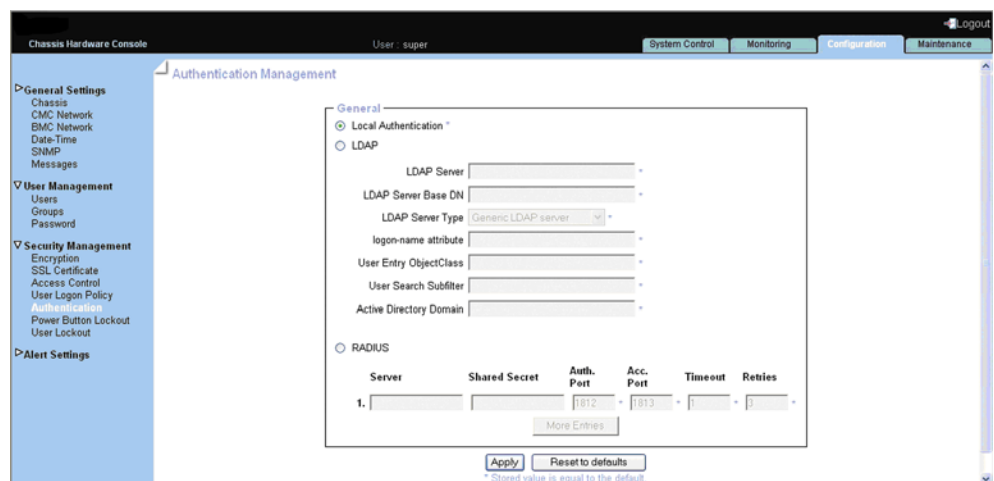
Figure 5-30. Authentication Management page

2. Depending on your needs, click **Local Authentication**, **LDAP** or **RADIUS,** complete the appropriate fields and click **Apply**.

| General	
Local Authentication	Enables the console's local authentication mechanism.
LDAP	
Enables LDAP server authentication.	
LDAP Server	LDAP server's hostname or IP address.
LDAP Server Base DN	Starting node to begin the search of user accounts. Example: dc=users,dc=domain,dc=com
LDAP Server Type	Novell Directory Service if you are using Novell eDirectory. Microsoft Active Directory. Generic LDAP Server if you are using any other LDAP directory. Default: Generic LDAP Server
Logon Name Attribute	If you have selected Novell Directory Service or Microsoft Active
User Entry Object Class	Directory, leave fields blank to use the directory's default value. Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory. For example, cn. User Entry Object Class: Object class that identifies a user in the directory. For example, organizationalPerson.
User Search Subfilter	Restricts the search to certain user accounts. For 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. For example, users.domain.com.
RADIUS	
Enables RADIUS authentication	
Server	RADIUS server's hostname or IP address.
Shared Secret	A shared secret is a text string used as a password between the RADIUS client and the RADIUS server. You can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z, a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation mark (!) or an asterisk (*).
Auth port	RADIUS server port number used to listen to authentication requests (#1812 by default).
Acc-port	RADIUS server port number used to listen to accounting requests (#1813 by default).
Timeout	Maximum amount of time in seconds to wait for the completion of the request. If the requested job is not completed within this interval of time it is cancelled. Default:1
Retries	Number of retries if a request cannot be completed. Default: 3
More entries	If you are using several RADIUS servers, click this button to add authentication configurations.

Table 5-6.   Authentication Management page description

> **Note** You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.4.5   Enabling/Disabling power button

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management > Power Button Lockout** to open the **Power Button Lockout Management** page.
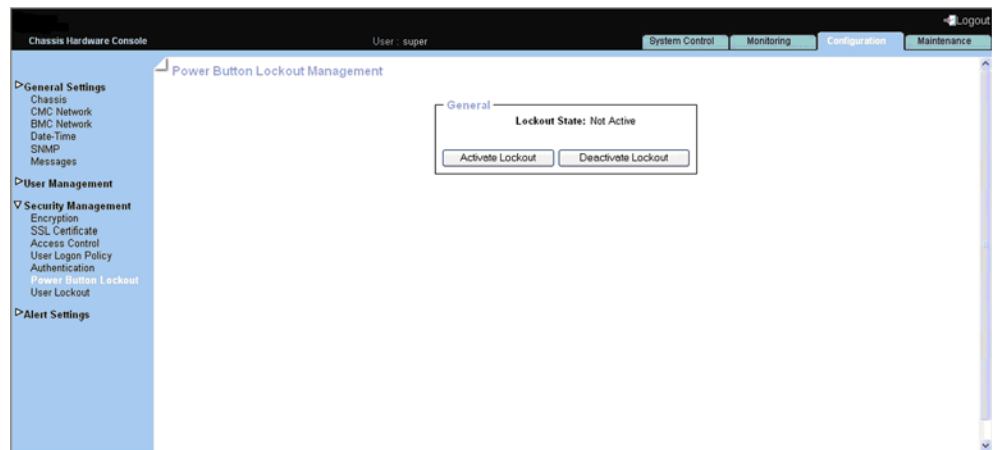
General	
Activate Lockout	The power button is locked on the LCP.
Deactivate Lockout	The power button is unlocked on the LCP.

Figure 5-31. Power Button Lockout Management page

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

5.4.6 Configuring user account lockout parameters

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Security Management** > **User Lockout** to display the **User Lockout Management** page.
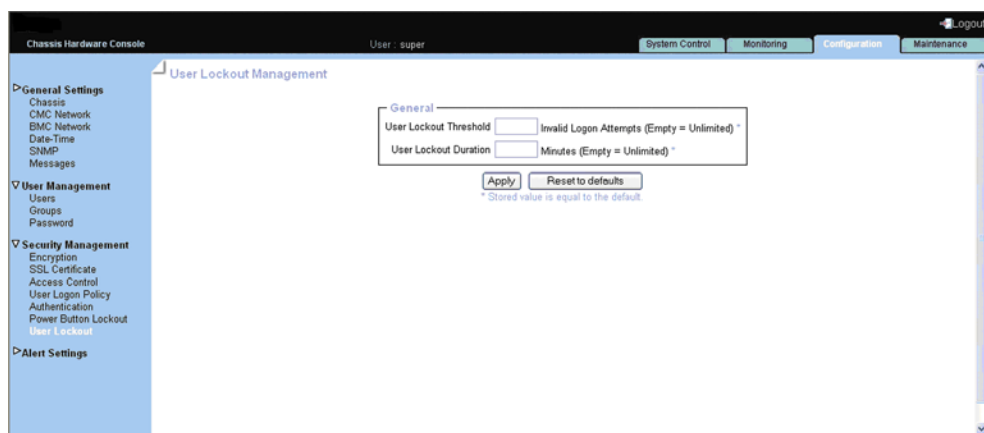
General	
User Lockout Threshold	Maximum number of invalid logon attempts before locking the user account. If you leave this field empty, the user account will never be locked.
User lockout Duration	Enter a time in minutes during which the user account is locked. Once this time is passed, the user account is automatically unlocked. If you leave this field empty, a locked user account stays locked until you unlock it manually.

Figure 5-32. User Lockout Management page

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

Note You can set the factory-default values (stored value is equal to default) by clicking **Reset to defaults**.

5.5 Configuring alerts

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

- Configure the event trap server IP address(es) and/or email recipient address(es)

- Configure the alert transmission policy(ies)

- Select the events you want to report

Note   This section explains how to set up the alert transmission feature to suit standard needs.

5.5.1 Configuring filters

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

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

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Alert Settings > Filters** to display the **Filter settings** page.

Figure 5-33. Filters settings page

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

Figure 5-34. Filter modification page

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) • **Reset**: The bullx blade system is reset. • **Power Off**: The bullx blade system is powered off. • **Power Cycle**: The bullx blade system is restarted
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.
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.
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)	

Table 5-7.   Configurable filter modification page description

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

5.5.2 Configuring alert policies

Alert policies allow you to define alert messaging strategies.

Note   Some of the features described below are reserved for advanced users.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Alert Settings > Policies** to display the **Policy Settings** page.

2. Select the first disabled alert policy and click **Modify** to display the **Policy Modification** page.
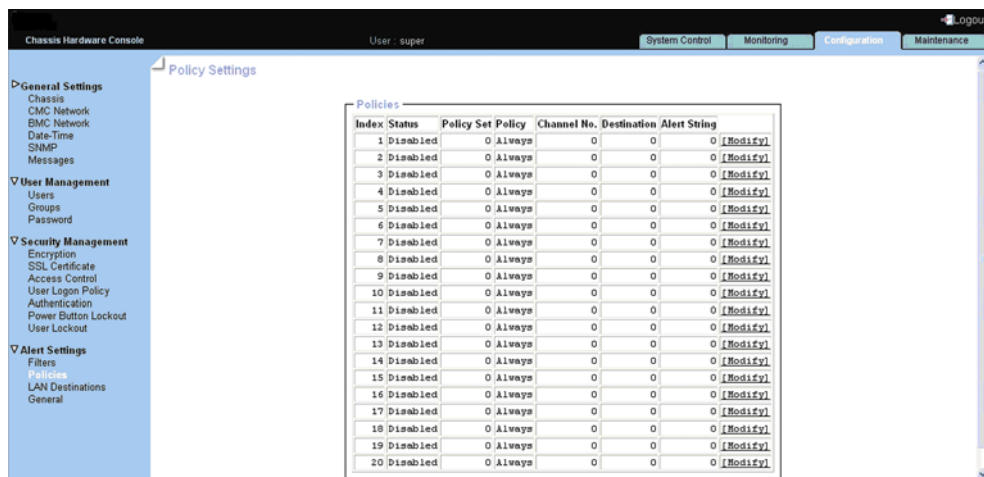
Figure 5-35. Policy Settings page

3. Select the first free disabled alert policy and click **Modify** to display the **Policy Modification** page.
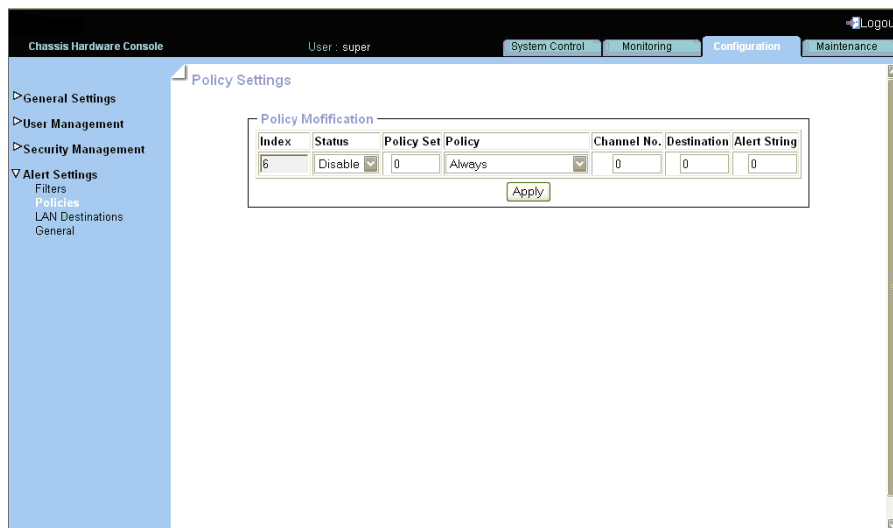
Figure 5-36. Policy Modification page

4. Complete the required fields using the following table and click **Apply**.

Policy Modification	
Index	Read-only.
Status	**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.
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 in the policy table belonging to the same policy set. As per the strategy you want to apply, select one of the following values: **Always**: Always sends 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 method (PET alert vs Email alert).
Channel No.	1 Read-only.
Destination	Enter the predefined number used to identify the destination to which alert messages are to be sent. This number corresponds to the number in the ID column on the LAN Destination Settings page.
Alert String	0 Read-only.

