

bullx blade chassis

User's Guide

extreme computing



REFERENCE
86 A1 50FB 02

extreme computing

bullx blade chassis

User's Guide

Hardware

March 2010

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

REFERENCE
86 A1 50FB 02

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright © Bull SAS 2009-2010

Printed in France

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.

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

Table of Contents

Preface	vii
Intended readers	vii
Highlighting.....	vii
Related publications	vii
Legal information	viii
Regulatory declarations and disclaimers	viii
FCC declaration of conformity.....	ix
Canadian compliance statement (Industry Canada)	ix
Laser compliance notice.....	x
Safety information	x
Definition of safety notices	x
Electrical safety.....	xii
Laser safety information	xii
Data integrity and verification	xiii
Waste management.....	xiii
Chapter 1. Getting to know the bullx blade system	1
1.1 Overview	2
1.2 What your bullx blade system offers.....	4
1.3 Reliability, Availability, and Serviceability (RAS)	6
1.4 Features and specifications.....	7
1.4.1 Cabinet specification.....	7
1.4.2 bullx blade chassis-level platform management.....	7
1.4.3 Server-level platform management.....	7
1.4.4 External connections/interfaces	8
1.5 Components, controls, and LEDs	9
1.5.1 Front view	10
1.5.2 Rear view.....	16
Chapter 2. Introducing the Chassis Hardware Console	27
2.1 Starting the Chassis Hardware Console	28
2.2 Chassis Hardware Console overview.....	30
2.3 Chassis Hardware Console interface and permissions	31
2.4 Logging off the Chassis Hardware Console	34
Chapter 3. Using chassis power controls	35
3.1 Using bullx blade chassis power management features.....	36
3.1.1 Viewing bullx blade chassis whole drawer power.....	38
3.1.2 Powering on the bullx blade chassis.....	40
3.1.3 Powering off the bullx blade chassis.....	41
3.1.4 Forcibly powering off the bullx blade chassis	42

3.1.5	Viewing bullx B500 compute blade information.....	44
3.1.6	Viewing IB switch module policies.....	45
3.2	Applying power policies	47
3.3	Viewing Ultra Capacitor Module.....	49
Chapter 4.	Monitoring the bullx blade chassis	51
4.1	Viewing sensor status.....	52
4.2	Viewing the System Event Log (SEL)	54
4.3	Viewing board and security messages	56
Chapter 5.	Configuring the bullx blade chassis	57
5.1	Configuring the general settings.....	58
5.1.1	Configuring the bullx blade chassis	58
5.1.2	Configuring the CMC network	58
5.1.3	Configuring the BMC network	61
5.1.4	Configuring date and time	63
5.1.5	Configuring SNMP settings.....	65
5.1.6	Saving the message log	68
5.2	Managing Users.....	71
5.2.1	Creating a user account.....	71
5.2.2	Modifying a user account.....	73
5.2.3	Viewing a user account.....	74
5.2.4	Deleting a user account	76
5.2.5	Disabling or enabling user accounts	77
5.2.6	Creating a group	78
5.2.7	Viewing groups.....	80
5.2.8	Deleting a group.....	81
5.2.9	Setting group permissions	83
5.2.10	Changing group membership	84
5.2.11	Modifying your password	86
5.3	Configuring security management	87
5.3.1	Enabling encryption.....	87
5.3.2	Installing SSL Certificate	88
5.3.3	Configuring the logon policy	89
5.3.4	Configuring authentication	90
5.3.5	Enabling/Disabling power button	93
5.3.6	Configuring user account lockout parameters	94
5.4	Configuring alerts.....	95
5.4.1	Configuring filters.....	95
5.4.2	Configuring alert policies	98
5.4.3	Configuring LAN destinations	101
5.4.4	Configuring general alert settings.....	103
Chapter 6.	Using maintenance features	105
6.1	Viewing and saving embedded management board information.....	106
6.2	Viewing and saving FRU information	107

6.3	Viewing firmware version information.....	108
6.4	Viewing drawer information	109
6.5	Upgrading Firmware	110
6.6	Resetting the management board	113
6.7	Enabling/Disabling LEDs.....	114
6.8	Excluding hardware	115
6.9	Managing bullx B500 compute blades	116
6.10	Managing the CMM.....	117
6.11	Managing the ESM	118
6.12	Managing the Quad Switch Module.....	119
6.13	Managing the LCP.....	120
6.14	Managing Power	121
6.15	Viewing connected users.....	124
Appendix A. bullx blade system specifications		125
Appendix B. Predefined alert filters description		127
Appendix C. SEL messages description.....		137
	Local Control Panel SEL messages	137
	Chassis Management Module SEL messages	138
	Ethernet Switch Module SEL messages	140
	Quad Switch Module SEL messages	141
	Ultra Capacitor Module SEL messages.....	143
	Power Supply Unit module SEL messages	143
	Fan blade SEL messages	155
	bullx B500 compute blade SEL messages.....	159
Appendix D. Error dictionary		187
Glossary		189
Index		199