Table 5-8.   Policy Modification page description

Notes
- 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.

- 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.

5.5.3   Configuring LAN destinations

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.

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Alert Settings > LAN Destinations** to display the **LAN Destination Settings** page.
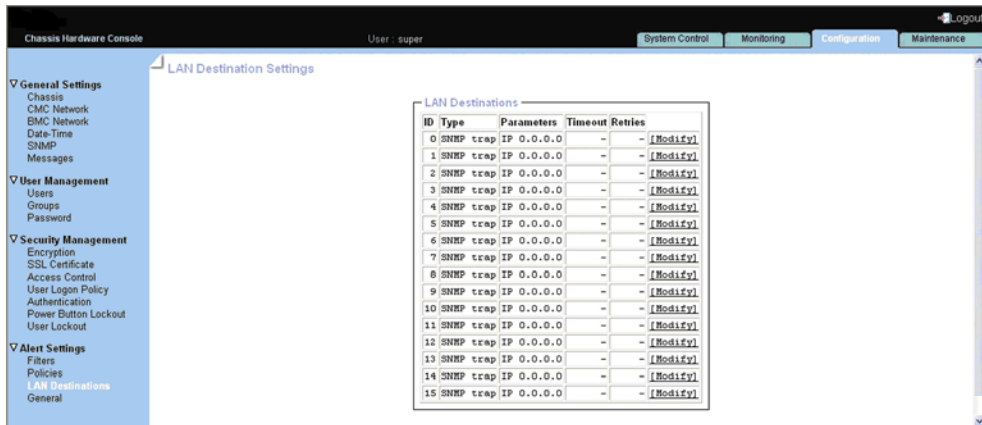
Figure 5-37. LAN destination settings page

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

Figure 5-38. Alert Settings: LAN Destination Edit page

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

Table 5-9. Alert Settings: LAN Destination Edit page description

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

5.5.4 Configuring general alert settings

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

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Configuration** tab and select **Alert Settings > General** to display the **General Settings** page.

General settings		
Event Trap	Community String	If you want to use PET alert messaging, enter the same Community String value as the one used by the SNMP trap server. Default value: public
Email Alert	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 5-39. General Settings page

2. Complete the fields as required and click **Apply** to update the modifications.

Chapter 6. Using maintenance features

This chapter explains the routine maintenance operations you can perform from the Chassis Hardware Console.

6.1   Viewing and saving embedded management board information

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

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Hardware Information > Management Board** to display the **Management Board Information** page.
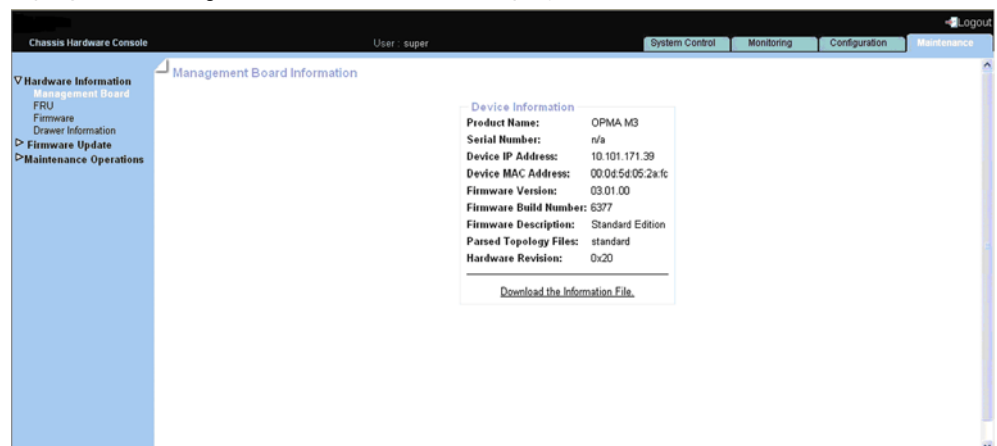
Figure 6-1.   Management Board Information page

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

6.2 Viewing and saving FRU information

FRU (Field Replaceable Unit) information can be viewed online and/or saved to an XML file and downloaded for offline analysis and archiving. This feature is particularly useful to support personnel and also allows you to maintain a record of system components after an upgrade or part replacement.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **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.
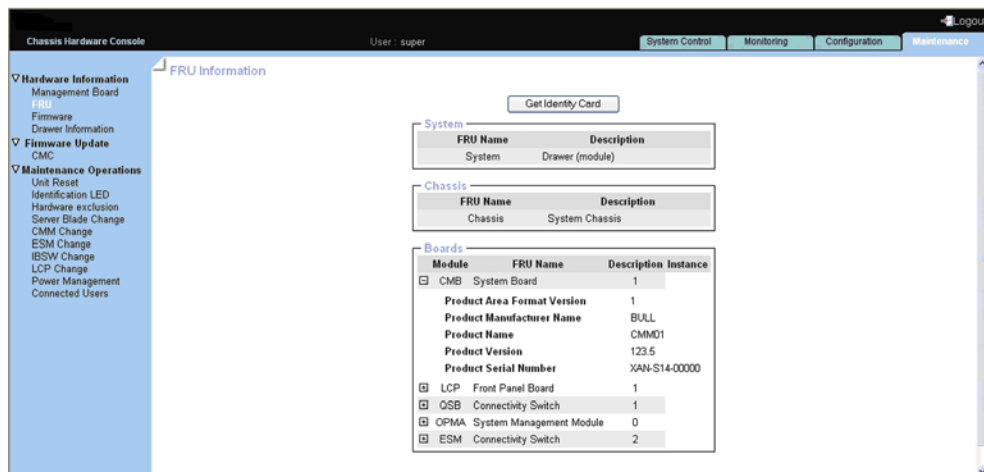
Figure 6-2.   FRU Information page

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

6.3 Viewing firmware version information

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

Procedure

Open the **Maintenance** tab and select **Hardware Information > Firmware** to display the **Firmware Information** page.

Figure 6-3.   Firmware Version Information page

6.4 Viewing drawer information

Procedure

Open the **Maintenance** tab and select **Hardware Information > Drawer Information** to display the **Drawer Information** page.
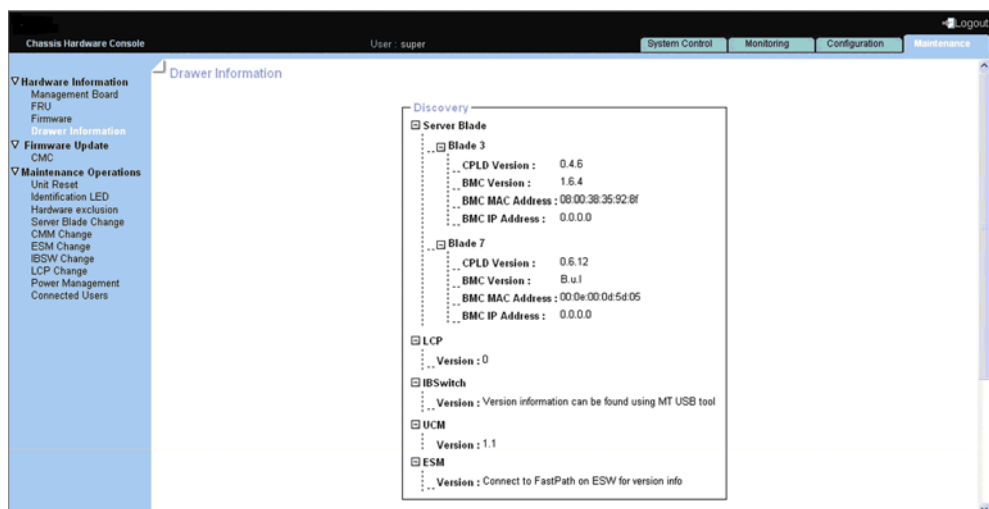
Figure 6-4.   Drawer Information page

6.5   Upgrading Firmware

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Firmware Update** > **CMC** to display the **Firmware Upload** page.
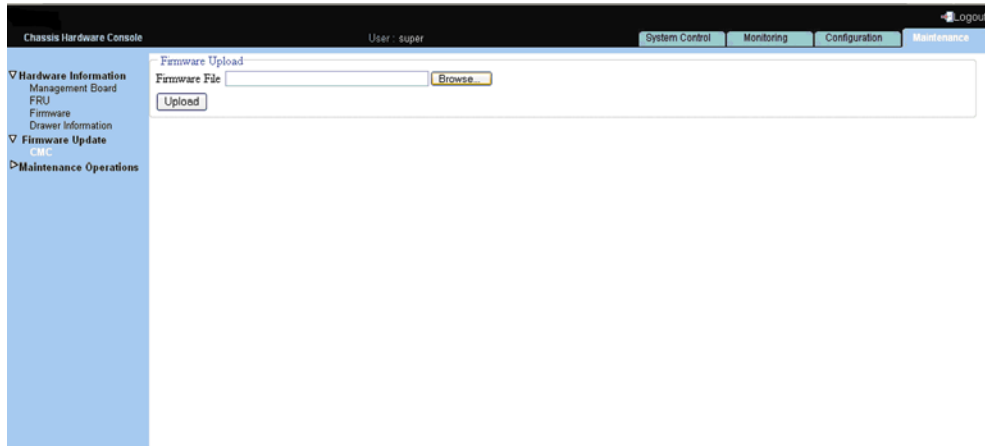
Figure 6-5.   Firmware Upload page

2. Click **Browse** to get the new version of the firmware file (or type the full file pathname in the Firmware File field) and click **Upload**.

The content of the firmware file is copied to the management board RAM and the following page appears:

Figure 6-6.   Firmware Upload page_Step2

3. Check that the new firmware version is correct and click **Update** to display **Firmware updated successfully** page.

Figure 6-7. Successful firmware update

You are then directed to Logon page in a minute. If not, click link to the login page link.

⚠ CAUTION

The upgrade process may take some time and must not be interrupted. No other actions may be performed during the process.

Once the upgrade is completed, the embedded management board software is automatically reset and you are redirected to the authentication page.

Note If the authentication page does not appear automatically, enter the bullx blade system IP address in your web browser.

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

5. To get the serial console, press **Esc** button immediately after the CMM update is complete, otherwise you need to manually restart the CMM after successful update and then press **Esc** button.

6. Type the following command in serial console to view the serial console.

```
=> erla
=> setenv serial_debug 1
=> saveenv
=> boot
```

6.6 Resetting the management board

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Maintenance Operation > Unit Reset** to display the **Management Board Reset** page.
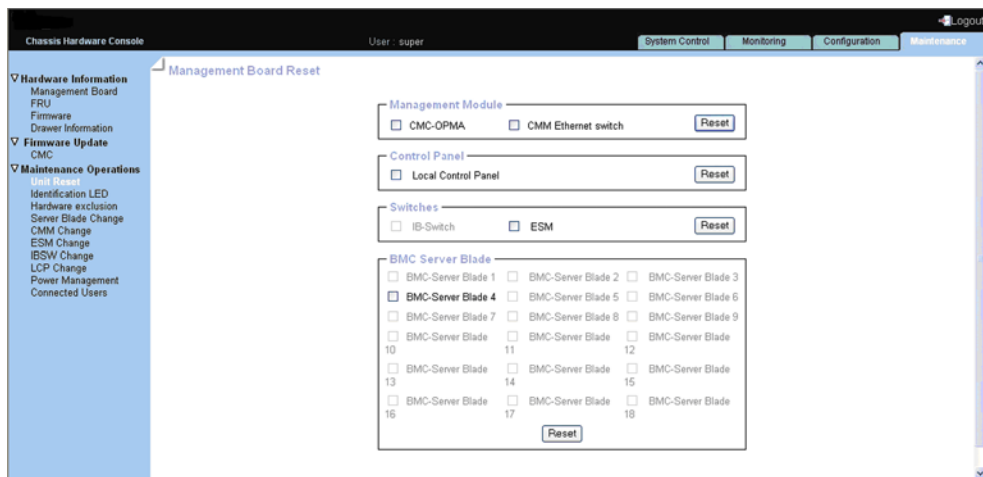
Management Board Reset page description	
Management Module	CMC-OPMA
	CMC Ethernet switch
Control Panel	Local Control Panel
Switches	IB-Switch (QSM)
	ESM
BMC-Server Blade	compute blade/ accelerator blade numbers

Figure 6-8.   Management Board Reset page

2. Check/Uncheck the box(es) as required and click **Reset**.

6.7 Enabling/Disabling LEDs

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance tab** and select **Maintenance Operations > Identification LED** to open the **Identification LED Management** page.
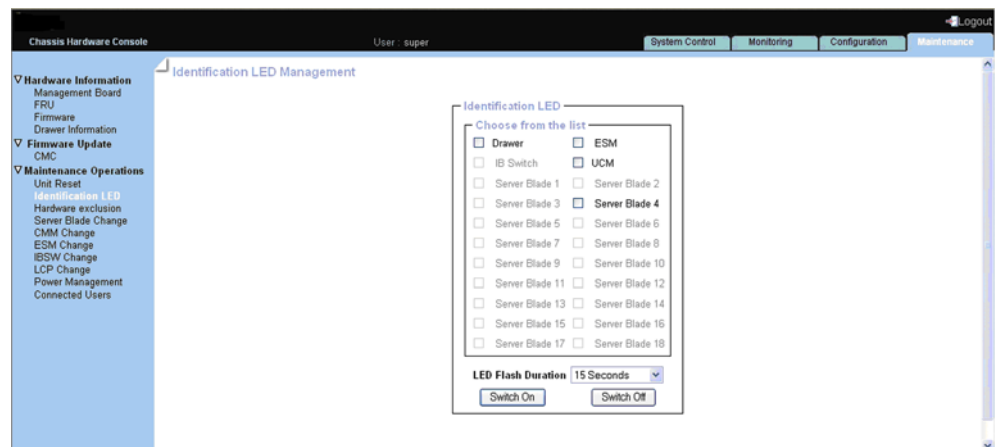
Figure 6-9.   Identification LED Management page

2. From the **Identification LED** box, check/uncheck required button.

3. Click the **Switch On/Switch Off** button in order to enable/disable LEDs.

You can set the LED flash duration for **15 Seconds**, **60 Seconds**, or **Permanent** by selecting the LED Flash Duration drop-down. Default is 15 seconds

6.8 Excluding hardware

The Chassis Hardware Console allows you to exclude compute blades/ accelerator blades statically. The system must be powered Off to select the components to exclude and the modification is taken into account at next power On.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance tab** and select **Maintenance Operations > Hardware Exclusion** to open the **Hardware Exclusions management** page.
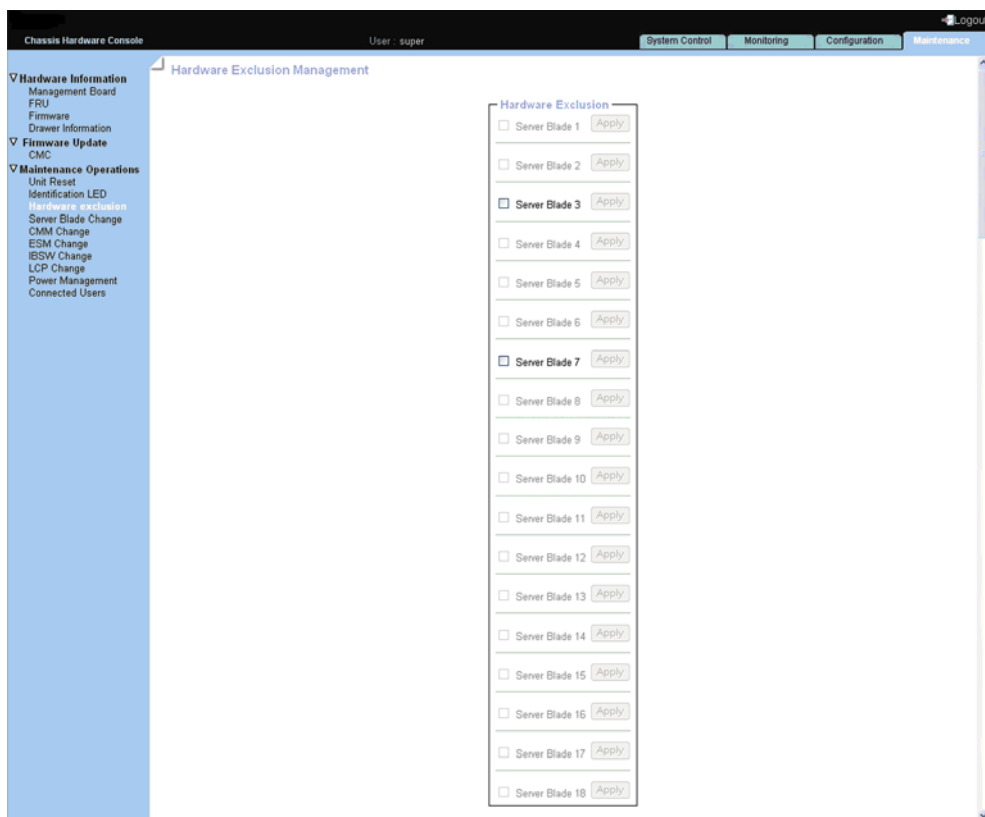
Figure 6-10. Hardware Exclusion Management page

2. Select the check box(es) corresponding to the compute blade/ accelerator blade to exclude and click **Apply**.

3. Power on the system to apply the modification.

6.9 Managing compute blade/accelerator blade removal/insertion

This feature manages the removal/insertion of compute blades/ accelerator blades from the Chassis Hardware Console and is required when servicing compute blades/accelerator blades.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance tab** and select **Maintenance Operations > Server Blade Change** to open the **Server blade Management** page.
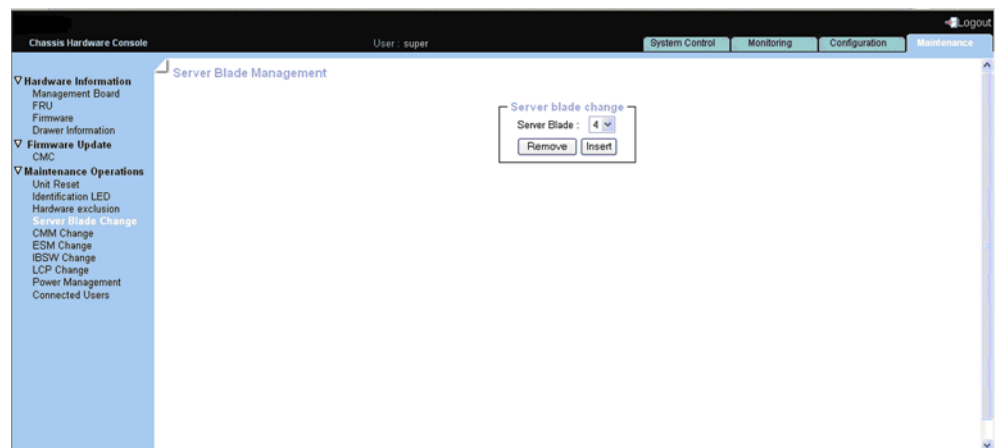
Figure 6-11. Sever Blade Management page

2. Select the **Server Blade** number from the drop-down.

3. Click **Remove/Insert** as required.

4. If the operation is to remove, blade should be in power off state, otherwise warning will be displayed. If the blade is in off state then ID LED will start blinking.

6.10 Managing CMM removal/insertion

This feature manages the removal/insertion of the CMM from the Chassis Hardware Console and is required when servicing the CMM.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance tab** and select **Maintenance Operations > CMM Change** to open the **CMM Management** page.
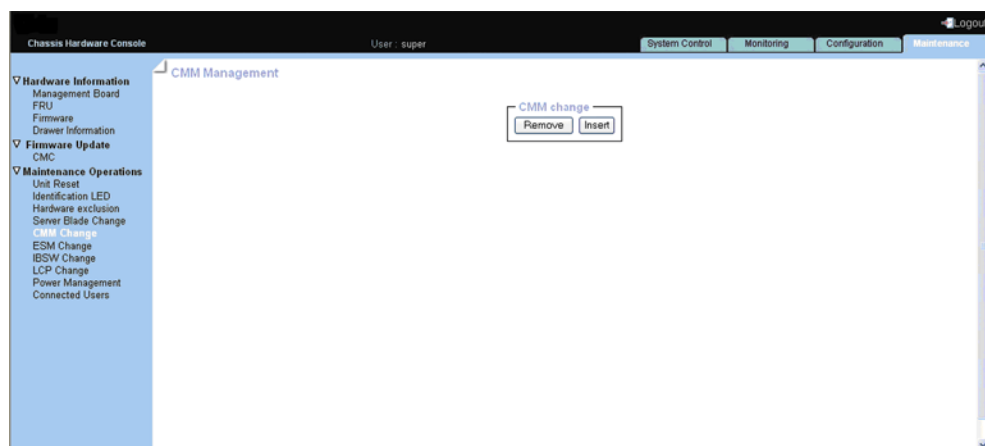
Figure 6-12. CMM Management page

2. Click **Remove/Insert** as required.

6.11   Managing ESM removal/insertion

This feature manages the removal/insertion of the ESM from the Chassis Hardware Console and is required when servicing the ESM.