List of figures

Figure 1-1.	User label	3
Figure 1-2.	Major bullx blade system components.....	9
Figure 1-3.	Front view	10
Figure 1-4.	bullx B500 compute blade (18 in total)	11
Figure 1-5.	bullx B500 compute blade	12
Figure 1-6.	Fan blades	14
Figure 1-7.	Local Control Panel	15
Figure 1-8.	Rear view	16
Figure 1-9.	Power Supply Unit.....	17
Figure 1-10.	Chassis Management Module.....	19
Figure 1-11.	Quad Switch Module	21
Figure 1-12.	Ultra Capacitor Module	22
Figure 1-13.	Ethernet Switch Module	24
Figure 2-1.	Authentication page	28
Figure 2-2.	Chassis Hardware Console page	29
Figure 2-3.	Chassis Hardware Console overview	30
Figure 2-4.	Logging off Chassis Hardware Console.....	34
Figure 3-1.	Whole drawer power page.....	38
Figure 3-2.	Powering on the bullx blade chassis	40
Figure 3-3.	Powering off the bullx blade chassis	41
Figure 3-4.	Forcibly powering off the bullx blade chassis	43
Figure 3-5.	Server blade page	44
Figure 3-6.	IB switch policies	46
Figure 3-7.	Power Policy page	47
Figure 3-8.	Ultra Capacitor Module page	49
Figure 4-1.	Sensor Status page.....	52
Figure 4-2.	System Event Log page	55
Figure 4-3.	Board & Security Messages page.....	56
Figure 5-1.	Chassis Settings page.....	58
Figure 5-2.	CMC Network Settings page	59
Figure 5-3.	BMC Network Settings page	62
Figure 5-4.	Date/Time Settings page	64
Figure 5-5.	SNMP Settings page	65
Figure 5-6.	Board, Security & Remote Console Messages Settings page.....	68
Figure 5-7.	User Management page	72
Figure 5-8.	User Creation dialog page.....	72
Figure 5-9.	User Management page	73
Figure 5-10.	User Account Modification box.....	74
Figure 5-11.	User Management page	75
Figure 5-12.	Account Details box	75
Figure 5-13.	User Management page	76
Figure 5-14.	Deleting a User Account	77
Figure 5-15.	User Management page	78
Figure 5-16.	User Account Modification	78
Figure 5-17.	Creating a group	79
Figure 5-18.	Group Creation box.....	80
Figure 5-19.	Group Management page.....	81

Figure 5-20.	Group Management page	82
Figure 5-21.	Deleting a Group.....	82
Figure 5-22.	Group Management page	83
Figure 5-23.	Group permission page	84
Figure 5-24.	User Management page	85
Figure 5-25.	User Account Modification box.....	85
Figure 5-26.	Password Management page	86
Figure 5-27.	Encryption Management page.....	87
Figure 5-28.	SSL Certificate Management page	88
Figure 5-29.	User Logon Policy Management page.....	89
Figure 5-30.	Authentication Management page.....	91
Figure 5-31.	Power Button Lockout Management page	93
Figure 5-32.	User Lockout Management page	94
Figure 5-33.	Filters settings page.....	96
Figure 5-34.	Filter modification page	97
Figure 5-35.	Policy Settings page	99
Figure 5-36.	Policy Modification page	99
Figure 5-37.	LAN destination settings page.....	101
Figure 5-38.	Alert Settings: LAN Destination Edit page	102
Figure 5-39.	General Settings page.....	103
Figure 6-1.	Management Board Information page	106
Figure 6-2.	FRU Information page.....	107
Figure 6-3.	Firmware Version Information page.....	108
Figure 6-4.	Drawer Information page.....	109
Figure 6-5.	Firmware Upload page.....	110
Figure 6-6.	Firmware Upload page_Step2.....	111
Figure 6-7.	Successful firmware update	111
Figure 6-8.	Management Board Reset page	113
Figure 6-9.	Identification LED Management page.....	114
Figure 6-10.	Hardware Exclusion Management page.....	115
Figure 6-11.	Sever Blade Management page.....	116
Figure 6-12.	CMM Management page	117
Figure 6-13.	ESM Management page	118
Figure 6-14.	IBSW Management page.....	119
Figure 6-15.	LCP Management page	120
Figure 6-16.	Power Management page.....	121
Figure 6-17.	Connected Users Information page.....	124

List of tables

Table 1-1.	Record information.....	2
Table 2-1.	Factory-default authentication.....	28
Table 2-2.	Chassis Hardware Console overview.....	30
Table 2-3.	Chassis Hardware Console interface features and permissions.....	33
Table 3-1.	bullx blade chassis Power Management page features.....	37
Table 3-2.	Whole drawer power page description.....	39
Table 3-3.	Power on features.....	40
Table 3-4.	Powering Off.....	42
Table 3-5.	Forcibly powering off the bullx blade chassis.....	43
Table 3-6.	Server blade page description.....	45
Table 3-7.	IB switch policies.....	46
Table 3-8.	Power policy description.....	48
Table 3-9.	UCM description.....	49
Table 4-1.	Sensor status page description.....	53
Table 4-2.	Sensor status icons description.....	53
Table 5-1.	CMC Network Settings page description.....	60
Table 5-2.	BMC Network Settings page description.....	63
Table 5-3.	Date/Time Settings page description.....	64
Table 5-4.	SNMP Settings page description.....	66
Table 5-5.	Board, security & Remote console Messages Settings page description.....	70
Table 5-6.	HTTP Encryption (HTTPS).....	87
Table 5-7.	SSL Certificate Management page description.....	89
Table 5-8.	User Logon Policy Management page description.....	90
Table 5-9.	Authentication Management page description.....	92
Table 5-10.	Power Button lockout Management page description.....	93
Table 5-11.	User Lockout Management page description.....	94
Table 5-12.	Configurable filter modification page description.....	98
Table 5-13.	Policy Modification page description.....	100
Table 5-14.	Alert Settings: LAN Destination Edit page description.....	102
Table 5-15.	General Settings page description.....	103
Table 6-1.	Management Board Reset page description.....	113
Table 6-2.	Power Management page description.....	123

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 the Administrators and Operators of bullx blade system.

Highlighting

The following highlighting conventions are used in this guide:

Bold	Identifies the following: <ul style="list-style-type: none">• Interface objects such as menu names, labels, buttons and icons• File directory and path names• Keywords to which particular attention must be paid
<i>Italics</i>	Identifies references such as manuals or URLs

Related publications

- *bullx blade system Installation Guide*, 86 A1 48FB 00
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 00
explains how to maintain, service, and upgrade the *bullx blade system*. This guide is intended for use by qualified support personnel.
- *bullx B500 compute blade User's Guide*, 86 A1 49FB 00
explains how to use the bullx B500 compute blades. This guide is intended for use by Customer Administrators and Operators.

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
- EC 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.

<p>Class 1 Laser Product Luokan 1 Laserlaite Klasse 1 Laser Apparat Laser Klasse 1</p>
--

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 bullx B500 compute blade/power supply, dummy bullx B500 compute 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 bullx 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.

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

Bull 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 bullx blade system

This chapter gives an overview at the bullx blade system-level architecture and a high-level description of each of these modules.

1.1 Overview

Your bullx blade system is a high-density server system providing cluster architecture. It has 18 bullx B500 compute blade bays, making it ideally suited for High Performance Computing (HPC) cluster environment that requires a large number of high-performance servers in a small space. The bullx blade system provides common resources that are shared by the bullx B500 compute blades, such as power, cooling, system management, network connections, and I/O switch. The use of common resources reduces the size of the bullx B500 compute blades, 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 the system hardware to meet your needs today, while providing flexible expansion capabilities for the future.

This guide provides information on:

- Installing the bullx blade system
- Connecting and testing the bullx blade system

This *bullx blade chassis User's Guide* and other publications that provide detailed information about your bullx blade chassis are provided in Portable Document Format (PDF) on the *bullx blade chassis Documentation and Resource CD*.

Record information about your bullx blade system in the following table:

	bullx blade system
Product Name	
Product Code	
Product Number	
Serial Number	

Table 1-1. Record information

The serial number and part number are on a label on the top of the bullx blade chassis, as shown in the following illustration.