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Maintenance Operations > ESM Change** to open the **ESM Management** page.
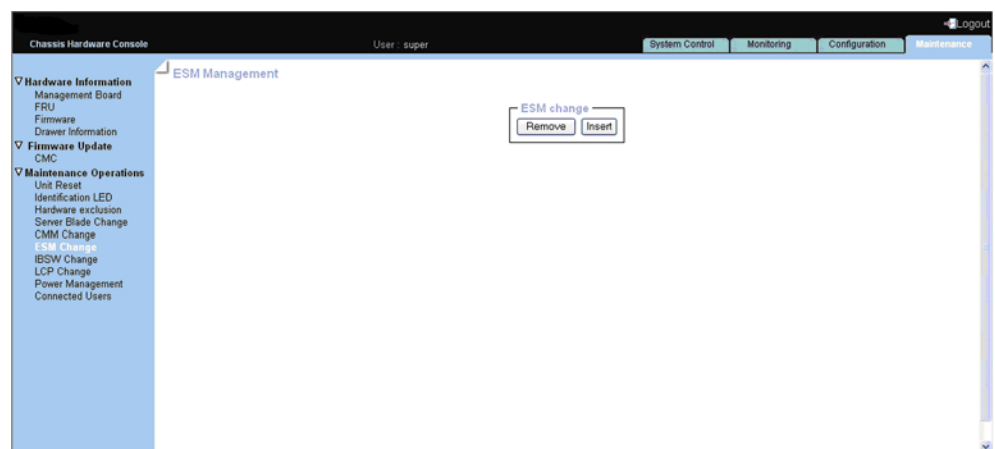
Figure 6-13. ESM Management page

2. Click **Remove/Insert** as required.

6.12   Managing QSM removal/insertion

This feature manages the removal/insertion of the QSM from the Chassis Hardware Console and is required when servicing the QSM.

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Maintenance Operations > IBSW Change** to open the **IBSW Management** page.
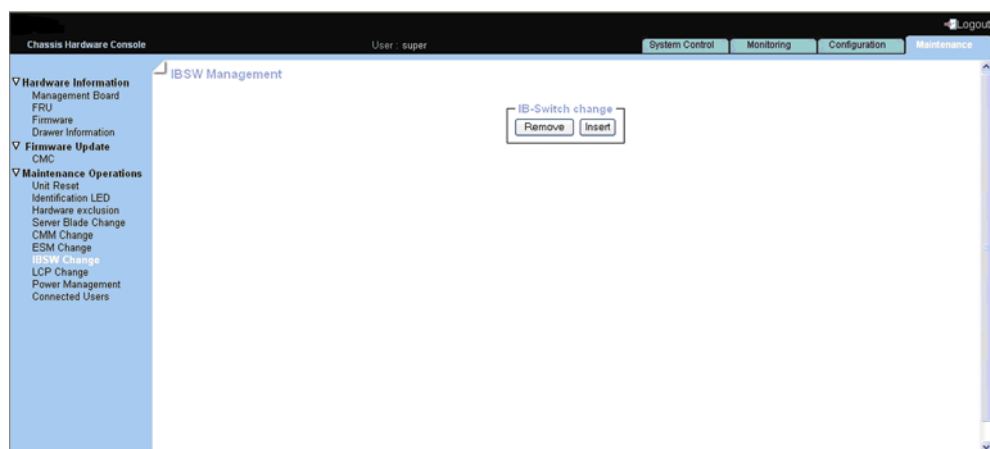
Figure 6-14. IBSW Management page

2. Click **Remove/Insert** as required.

6.13 Managing LCP removal/insertion

This feature manages the removal/insertion of the LCP from the Chassis Hardware Console and is required when servicing the LCP.

Prerequisites

- Viewing: all users
- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Maintenance Operations > LCP Change** to open the **LCP Management p**age.
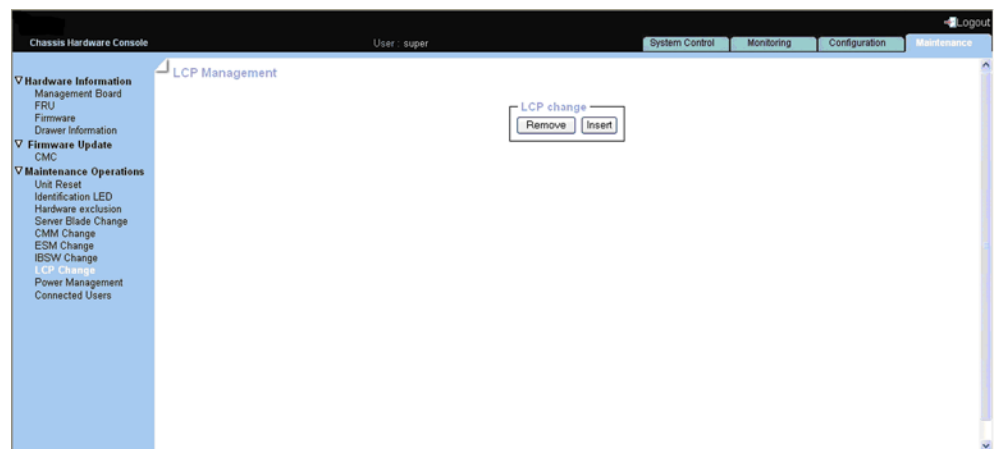
Figure 6-15. LCP Management page

2. Click **Remove/Insert** as required.

6.14   Managing Power

The Power Management page is divided into three areas:

- Whole drawer power (all the blades) used to check system power status

- Server blade used to perform routine power on/off sequences

- IB switch power used to perform power on/off sequences

Prerequisites

- Viewing: all users

- Operations: root users

Procedure

1. Open the **Maintenance** tab and select **Maintenance Operations** > **Power Management** to open the **Power Management** page.

Figure 6-16. Power Management page

Whole drawer power	
Drawer power status	Provides the status of drawer power at AC cable plugging. • **Deep stand-by**: The Deep stand-by state is the lowest power consumption waking state for the drawer • **Light stand-by**: The Light stand-by state is moderate consumption working state for the drawer. • **Unlocked**: This state is the functional state of the drawer
Drawer power on mode	Provides the status of drawer power on mode. • **Full power on**: This means all the blades and other boards are powered on when the drawer powering on is launched • **Unlocked**: This means all the blades and other boards are unlocked (12 V hot swap enabled) when the drawer powering on is launched
Start mode	Provides the status of start mode. • **Deep Stand-by**: In this mode, the compute blade/accelerator blade stays in stand-by off state (i.e. BMC not running) • **Light Stand-by**: In this mode, the compute blade/accelerator blade state becomes stand-by on (i.e. the BMC will be running) • **Unlocked Power**: In this mode, the compute blade/accelerator blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)
Eco mode	Provides the status of Eco mode. • **Yes**: This forces drawer to silent mode. (The drawer can be configured to save the energy when the compute blades/accelerator blades are not used any more. The drawer passes in an awaken state with very low power consumption (deep stand-by state) as soon as blades inactivity will be detected) • **No**: This forces drawer to off

Server blade	
Power	Compute blade/ accelerator blade number.
Presence status	• **Present**: The corresponding compute blade/accelerator blade is Present • **Absent**: The corresponding compute blade/accelerator blade is Absent
Power status	• **Off**: The corresponding compute blade/ accelerator blade is powered Off • **On**: The corresponding compute blade/ accelerator blade is powered On • **Unknown**: The corresponding compute blade/ accelerator blade is Absent
IB switch power	
Presence status	Provides the presence of Quad Switch Module. • Absent: The Quad Switch Module is absent • **Present**: The Quad Switch Module is present
Power status	Provides the power status of the Quad Switch Module. • **Unknown**: The Quad Switch Module is absent • **Stand-by off**: The Quad Switch Module is powered Off • **On**: The Quad Switch Module is powered On
IB switch silent mode	Provides the status of IB silent mode. • **Yes**: The IB switch silent mode is set to silent • **No**: The IB switch can be explicitly powered on/off.

Table 6-1.   Power Management page description

2. Click the buttons as required.

You can refresh status of compute blade/ accelerator blade by clicking the **Refresh Blade Status** button.

6.15   Viewing connected users

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

Procedure

Open the **Maintenance** tab and select **Maintenance Operations** > **Connected Users** to display the **Connected Users Information** page.

Figure 6-17. Connected Users Information page

Appendix A. Specifications

Dimensions /Weight	
Height	7U – 31.1 cm (12.24 in)
Width	48 cm (19 in)
Depth	74 cm (29.13 in)
Weight (maximum)	126 kg (278 lb)
Operating Limits	
Dry bulk temperature range	+10 °C to +30 °C (50 °F to 86 °F)
Relative humidity (non-condensing)	8% to 90% (Gradient 5% /h)
Maximum wet bulb temperature	+16 °C (60.8 °F)
Moisture content	0.019 kg water/kg dry air
Pressure / Elevation	Sea level < 2500 m
Non-Operating Limits	
Dry bulk temperature range	+5°C to +50°C (+41°F to +122°F)
Relative humidity (non-condensing)	5 to 95% (Gradient 30 %)
Maximum wet bulb temperature	+28°C (+82.4°F)
Moisture content	0.024 kg water/kg dry air
Shipping Limits	
Dry bulk temperature range	-40 °C to +70 °C (-40 °F to 158 °F) (Gradient 25° C/h (77° F))
Relative humidity (non-condensing)	5 to 95 % (Gradient 30 %/h)
Power Cables	
AC (16A)	1 per PSU
PSU connector type	C19, 250 VAC, 16 A
Power cable type	C19, 16A
Electrical Specifications	
Maximum current draw	41.4 A
Power consumption	Typical: 5.5 KW, Maximum: 8.2 KW, Idle: <3 KW
Thermal dissipation	Maximum: 8260 W
Nominal voltage	210-240 VAC
Frequency	50/60Hz
Breaker Protection (Mains Power)	
PDU	16A per PSU
Maximum inrush current	210A / per quarter period

Table A.1.   Specifications

Appendix B. Troubleshooting the blade system

This appendix explains how to troubleshoot the blade system.