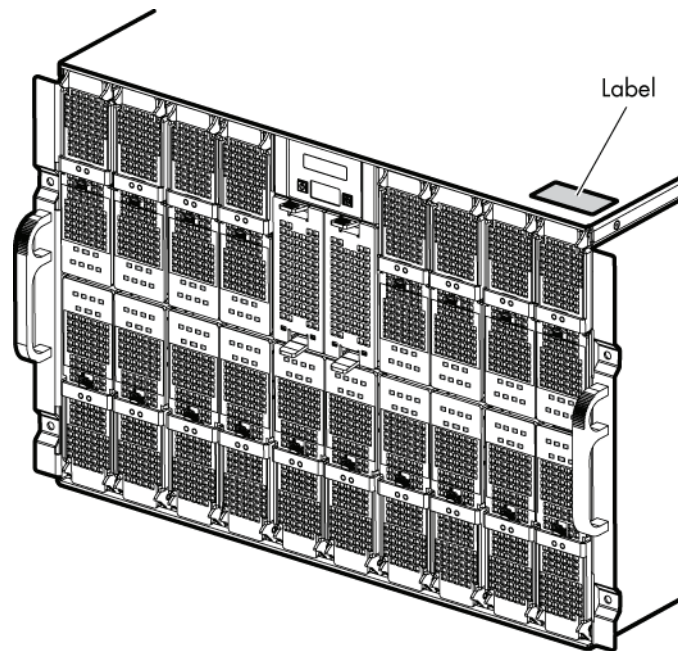


Figure 1-1. User label

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

- Eighteen dual processor (DP) bullx B500 compute blades, called Nehalem CPU blade (NCB). Each NCB includes two fans for cooling
- A Quad Switch Module
- Provision for an optional Ultra Capacitor Module (UCM)
- A Chassis Management Module (CMM)
- An optional Ethernet Switch Module (ESM)
- Front panel module Local Control Panel (LCP) providing a LCD display power button and reset button
- Up to four Power Supply Unit modules (PSU) providing N+1 redundancy on power
- Two Fan blades in the front of the bullx blade chassis, to provide cooling to the Quad Switch Module, CMM, and ESM

1.2 What your bullx blade system offers

The design of your bullx blade system takes advantage of advancements in server technology. It hosts up to 18 functionally separate bullx B500 compute blades and their shared resources in a single bullx blade chassis. Your bullx blade system combines:

Innovative technology

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

Expansion capabilities

You can add bullx B500 compute blades to the bullx blade system as needed and it can host a maximum of 18 blades.

Hot-swap/Hot-plug capabilities

The front bays on the bullx blade system are hot-plug blade bays. The rear switch and management bays on the bullx blade system are hot-plug module bays. You can add, remove or replace bullx B500 compute blades, CMM in hot-plug bays without removing power from the bullx blade system by first ensuring the module is not in use by the system, which means that no active software or applications are running. The rear power supply bays on the bullx blade system are also hot-swappable. You can add, remove or replace the power or Fan blades from the bullx blade system without powering off the bullx blade system.



CAUTION

To maintain proper system cooling; each unoccupied bay must contain a filler blade or filler module.

Redundancy capabilities

The redundant components in the front and in the rear of your bullx blade system enable continued operation even if a component fails.

PSU modules and Fan blades: Normally, the redundant PSU modules and Fan blades share the load. If one of the power modules or Fan blades fails, the non-failing power module or Fan blade handles the entire load. You can then replace the failed Fan blades or power module without shutting down the bullx B500 compute blade.

Redundant network connection capabilities

The optional ESM provides redundant Ethernet interface to the blades.

System management capabilities

Your bullx blade system comes with a service processor in the CMM. This service processor, in conjunction with the system-management firmware that is provided with the service processor in each bullx B500 compute blade, enables you to remotely manage the bullx blade system components, and the bullx B500 compute blades. The CMM also multiplexes the USB, keyboard, mouse, and video ports across the multiple bullx B500 compute blades.

The service processor in each bullx B500 compute blade provides bullx B500 compute blade system monitoring, event recording, and alert capability.

Network environment support

Your bullx blade system supports up to two Ethernet Switches: One in the CMM and the second one in the ESM. These Ethernet Switch Modules can be used for bullx B500 compute blade communication with the network. Each CMM/ESM provides an internal connection to each bullx B500 compute blade and up to 18 internal connections.

1.3 Reliability, Availability, and Serviceability (RAS)

Three of the most important features in server design are reliability, availability, and serviceability (RAS). These factors help to ensure the integrity of the data stored on your bullx B500 compute blade; that your bullx B500 compute blade is available when you want to use it; and that should a failure occur you can easily diagnose and repair the failure with minimal inconvenience.

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

- Shared key components, such as power, cooling, and I/O
- All components serviced from the front or rear of the bullx 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 CMM
- Remote CMM firmware upgrade
- Remote upgrade of bullx B500 compute blade service processor microcode
- Redundant components:
 - Cooling fans blades (blowers)
 - Power Supply Unit Modules
- Hot-plug components:
 - bullx B500 compute blades
 - Chassis Management Module
 - Ethernet Switch Module
 - Quad Switch Module
 - Power Supply Unit module
- Non Hot-swappable components: Ultra Capacitor Module

1.4 Features and specifications

Following is a summary of the features and specifications for your bullx blade system:

- The bullx blade system, 18 server, 7U Chassis, rack-able within a standard 19 cabinet includes front panel, power supplies and Midplane
- Dual CPU socket bullx B500 compute blades using the EP family of Xeon processors from Intel®
- Module height 307 mm maximum
- Width 446 mm maximum
- Depth 740 mm
- Weight up to 125 kg depending on the system configuration
- Typical power consumption is about 8000 W
- AC power modules offer N+1 redundancy
- Maximum number of power modules with/without redundancy: 4/3
- Two Fan blades in front, cooling the Quad Switch Module, CMM and ESM
- LCP display in front

1.4.1 Cabinet specification

- Rack mounted system, using a standard cabinet
- 480mm (19") wide
- 740mm deep chassis

1.4.2 bullx blade chassis-level platform management

- Embedded web server
- Supports both 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

1.4.3 Server-level platform management

- Embedded web server
- Supports both 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

1.4.4 External connections/interfaces

Following are external connections available in the bullx blade system:

- Eighteen IB QDR connections (QSFP connector with power) on the Quad Switch Module
- Three 1Gb Ethernet ports -RJ45 connectors on the ESM
- Three 1Gb Ethernet ports -RJ45 connectors and a serial COM port for maintenance purpose are present on the CMM
- There is a control panel on the front of the bullx blade chassis
- bullx blade chassis power On/Off switch
- bullx blade chassis power indicator LED
- bullx blade chassis indicator blue LEDs – LCP indicator LED, CMM indicator LED at the rear
- bullx B500 compute blade indicator LEDs
- Quad Switch Module indicator LED
- Gbit Ethernet switch indicator LED
- Ultra Capacitor Module indicator LED
- CMM reset push button to reset Chassis Management Controller (CMC)

1.5 Components, controls, and LEDs

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

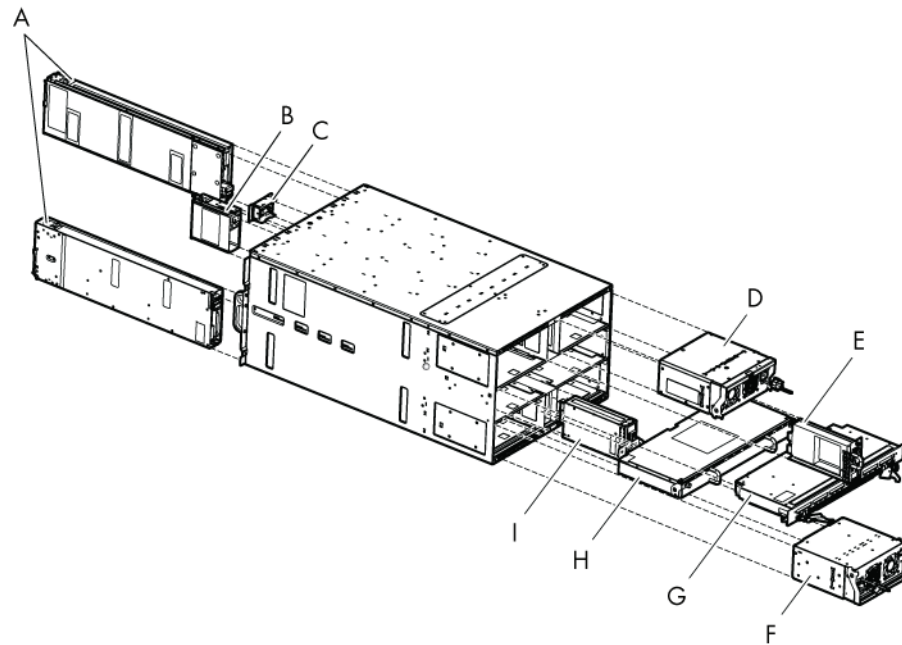


Figure 1-2. Major bullx blade system components

- A. bullx B500 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

Note The illustrations in this document might differ slightly from your hardware.