B.1. Predefined alert filters description

A set of predefined alert 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.

Pre-defined filters cannot be modified. 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 following table details the events associated with each predefined filter.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
1	CMM	CMM Temperature (0x01)	At or below lower critical threshold (going low).	Critical	The CMM temperature is lower than the minimum.
			At or above upper critical threshold (going high).	Critical	The CMM temperature is upper than the maximum.
			At or below lower critical threshold (going low).	Return to OK	The CMM temperature is now OK.
			At or above upper critical threshold (going high).	Return to OK	The CMM temperature is now OK.
2	ESM	ESM Temperature (0x02)	At or below lower critical threshold (going low).	Critical	The ESM temperature is lower than the minimum.
			At or above upper critical threshold (going high).	Critical	The ESM temperature is upper than the maximum.
			At or below lower critical threshold (going low).	Return to OK	The ESM temperature is now OK.
			At or above upper critical threshold (going high).	Return to OK	The ESM temperature is now OK.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
5	LCP	LCP Temperature (0x05)	At or below lower critical threshold (going low).	Critical	The LCP temperature is lower than the minimum.
			At or above upper critical threshold (going high).	Critical	The LCP temperature is upper than the maximum.
			At or below lower critical threshold (going low).	Return to OK	The LCP temperature is now OK.
			At or above upper critical threshold (going high).	Return to OK	The LCP temperature is now OK.
6	IBSW	IBSW Temperature (0x06)	At or below lower critical threshold (going low).	Critical	The IBSW temperature is lower than the minimum.
			At or above upper critical threshold (going high).	Critical	The IBSW temperature is upper than the maximum.
			At or below lower critical threshold (going low).	Return to OK	The IBSW temperature is now OK.
			At or above upper critical threshold (going high).	Return to OK	The IBSW temperature is now OK.
7	FAN 1A	FAN 1A Speed (0x07)	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
			At or below lower critical threshold (going low).	Return to OK	Fan speed is returning to normal.
8	FAN 1B	FAN 1B Speed(0x08)	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
			At or below lower critical threshold (going low).	Return to OK	Fan speed is returning to normal.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
9	FAN 2A	FAN 2A Speed (0x09)	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
			At or below lower critical threshold (going low).	Return to OK	Fan speed is returning to normal.
10	FAN 2B	FAN 2B Speed (0x0A)	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
			At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
			At or below lower critical threshold (going low).	Return to OK	Fan speed is returning to normal.
11	Blade 1	Blade1 Presence(0x0B)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
12	Blade 2	Blade2 Presence(0x0C)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
13	Blade 3	Blade3 Presence(0x0D)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
14	Blade 4	Blade4 Presence(0x0E)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
15	Blade 5	Blade5 Presence(0x0F)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
16	Blade 6	Blade6 Presence(0x10)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
17	Blade 7	Blade7 Presence(0x11)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
18	Blade 8	Blade8 Presence(0x12)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
19	Blade 9	Blade9 Presence(0x13)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
20	Blade 10	Blade10 Presence(0x14)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
21	Blade 11	Blade11 Presence(0x15)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
22	Blade 12	Blade12 Presence(0x16)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
23	Blade 13	Blade13 Presence(0x17)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present	Information	Blade is present.
24	Blade 14	Blade14 Presence(0x18)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
25	Blade 15	Blade15 Presence(0x19)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
26	Blade 16	Blade16 Presence(0x1A)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
27	Blade 17	Blade17 Presence(0x1B)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
28	Blade 18	Blade18 Presence(0x1C)	Device removed/Device absent.	Information	Blade is not present.
			Device inserted/Device present.	Information	Blade is present.
29	IBSW	IBSW Presence (0x1D)	Device removed/Device absent.	Information	IBSW is not present.
			Device inserted/Device present.	Information	IBSW is present.
30	UCM	UCM Presence (0x1E)	Device removed/Device absent.	Information	UCM is not present.
			Device inserted/Device present.	Information	UCM is present.
31	PSU-X	• PSU-1 Presence(0x1F) • PSU-2 Presence(0x20) • PSU-3 Presence(0x21) • PSU-4 Presence(0x22)	Device removed/Device absent.	Information	PSU-X is not present.
			Device inserted/Device present.	Information	PSU-X is present.
35	Blade1	Blade 1 3v3 PG(0x23)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
36	Blade2	Blade 2 3v3 PG(0x24)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
37	Blade 3	Blade 3 3v3 PG(0x25)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
38	Blade 4	Blade 4 3v3 PG(0x26)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
39	Blade 5	Blade 5 3v3 PG(0x27)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
40	Blade 6	Blade 6 3v3 PG(0x28)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
41	Blade 7	Blade 7 3v3 PG(0x29)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
42	Blade 8	Blade 8 3v3 PG(0x2A)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
43	Blade 9	Blade 9 3v3 PG(0x2B)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
44	Blade 10	Blade 10 3v3 PG(0x2C)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
45	Blade 11	Blade 11 3v3 PG(0x2D)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
46	Blade 12	Blade 12 3v3 PG(0x2E)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
47	Blade13	Blade 13 3v3 PG(0x2F)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
48	Blade 14	Blade 14 3v3 PG(0x30)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
49	Blade 15	Blade 15 3v3 PG(0x31)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
50	Blade 16	Blade 16 3v3 PG(0x32)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
51	Blade17	Blade 17 3v3 PG(0x33)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
52	Blade18	Blade 18 3v3 PG(0x34)	State Deassertion.	Information	The 3.3V power is not present.
			State Assertion.	Information	The 3.3V power is present.
53	Blade 1	Blade 1 SYSPG (0x35)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
54	Blade 2	Blade 2 SYSPG (0x36)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
55	Blade 3	Blade 3 SYSPG (0x37)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
56	Blade 4	Blade 4 SYSPG (0x38)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
57	Blade 5	Blade 5 SYSPG (0x39)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
58	Blade 6	Blade 6 SYSPG (0x3A)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
59	Blade 7	Blade 7 SYSPG (0x3B)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
60	Blade 8	Blade 8 SYSPG (0x3C)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
61	Blade 9	Blade 9 SYSPG (0x3D)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
62	Blade 10	Blade 10 SYSPG (0x3E)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
63	Blade 11	Blade 11 SYSPG (0x3F)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
64	Blade 12	Blade 12 SYSPG (0x40)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
65	Blade 13	Blade 13 SYSPG (0x41)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
66	Blade 14	Blade 14 SYSPG (0x42)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
67	Blade 15	Blade 15 SYSPG (0x43)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
68	Blade 16	Blade 16 SYSPG (0x44)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
69	Blade 17	Blade 17 SYSPG (0x45)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.
70	Blade 18	Blade 18 SYSPG (0x46)	State Deassertion.	Information	The 12V power is not present.
			State Assertion.	Information	The 12V power is present.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
71	PSU-X	• PSU-1 Input Volt(0x47) • PSU-2 Input Volt(0x48) • PSU-3 Input Volt(0x49) • PSU-4 Input Volt(0x4A)	At or below lower non-critical threshold (going low).	Critical	PSU-X input voltage lesser than expected.
			At or below lower critical threshold (going low).	Critical	PSU input voltage lesser than expected.
			At or above upper critical threshold (going high).	Critical	PSU input voltage greater than expected.
			At or above upper non-critical threshold (going high).	Critical	PSU input voltage greater than expected.
			At or below lower non-critical threshold (going low).	Return to OK	PSU input voltage returning to normal.
			At or below lower critical threshold (going low).	Return to OK	PSU input voltage returning to normal.
			At or above upper critical threshold (going high).	Return to OK	PSU input voltage returning to normal.
			At or above upper non-critical threshold (going high).	Return to OK	PSU input voltage returning to normal.
75	PSU-X	• PSU-1 Input Power Consumption (0x4B) • PSU-2 Input Power Consumption (0x4C) • PSU-3 Input Power Consumption (0x4D) • PSU-4 Input Power Consumption (0x4E)	None (Info only; no monitoring)	Information	None.

Table B-1.　Predefined alert filter numbers and description

Notes　3v3 PG (Power Good) means the 3.3V power is running in the compute blade/ accelerator blade

SYSPG (SYStem Power Good) means the 12V power is running in the compute blade/ accelerator blade

B.2. SEL messages description

This section contains additional information about messages that appear in the System Event Log.

Local Control Panel SEL messages

LCP Temperature (0x05)

Description	The LCP temperature is lower than the minimum.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 5.
	For more information on filters, see Configuring filters.

LCP Temperature (0x05)

Description	The LCP temperature is now OK.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 5.
	For more information on filters, see Configuring filters.

LCP Temperature (0x05)

Description	The LCP temperature is upper than the maximum.
	At or above upper critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Check environmental conditions, fan blades, AC etc…
Comments	This log corresponds to sensor number 5.
	For more information on filters, see Configuring filters.

LCP Temperature (0x05)

Description	The LCP temperature is now OK.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 5.
	For more information on filters, see Configuring filters.

Chassis Management Module SEL messages

CMM Temperature (0x01)

Description	The CMM temperature is lower than the minimum.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 1.
	For more information on filters, see Configuring filters.

CMM Temperature (0x01)

Description	The CMM temperature is now OK.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 1.
	For more information on filters, see Configuring filters.

CMM Temperature (0x01)

Description	The CMM temperature is upper than the maximum.
	At or above upper critical threshold (going high).
Severity	Critical.
Direction	Assertion
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 1.
	For more information on filters, see Configuring filters.

CMM Temperature (0x01)

Description	The CMM temperature is now OK.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 1.
	For more information on filters, see Configuring filters.

Ethernet Switch Module SEL messages

ESM Temperature (0x02)

Description	The ESM temperature is lower than the minimum.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 2.
	For more information on filters, see Configuring filters.

ESM Temperature (0x02)

Description	The ESM temperature is now OK.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 2.
	For more information on filters, see Configuring filters.

ESM Temperature (0x02)

Description	The ESM temperature is upper than the maximum.
	At or above upper critical threshold (going high).
Severity	Critical.
Direction	Assertion
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 2.
	For more information on filters, see Configuring filters.

ESM Temperature (0x02)

Description	The ESM temperature is now OK.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 2.
	For more information on filters, see Configuring filters.

Quad Switch Module SEL messages

IBSW Temperature (0x06)

Description	The IBSW temperature is lower than the minimum.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 6.
	For more information on filters, see Configuring filters.

IBSW Temperature (0x06)

Description	The IBSW temperature is now OK. At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 6. For more information on filters, see Configuring filters.

IBSW Temperature (0x06)

Description	The IBSW temperature is upper than the maximum. At or above upper critical threshold (going high).
Severity	Critical.
Direction	Assertion
Action	Check environmental conditions, fan blades, AC…
Comments	This log corresponds to sensor number 6. For more information on filters, see Configuring filters.

IBSW Temperature (0x06)

Description	The IBSW temperature is now OK. At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 6. For more information on filters, see Configuring filters.

IBSW Presence (0x1D)

Description	The IBSW is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert IBSW.
Comments	This log corresponds to sensor number 29. For more information on filters, see Configuring filters.

Description	The IBSW is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 29.
	For more information on filters, see Configuring filters.

Ultra Capacitor Module SEL messages

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_1_SENS (0xD0)

Description	UCM Capacitor 1 voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 208.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 209.
	For more information on filters, see Configuring filters.

UCM_VCAP_2_SENS (0xD1)

Description	UCM Capacitor 2 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 209. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage is lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage returning to normal. At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage greater than expected. At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage returning to normal. At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage greater than expected. At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 210. For more information on filters, see Configuring filters.

UCM_21V1_SENS (0xD2)

Description	UCM 21 voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 210.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 211.
	For more information on filters, see Configuring filters.

UCM_21V2_SENS (0xD3)

Description	UCM 21 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 211. For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage is lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 212. For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 212. For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 212. For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 212.
	For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 212.
	For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

escription	UCM 12 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 212.
	For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 212.
	For more information on filters, see Configuring filters.

UCM_12V_SENS (0xD4)

Description	UCM 12 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 212. For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage is lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 213. For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 213. For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 213. For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 213.
	For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 213.
	For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 213.
	For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 213.
	For more information on filters, see Configuring filters.

UCM_VREF_SENS (0xD5)

Description	UCM Vref voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 213.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 214.
	For more information on filters, see Configuring filters.

UCM_S1_C2_SENS (0xD6)

Description	UCM Stack 1 Capacitor 2 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 214. For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage is lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 215. For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 215 For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 215. For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 215.
	For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 215.
	For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 215.
	For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 215.
	For more information on filters, see Configuring filters.

UCM_S1_C4_SENS (0xD7)

Description	UCM Stack 1 Capacitor 4 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 215. For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage is lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 216. For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 216. For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 216. For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 216.
	For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 216.
	For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 216.
	For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 216.
	For more information on filters, see Configuring filters.

UCM_S2_C2_SENS (0xD8)

Description	UCM Stack 2 Capacitor 2 voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 216.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

UCM_S2_C4_SENS (0xD9)

Description	UCM Stack 2 Capacitor 4 voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the UCM. If the problem persists replace the UCM.
Comments	This log corresponds to sensor number 217.
	For more information on filters, see Configuring filters.

Description	UCM Stack 2 Capacitor 4 voltage returning to normal. At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 217. For more information on filters, see Configuring filters.

UCM Presence (0x1E)

Description	The UCM is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert UCM.
Comments	This log corresponds to sensor number 30. For more information on filters, see Configuring filters.

UCM Presence (0x1E)

Description	The UCM is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 30. For more information on filters, see Configuring filters.

Power Supply Unit module SEL messages

PSU-1 Presence (0x1F)

Description	The PSU-1 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert this PSU
Comments	This log corresponds to sensor number 31. For more information on filters, see Configuring filters.

PSU-1 Presence (0x1F)

Description	The PSU-1 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 31.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Volt (0x47)

Description	PSU input voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-1 Input Power Consumption (0x4B)

Description	None (Info only; no monitoring).
Severity	Information.
Direction	None.
Action	None.
Comments	This log corresponds to sensor number 75.
	For more information on filters, see Configuring filters.

PSU-2 Presence (0x20)

Description	The PSU-2 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert this PSU.
Comments	This log corresponds to sensor number 31.
	For more information on filters, see Configuring filters.

PSU-2 Presence (0x20)

Description	The PSU-2 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 31.
	For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71. For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage returning to normal. At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71. For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage lesser than expected. At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71. For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage returning to normal. At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71. For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-2 Input Volt (0x48)

Description	PSU input voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-2 Input Power Consumption (0x4C)

Description	None (Info only; no monitoring).
Severity	Information.
Direction	None.
Action	None.
Comments	This log corresponds to sensor number 75. For more information on filters, see Configuring filters.

PSU-3 Presence (0x21)

Description	The PSU-3 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert this PSU.
Comments	This log corresponds to sensor number 31. For more information on filters, see Configuring filters.

PSU-3 Presence (0x21)

Description	The PSU-3 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 31. For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage lesser than expected. At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71. For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Volt (0x49)

Description	PSU input voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-3 Input Power Consumption (0x4D)

Description	None (Info only; no monitoring).
Severity	Information.
Direction	None.
Action	None.
Comments	This log corresponds to sensor number 75.
	For more information on filters, see Configuring filters.

PSU-4 Presence (0x22)

Description	The PSU-4 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert this PSU.
Comments	This log corresponds to sensor number 31.
	For more information on filters, see Configuring filters.

PSU-4 Presence (0x22)

Description	The PSU-4 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 31.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage returning to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage returning to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage greater than expected.
	At or above upper critical threshold (going high)
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage returning to normal.
	At or above upper critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage greater than expected.
	At or above upper non-critical threshold (going high).
Severity	Critical.
Direction	Assertion.
Action	Restart the PSU. If the problem persists replace the PSU.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Volt (0x4A)

Description	PSU input voltage returning to normal.
	At or above upper non-critical threshold (going high).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 71.
	For more information on filters, see Configuring filters.

PSU-4 Input Power Consumption (0x4E)

Description	None (Info only; no monitoring).
Severity	Information.
Direction	None.
Action	None.
Comments	This log corresponds to sensor number 75.
	For more information on filters, see Configuring filters.

Blade fan SEL messages

FAN 1A Speed (0x07)

Description	Fan blade speed is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 7.
	For more information on filters, see Configuring filters.

FAN 1A Speed (0x07)

Description	Fan blade speed is returned to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 7.
	For more information on filters, see Configuring filters.

FAN 1A Speed (0x07)

Description	Fan blade speed is lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 7.
	For more information on filters, see Configuring filters.

FAN 1A Speed (0x07)

Description	Fan blade speed is returned to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 7.
	For more information on filters, see Configuring filters.

FAN 1B Speed (0x08)

Description	Fan blade speed is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 8.
	For more information on filters, see Configuring filters.

FAN 1B Speed (0x08)

Description	Fan blade speed is returned to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 8.
	For more information on filters, see Configuring filters.

FAN 1B Speed (0x08)

Description	Fan blade speed is lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 8.
	For more information on filters, see Configuring filters.

FAN 1B Speed (0x08)

Description	Fan blade speed is returned to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 8.
	For more information on filters, see Configuring filters.

FAN 2A Speed (0x09)

Description	Fan blade speed is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 9.
	For more information on filters, see Configuring filters.

FAN 2A Speed (0x09)

Description	Fan blade speed is returned to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 9.
	For more information on filters, see Configuring filters.

FAN 2A Speed (0x09)

Description	Fan blade speed is lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 9.
	For more information on filters, see Configuring filters.

FAN 2A Speed (0x09)

Description	Fan blade speed is returned to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 9.
	For more information on filters, see Configuring filters.

FAN 2B Speed (0x0A)

Description	Fan blade speed is lesser than expected.
	At or below lower non-critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 10.
	For more information on filters, see Configuring filters.

FAN 2B Speed (0x0A)

Description	Fan blade speed is returned to normal.
	At or below lower non-critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 10.
	For more information on filters, see Configuring filters.

FAN 2B Speed (0x0A)

Description	Fan blade speed is lesser than expected.
	At or below lower critical threshold (going low).
Severity	Critical.
Direction	Assertion.
Action	If the problem persists, change the fan blade.
Comments	This log corresponds to sensor number 10.
	For more information on filters, see Configuring filters.

FAN 2B Speed (0x0A)

Description	Fan blade speed is returned to normal.
	At or below lower critical threshold (going low).
Severity	Return to OK.
Direction	Deassertion.
Action	None.
Comments	This log corresponds to sensor number 10.
	For more information on filters, see Configuring filters.

Compute blade/ accelerator blade SEL messages

Blade1 Presence (0x0B)

Description	bullx B500 compute blade 1/bullx B505 accelerator blade 1 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 1.
Comments	This log corresponds to sensor number 11.
	For more information on filters, see Configuring filters.

Blade1 Presence (0x0B)

Description	bullx B500 compute blade 1/bullx B505 accelerator blade 1 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 11.
	For more information on filters, see Configuring filters.

Blade1 3v3 PG (0x23)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 35.
	For more information on filters, see Configuring filters.

Blade1 3v3 PG (0x23)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 35.
	For more information on filters, see Configuring filters.

Blade1 SYSPG (0x35)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 53.
	For more information on filters, see Configuring filters.

Blade1 SYSPG (0x35)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 53.
	For more information on filters, see Configuring filters.

Blade2 Presence (0x0C)

Description	bullx B500 compute blade 2 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 2.
Comments	This log corresponds to sensor number 12.
	For more information on filters, see Configuring filters.

Blade2 Presence (0x0C)

Description	bullx B500 compute blade 2 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 12.
	For more information on filters, see Configuring filters.

Blade2 3v3 PG (0x24)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 36.
	For more information on filters, see Configuring filters.

Blade2 3v3 PG (0x24)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 36.
	For more information on filters, see Configuring filters.

Blade2 SYSPG (0x36)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 54.
	For more information on filters, see Configuring filters.

Blade2 SYSPG (0x36)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 54.
	For more information on filters, see Configuring filters.

Blade3 Presence (0x0D)

Description	Compute blade 3/ accelerator blade 2 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 3/accelerator blade 2.
Comments	This log corresponds to sensor number 13.
	For more information on filters, see Configuring filters.

Blade3 Presence (0x0D)

Description	Compute blade 3/accelerator blade 2 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 13. For more information on filters, see Configuring filters.

Blade3 3v3 PG (0x25)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 37. For more information on filters, see Configuring filters.

Blade3 3v3 PG (0x25)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 37. For more information on filters, see Configuring filters.

Blade3 SYSPG (0x37)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 55. For more information on filters, see Configuring filters.

Blade3 SYSPG (0x37)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 55. For more information on filters, see Configuring filters.

Blade4 Presence (0x0E)

Description	Compute blade 4 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 4.
Comments	This log corresponds to sensor number 14. For more information on filters, see Configuring filters.

Blade4 Presence (0x0E)

Description	Compute blade 4 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 14. For more information on filters, see Configuring filters.

Blade4 3v3 PG (0x26)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 38. For more information on filters, see Configuring filters.

Blade4 3v3 PG (0x26)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 38. For more information on filters, see Configuring filters.

Blade4 SYSPG (0x38)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 56. For more information on filters, see Configuring filters.