1.5.1 Front view

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

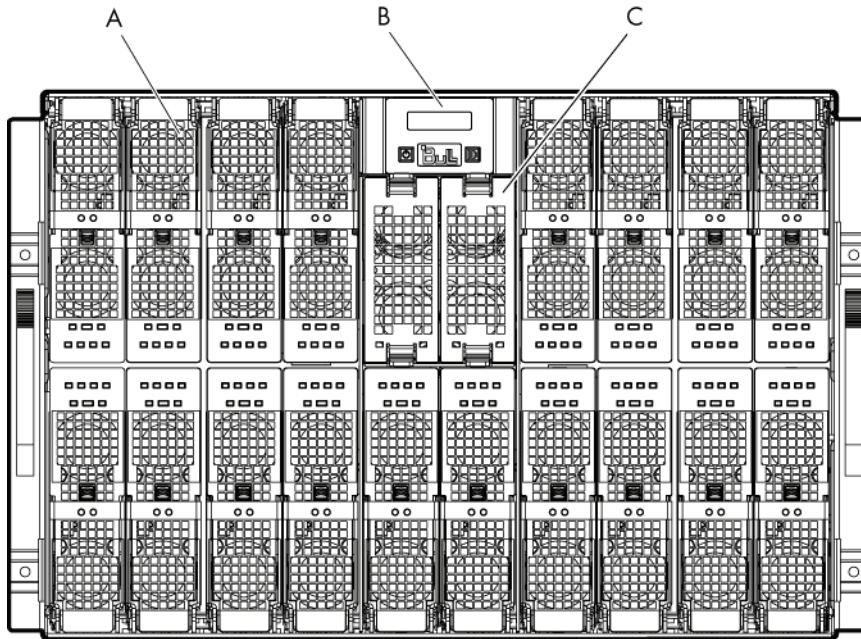


Figure 1-3. Front view

- A. bullx B500 compute blade
- B. Local Control Panel
- C. Fan blade

1.5.1.1 bullx blade chassis

In the front side, the bullx blade chassis has a LCP, 18 bays to host bullx B500 compute blades and two bays to host fan blades. The bullx blade chassis includes two handles that help in moving the bullx blade chassis. The Midplane, in the middle of the bullx blade chassis, provides interconnectivity among blades and the various modules located in the rear of the bullx blade chassis.

1.5.1.2 bullx B500 compute blades

The 18 bullx B500 compute blades are distributed in two rows, with eight on top row and 10 on the bottom row. All the blades are inserted from the front of the bullx blade system and plugged vertically into the Midplane.

The bullx B500 compute blade provides the server motherboard functionality based on dual Nehalem-EP (Efficient Performance) processors from Intel®. The processor features a quad-core processing to maximize performance and performance/watt for datacenter infrastructures and highly dense deployments. Each Nehalem-EP processor interconnects with the other Nehalem-EP processor and the Tylersburg north bridge through the Intel's Quick Path Interconnect (QPI) feature. Each bullx B500 compute blade interconnects with other bullx B500 compute blades through an embedded ConnectX QDR component and the Quad Switch Module.

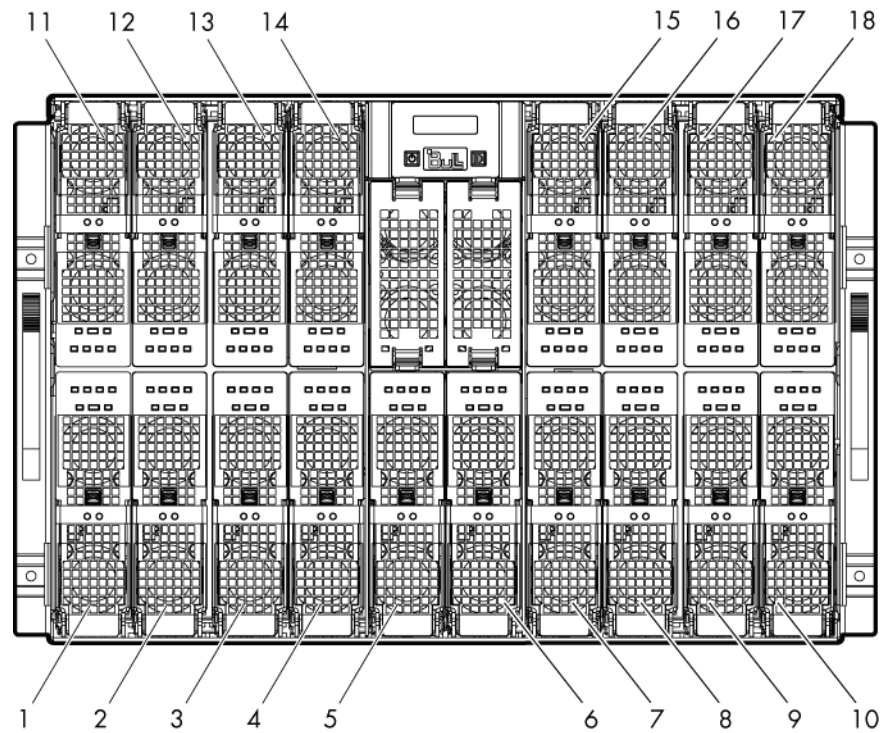


Figure 1-4. bullx B500 compute blade (18 in total)

The bullx B500 compute blade has seven LEDs, which are visible on the front bezel. These LEDs provide the visual status and indications of various functions as described below.