Blade4 SYSPG (0x38)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 56. For more information on filters, see Configuring filters.

Blade5 Presence (0x0F)

Description	Compute blade 5/ accelerator blade 3 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 5/accelerator blade 3.
Comments	This log corresponds to sensor number 15. For more information on filters, see Configuring filters.

Blade5 Presence (0x0F)

Description	Compute blade 5/ accelerator blade 3 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 15.
	For more information on filters, see Configuring filters.

Blade5 3v3 PG (0x27)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 39.
	For more information on filters, see Configuring filters.

Blade5 3v3 PG (0x27)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 39.
	For more information on filters, see Configuring filters.

Blade5 SYSPG (0x39)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 57.
	For more information on filters, see Configuring filters.

Blade5 SYSPG (0x39)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 57. For more information on filters, see Configuring filters.

Blade6 Presence (0x10)

Description	Compute blade 6 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 6.
Comments	This log corresponds to sensor number 16. For more information on filters, see Configuring filters.

Blade6 Presence (0x10)

Description	Compute blade 6 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 16. For more information on filters, see Configuring filters.

Blade6 3v3 PG (0x28)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 40. For more information on filters, see Configuring filters.

Blade6 3v3 PG (0x28)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 40. For more information on filters, see Configuring filters.

Blade6 SYSPG (0x3A)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 58. For more information on filters, see Configuring filters.

Blade6 SYSPG (0x3A)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 58. For more information on filters, see Configuring filters.

Blade7 Presence (0x11)

Description	Compute blade 7/ accelerator blade 4 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 7/accelerator blade 4.
Comments	This log corresponds to sensor number 17. For more information on filters, see Configuring filters.

Blade7 Presence (0x11)

Description	Compute blade 7/ accelerator blade 4 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 17.
	For more information on filters, see Configuring filters.

Blade7 3v3 PG (0x29)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 41.
	For more information on filters, see Configuring filters.

Blade7 3v3 PG (0x29)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 41.
	For more information on filters, see Configuring filters.

Blade7 SYSPG (0x3B)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 59.
	For more information on filters, see Configuring filters.

Blade7 SYSPG (0x3B)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 59. For more information on filters, see Configuring filters.

Blade8 Presence (0x12)

Description	Compute blade 8 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 8.
Comments	This log corresponds to sensor number 18. For more information on filters, see Configuring filters.

Blade8 Presence (0x12)

Description	Compute blade 8 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 18. For more information on filters, see Configuring filters.

Blade8 3v3 PG (0x2A)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 42. For more information on filters, see Configuring filters.

Blade8 3v3 PG (0x2A)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 42.
	For more information on filters, see Configuring filters.

Blade8 SYSPG (0x3C)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 60.
	For more information on filters, see Configuring filters.

Blade8 SYSPG (0x3C)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 60.
	For more information on filters, see Configuring filters.

Blade9 Presence (0x13)

Description	Compute blade 9/ accelerator blade 5 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 9/accelerator blade 5.
Comments	This log corresponds to sensor number 19.
	For more information on filters, see Configuring filters.

Blade9 Presence (0x13)

Description	Compute blade 9/ accelerator blade 5 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 19.
	For more information on filters, see Configuring filters.

Blade9 3v3 PG (0x2B)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 43.
	For more information on filters, see Configuring filters.

Blade9 3v3 PG (0x2B)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 43.
	For more information on filters, see Configuring filters.

Blade9 SYSPG (0x3D)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 61.
	For more information on filters, see Configuring filters.

Blade9 SYSPG (0x3D)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 61. For more information on filters, see Configuring filters.

Blade10 Presence (0x14)

Description	Compute blade 10 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 10.
Comments	This log corresponds to sensor number 20. For more information on filters, see Configuring filters.

Blade10 Presence (0x14)

Description	Compute blade 10 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 20. For more information on filters, see Configuring filters.

Blade10 3v3 PG (0x2C)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 44. For more information on filters, see Configuring filters.

Blade10 3v3 PG (0x2C)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 44.
	For more information on filters, see Configuring filters.

Blade10 SYSPG (0x3E)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 62.
	For more information on filters, see Configuring filters.

Blade10 SYSPG (0x3E)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 62.
	For more information on filters, see Configuring filters.

Blade11 Presence (0x15)

Description	Compute blade 11 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 11.
Comments	This log corresponds to sensor number 21.
	For more information on filters, see Configuring filters.

Blade11 Presence (0x15)

Description	Compute blade 11 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 21. For more information on filters, see Configuring filters.

Blade11 3v3 PG (0x2D)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 45. For more information on filters, see Configuring filters.

Blade11 3v3 PG (0x2D)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 45. For more information on filters, see Configuring filters.

Blade11 SYSPG (0x3F)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 63. For more information on filters, see Configuring filters.

Blade11 SYSPG (0x3F)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 63.
	For more information on filters, see Configuring filters.

Blade12 Presence (0x16)

Description	Compute blade 12/ accelerator blade 6 is not present.
	Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 12 / accelerator blade 6.
Comments	This log corresponds to sensor number 22.
	For more information on filters, see Configuring filters.

Blade12 Presence (0x16)

Description	Compute blade 12/ accelerator blade 6 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 22.
	For more information on filters, see Configuring filters.

Blade12 3v3 PG (0x2E)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 46.
	For more information on filters, see Configuring filters.

Blade12 3v3 PG (0x2E)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 46. For more information on filters, see Configuring filters.

Blade12 SYSPG (0x40)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 64. For more information on filters, see Configuring filters.

Blade12 SYSPG (0x40)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 64. For more information on filters, see Configuring filters.

Blade13 Presence (0x17)

Description	Compute blade 13 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 13.
Comments	This log corresponds to sensor number 23. For more information on filters, see Configuring filters.

Blade13 Presence (0x17)

Description	Compute blade 13 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 23. For more information on filters, see Configuring filters.

Blade13 3v3 PG (0x2F)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 47. For more information on filters, see Configuring filters.

Blade13 3v3 PG (0x2F)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 47. For more information on filters, see Configuring filters.

Blade13 SYSPG (0x41)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 65. For more information on filters, see Configuring filters.

Blade13 SYSPG (0x41)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 65. For more information on filters, see Configuring filters.

Blade14 Presence (0x18)

Description	Compute blade 14/ accelerator blade 7 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 14 / accelerator blade 7.
Comments	This log corresponds to sensor number 24. For more information on filters, see Configuring filters.

Blade14 Presence (0x18)

Description	Compute blade 14/ accelerator blade 7 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 24. For more information on filters, see Configuring filters.

Blade14 3v3 PG (0x30)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 48. For more information on filters, see Configuring filters.

Blade14 3v3 PG (0x30)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 48. For more information on filters, see Configuring filters.

Blade14 SYSPG (0x42)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 66. For more information on filters, see Configuring filters.

Blade14 SYSPG (0x42)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 66. For more information on filters, see Configuring filters.

Blade15 Presence (0x19)

Description	Compute blade 15 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 15.
Comments	This log corresponds to sensor number 25. For more information on filters, see Configuring filters.

Blade15 Presence (0x19)

Description	Compute blade 15 is present.
	Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 25.
	For more information on filters, see Configuring filters.

Blade15 3v3 PG (0x31)

Description	The 3.3V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 49.
	For more information on filters, see Configuring filters.

Blade15 3v3 PG (0x31)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 49.
	For more information on filters, see Configuring filters.

Blade15 SYSPG (0x43)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 67.
	For more information on filters, see Configuring filters.

Blade15 SYSPG (0x43)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 67. For more information on filters, see Configuring filters.

Blade16 Presence (0x1A)

Description	Compute blade 16/ accelerator blade 8 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 16 / accelerator blade 8.
Comments	This log corresponds to sensor number 26. For more information on filters, see Configuring filters.

Blade16 Presence (0x1A)

Description	Compute blade 16/ accelerator blade 8 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 26. For more information on filters, see Configuring filters.

Blade16 3v3 PG (0x32)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 50. For more information on filters, see Configuring filters.

Blade16 3v3 PG (0x32)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 50. For more information on filters, see Configuring filters.

Blade16 SYSPG (0x44)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 68. For more information on filters, see Configuring filters.

Blade16 SYSPG (0x44)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 68. For more information on filters, see Configuring filters.

Blade17 Presence (0x1B)

Description	Compute blade 17 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 17.
Comments	This log corresponds to sensor number 27. For more information on filters, see Configuring filters.

Blade17 Presence (0x1B)

Description	Compute blade 17 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 27. For more information on filters, see Configuring filters.

Blade17 3v3 PG (0x33)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 51. For more information on filters, see Configuring filters.

Blade17 3v3 PG (0x33)

Description	The 3.3V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 51. For more information on filters, see Configuring filters.

Blade17 SYSPG (0x45)

Description	12V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 69. For more information on filters, see Configuring filters.

Blade17 SYSPG (0x45)

Description	12V power is present. State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 69. For more information on filters, see Configuring filters.

Blade18 Presence (0x1C)

Description	Compute blade 18/ accelerator blade 9 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert compute blade 18/ accelerator blade 9.
Comments	This log corresponds to sensor number 28. For more information on filters, see Configuring filters.

Blade18 Presence (0x1C)

Description	Compute blade 18/ accelerator blade 9 is present. Device inserted/Device present.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 28. For more information on filters, see Configuring filters.

Blade18 3v3 PG (0x34)

Description	The 3.3V power is not present. State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 52. For more information on filters, see Configuring filters.

Blade18 3v3 PG (0x34)

Description	The 3.3V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 52.
	For more information on filters, see Configuring filters.

Blade18 SYSPG (0x46)

Description	12V power is not present.
	State deasserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 70.
	For more information on filters, see Configuring filters.

Blade18 SYSPG (0x46)

Description	12V power is present.
	State asserted.
Severity	Information.
Direction	Assertion.
Action	None.
Comments	This log corresponds to sensor number 70.
	For more information on filters, see Configuring filters.

Notes   3v3 PG (Power Good) means the 3.3V power is running in the compute blade/accelerator blade

SYSPG (SYStem Power Good) means the 12V power is running in the compute blade/accelerator blade

B.3.   Error dictionary

The following table details the errors and corrective action associated with each blade chassis hardware component.

Component	Event/Description	Severity	Meaning	Corrective action
CMM	At or below lower critical threshold (going low).	Critical	The CMM temperature is lower than the minimum.	Check the environmental conditions, fan, ac…
	At or above upper critical threshold (going high).	Critical	The CMM temperature is upper than the maximum.	Check the environmental conditions, fan, ac…
ESM	At or below lower critical threshold (going low).	Critical	The ESM temperature is lower than the minimum.	Check the environmental conditions, fan, ac…
	At or above upper critical threshold (going high).	Critical	The ESM temperature is upper than the maximum.	Check the environmental conditions, fan, ac…
LCP	At or below lower critical threshold (going low).	Critical	The LCP temperature is lower than the minimum.	Check the environmental conditions, fan, ac…
	At or above upper critical threshold (going high).	Critical	The LCP temperature is upper than the maximum.	Check the environmental conditions, fan, ac…
IBSW	At or below lower critical threshold (going low).	Critical	The IBSW temperature is lower than the minimum.	Check the environmental conditions, fan, ac…
	At or above upper critical threshold (going high).	Critical	The IBSW temperature is upper than the maximum.	Check the environmental conditions, fan, ac…
FAN 1A	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected	If the problem persists, change the fan blade.
FAN 1B	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.

Component	Event/Description	Severity	Meaning	Corrective action
FAN 2A	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
FAN 2B	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.	If the problem persists, change the fan blade.
Blade-X	Device removed/Device absent.	Information	bullx B500 compute blade/bullx B505 accelerator blade is not present.	Insert the corresponding compute blade/ accelerator blade.
PSU-X	Device removed/Device absent.	Information	PSU-X is not present	Insert the corresponding PSU.
Blade-X	State Deassertion.	Information	The 3.3V power is not present.	
Blade-X	State Deassertion.	Information	The 12V power is not present.	
PSU-X	At or below lower non-critical threshold (going low).	Critical	PSU-X input voltage lesser than expected.	AC input supply may be improper, check the AC input.
	At or above upper non-critical threshold (going high).	Critical	PSU input voltage greater than expected.	AC input supply may be improper, check the AC input.
UCM_VCAP_X_SENS	At or below lower non-critical threshold (going low).	Critical	UCM_VCAP voltage lesser than expected.	If the problem persists, change the UCM.
	At or above upper non-critical threshold (going high).	Critical	UCM_VCAP voltage greater than expected.	If the problem persists, change the UCM.
UCM_21V_X_SENS	At or below lower non-critical threshold (going low).	Critical	UCM_21V voltage lesser than expected.	If the problem persists, change the UCM.
	At or above upper non-critical threshold (going high).	Critical	UCM_21V voltage greater than expected.	If the problem persists, change the UCM.

Component	Event/Description	Severity	Meaning	Corrective action
UCM_12V_SENS	At or below lower non-critical threshold (going low).	Critical	UCM_12V voltage lesser than expected.	If the problem persists, change the UCM.
	At or above upper non-critical threshold (going high).	Critical	UCM_12V voltage greater than expected.	If the problem persists, change the UCM.
UCM_VREF_SENS	At or below lower non-critical threshold (going low).	Critical	UCM VREF voltage lesser than expected.	If the problem persists, change the UCM.
	At or above upper non-critical threshold (going high).	Critical	UCM VREF voltage greater than expected.	If the problem persists, change the fan blade.
UCM_SX_CX_SENS	At or below lower non-critical threshold (going low).	Critical	UCM Capacitor Stack voltage lesser than expected.	If the problem persists, change the UCM.
	At or above upper non-critical threshold (going high).	Critical	UCM capacitor stack voltage greater than expected.	If the problem persists, change the UCM.

Table B-2.   Error dictionary

Glossary

A

ABR: Automatic BIOS Recovery

Recovery method for a computer system that has corrupted initialization, or boot code.

ACPI: Advanced Configuration and Power Interface

Open industry specification enabling OS-directed configuration, power management, and thermal management of server platforms.

ASR: Automatic Server Restart

The Automatic Server Restart event occurs when the operating system locks up and no longer responds. Subsequently, a system restart (reboot) begins.

B

BHC: Blade Hardware Console

Web based GUI, used to control and monitor an individual compute blade.

Blade fans

The two counter rotating fans that are mounted in each compute blade for cooling.

BMC: Baseboard Management Controller

Embedded management controller.

BOOTP

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

C

CHC: Chassis Hardware Controller

Web-based GUI, used to control and monitor the complete blade system.

CLP: Command Line Protocol

The command line protocol specifies the syntax and semantics used to allow the manipulation of the managed elements within servers, as collections or individually.

CMB: Chassis Management Board

Board in the CMM hosting a 1 Gb Ethernet switch, 24 ports, as well as a SO-DIMM 200 connector to plug the OPMA daughter board (CMC)

CMC: Chassis Management Controller

The CMC is a daughter card, M3-G4 from Raritan, based on OPMA.

CMM: Chassis Management Module

A module used to manage the blade chassis hardware enabling the inter-networking of different components of bullx blade chassis.

CSR: Certificate Signing Request

Message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

D

DDR3: Double Data Rate 3

Random access memory interface technology used for high bandwidth storage of the working data of a computer or other digital electronic devices.

DHCP: Dynamic Host Configuration Protocol

Network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

DN: Distinguished Name

LDAP entry that uniquely identifies and describes an entry in a directory (LDAP) server.

E

EP: Efficient Performance

ESM: Ethernet Switch Module

The hardware is same as the CMM without the OPMA card for management. See CMM.

Ethernet Controller

The Ethernet controller is located on either a MiniPCI card, Communications Daughter Card (CDC), or integrated on the system board.

Ethernet interconnect

Used to aggregate traffic between clients and 'server farms,' and for connecting Fast Ethernet switches.

F

Fan blade

Refers to the fan modules located at the front of the system, below the LCP.

FRU: Field Replaceable Unit

Component (board, module, fan, power supply…) replaced or added by Customer Service Engineers as a single entity.

G

GUI: Graphical User Interface

GPU: Graphical Processing Unit

Specialized processor that offloads 3D graphics rendering from the microprocessor.

H

Hot plugging

Operation of adding a component without disturbing system activity.

Hot swapping

Operation of removing and replacing a faulty component without interrupting system activity.

HPC: High Performance Computing

Uses supercomputers and computer clusters to solve advanced computation problems.

HTTPS: Hyper Text Transfer Protocol Secure

Combination of the Hypertext Transfer Protocol and a cryptographic protocol.

I

I2C: Inter Integrated Circuit

Simple bi-directional 2-wire bus for efficient inter-IC control

IB: InfiniBand

Industry standard that defines a new high-speed switched fabric subsystem designed to connect processor nodes and I/O nodes to form a system area network.

IB Switch Module

This is same as QSM or Quad.

iBMC: Integrated Baseboard Management Controller

Specialized microcontroller that is integrated in the server motherboard. The BMC is the intelligence in the Intelligent Platform Management Interface (IPMI) architecture. The BMC manages the interface between system management software and platform hardware.

ILB: I/O Legacy Board

Video, LAN, USB, etc…

INCA

INtegrated Cluster Architecture, a high-density server system.

Interconnect

Point-to-point processor interconnects.

IPMI: Intelligent Platform Management Interface

Specification owned by Intel describing mechanisms and devices to completely offload the task of managing system hardware from the primary CPU.

J

JTAG: Joint Test Action Group

Common name used for the IEEE 1149.1 standard entitled Standard Test Access Port and Boundary-Scan Architecture for test access ports used for testing printed circuit boards using boundary scan.

K

KVM: Keyboard-Video-Mouse

Hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse.

L

LCP: Local Control Panel

Module consisting of a controller, an LCD color display, a green and a blue LED and a Power ON button.

LDAP: Lightweight Directory Access Protocol

An application protocol for querying and modifying directory services running over TCP/IP.

M

MAC: Mandatory Access Control

MIB: Management Information Base

Database used to manage the devices in a communications network.

Midplane

Passive board that provides the physical and electrical connectivity to all the hardware modules.

N

Nehalem CPU Board

Compute blade or NCB.

NTP server

Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.

NVRAM: Non-Volatile Random Access Memory

RAM that retains its contents even when the computer is powered off.

O

OPMA: Open Platform Management Architecture

Open standard for connecting a modular, platform hardware management subsystem (an "mCard") to a computer motherboard.

Out-of-band compliant interface

Communications which occur outside a previously established communications method or channel.

P

PDU: Power Distribution Unit

Power bus used for the connection of peripheral system components.

PET: Platform Event Trap

Automatic alert sent by a Device over the network. (IPMI standard)

PSMI: Power Supply Management Interface

Communication with the power supply to access currents, voltages, fan speeds, and temperatures.

PSU: Power Supply Unit Module

Refers to the power supply unit that supplies 12V and 3v3 standby to the blade system. It converts AC input voltages to DC voltages.

PWM fan: Pulse Width Modulation fan

PWM involves rapidly switching the supply to the fan on and off. By altering the relative on to off times the average voltage "seen" by the fan is also altered.

Q

QDR InfiniBand: Quad Data Rate InfiniBand

Quad Data Rate InfiniBand data speed, which is 10Gbps per lane.

Quad Data Rate

Communication signaling technique where data is transmitted at four points in the clock cycle.

QSB: QDR Switch Board

Board within the Quad Switch Module

QSFP: Quad Small Form-factor Pluggable

Interconnect technology that is much lower power-consuming

QSM: Quad Switch Module

Blade system InfiniBand Switch

R

RADIUS: Remote Authentication Dial-In User Service

Networking protocol that provides centralized Authentication, Authorization and Accounting (AAA) management for computers to connect and use a network service

RAM: Random Access Memory

A temporary storage area for data and programs. This type of memory must be periodically refreshed to maintain valid data and is lost when the computer is power off. See NVRAM.

RPM: Rotations Per Minute

S

SATA: Serial Advanced Technology Attachment

Storage-interface for connecting host bus adapters to mass storage devices such as hard disk drives and optical drives.

SEL: System Event Log

Hardware log (512 entries)

SMT: Simultaneous Multi-Threading

Ability of a single physical processor to simultaneously dispatch instructions from more than one hardware thread

SMTP: Simple Mail Transfer Protocol

Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

SNMP: Simple Network Management Protocol

Protocol governing network management and the monitoring of network devices and their functions.

SSD: Solid State Drive

Data storage device that uses solid-state memory to store persistent data.

SSH: Secured Shell

Network protocol that allows data to be exchanged using a secure channel between two networked devices.

SSL: Secure Socket Layer

Cryptographic protocol that provide security and data integrity for communications over networks such as the Internet.

T

No entries.

U

UCM: Ultra Capacitor Module

Hold-up device. The module can ride through AC outages of max. 250ms.

UID: Unit Identifier

Unsigned integer value that identify users within the Linux kernel.

UPS: Uninterrupted Power Supply

Supplying power from a separate source when utility power is not available.

UTC: Coordinated Universal Time

Time standard based on International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation.

W

WOL: Wake-on LAN

Feature that provides the ability to remotely power on a system through a network connection.

X

XML: eXtended MarkUp Language

General-purpose specification for creating custom markup language

Y

No entries.

Z

No entries.

BULL CEDOC

357 AVENUE PATTON

B.P.20845

49008 ANGERS CEDEX 01

FRANCE

REFERENCE
86 A1 50FB 04