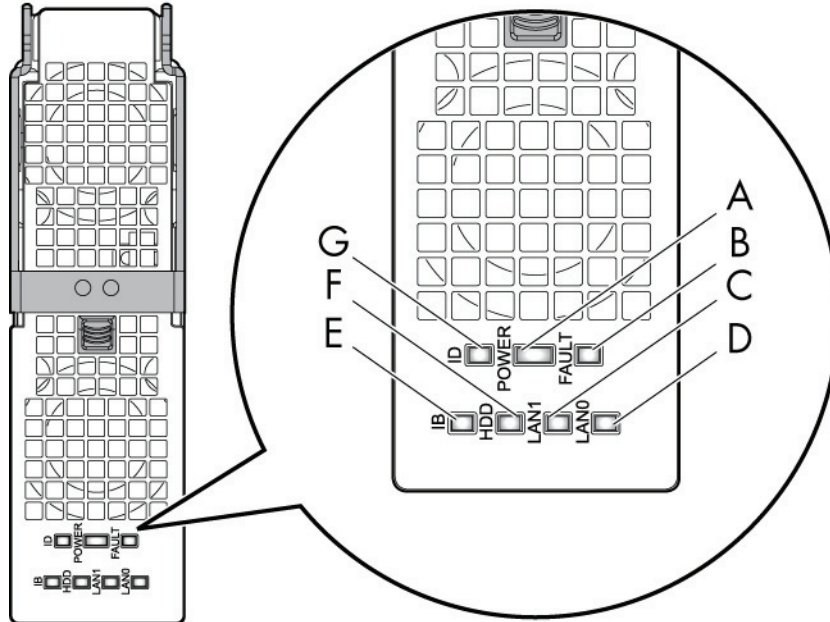


Figure 1-5. bullx B500 compute blade

- A. Power LED
- B. Fault LED
- C. LAN1 LED
- D. LAN0 LED
- E. IB activity LED
- F. HDD activity LED
- G. Identification LED

1.5.1.3 bullx B500 compute blade specific features

The other bullx B500 compute blade features are:

- Powered down bullx B500 compute blades can be inserted and removed without disturbing operations
- Two processor sockets
- Up to two Nehalem-EP processor
- All processor SKUs supported up to 95W

- Double Data Rate 3 at 1333 or 1066 MHz
- Twelve DIMM slots (6 per socket)
- Only one DIMM per channel is supported for DDR3 1333MHz (3 per socket)
- hot plugging is supported
- No PCI Express slots
- Optional SATA drive (HDD or SSD) form factor 1.8 inch
- Sleep state four (Suspend to disk) supported on HDD/SSD when available
- LEDs in front for status indication

LED indicators

- **Identification LED**

The identification LED indicator is blue.

This indicator is a unit identifier dedicated to the maintenance operations to localize physically a bullx B500 compute blade.

The switching On/Off of this indicator is driven by the maintenance operator through the Chassis Hardware Console web interface.

- **Power LED**

The power LED indicator is bicolor: amber/green.

This indicator provides the bullx B500 compute blade power state:

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

This indicator is managed by the hardware.

- **Fault LED**

The fault LED indicator is red.

This indicator allows display fault 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 blinking green.

This indicator flashes On and Off to indicate traffic (Tx and Rx data) on the Ethernet network channel 0 (to/from CMM) for this bullx B500 compute blade.

- **LAN 1 activity LED**

The LAN 1 activity LED indicator is blinking green.

This indicator flashes On and Off to indicate traffic (Tx and Rx data) over the Ethernet network channel 1 (to/from ESM) for this bullx B500 compute blade through the Ethernet component.

This indicator is managed by the hardware.

- **IB activity LED**

The IB activity LED indicator is blinking amber

This indicator flashes On and Off to indicate traffic over the IB network channel 0 for this bullx B500 compute blade (through the ConnectX component).

This indicator is managed by the hardware

- **HDD activity LED**

The HDD activity LED indicator is blinking amber

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

This indicator is managed by the hardware.



DANGER

Hazardous energy is present when the bullx B500 compute blade is connected to the power source. Always replace the blade cover before inserting the blades into the bullx blade chassis.

1.5.1.4 Fan blade

Two Fan blades provide cooling to the Quad Switch Module, CMM, and ESM. Fan blades cannot be hot swapped.



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.

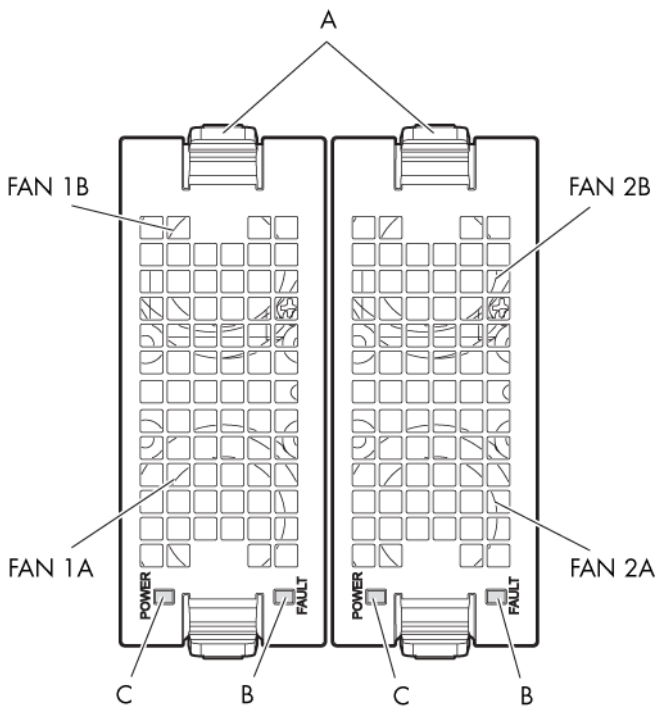


Figure 1-6. Fan blades

A. Latch

B. Fault LED

C. Power LED

LED indicators

- **Fault LED**
When the fans do not rotate as per the expected speed, the fault LED switches On: Red.
- **Power LED**
When the Fans are rotating as per the expected speed, the power LED switches On.

1.5.1.5 Local Control Panel

The Local Control Panel (LCP) is the panel related to the bullx blade chassis. This panel is placed in the center of the bullx blade chassis.

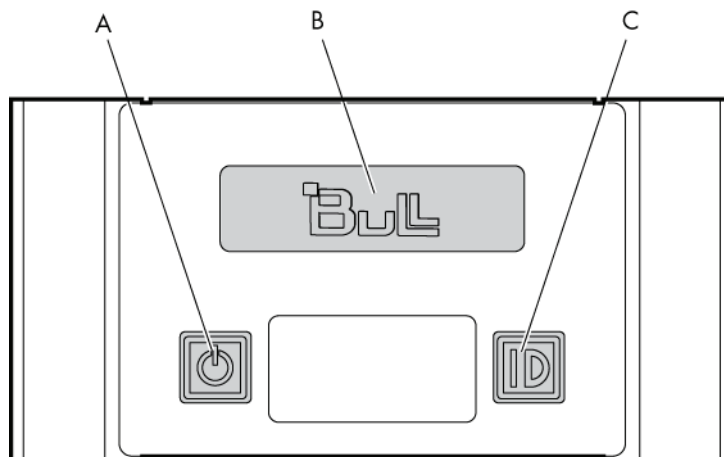


Figure 1-7. Local Control Panel

- A. Power On/Off button
- B. Display screen
- C. Identification button

LED indicators

- **Identification LED**
The identification LED indicator is blue.
This indicator is a unit identifier dedicated to the maintenance operations to localize physically a bullx blade chassis from the front side. This LED is turned On simultaneously with the CMM identification LED indicator for the backside.
The switching On/Off of this indicator is driven by the maintenance operator through the CMC or locally through the identification button of the LCP.
- **Power LED**
The power LED indicator is green.
This indicator indicates the 12V main power presence within the bullx blade chassis. This indicator is managed by the CMC firmware.

1.5.2 Rear view

This section identifies the components and indicators on the rear of your bullx blade system.

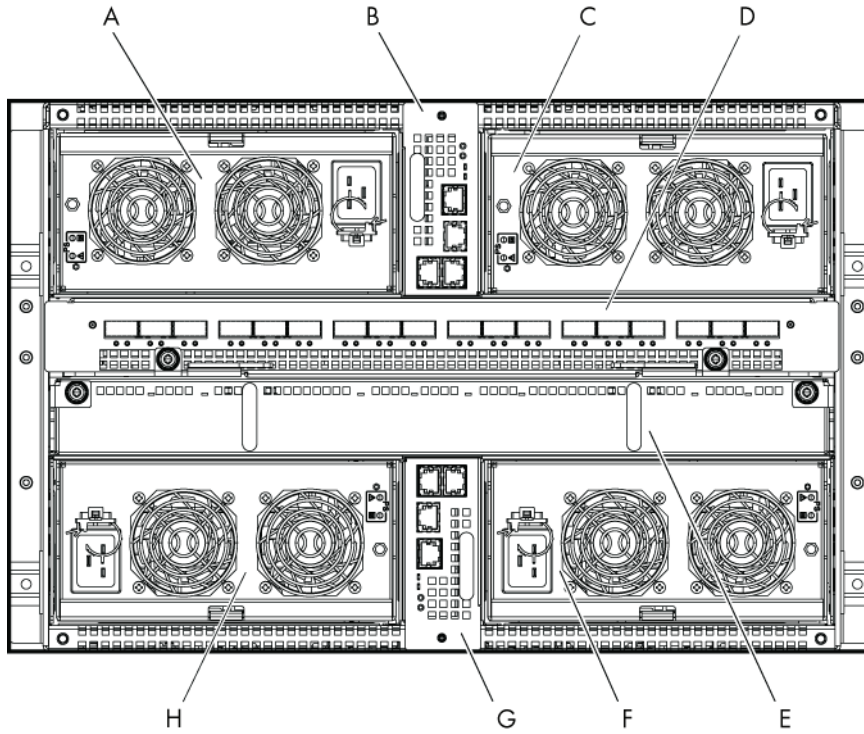


Figure 1-8. Rear view

- A. PSU3
- B. CMM
- C. PSU4
- D. Quad Switch Module
- E. UCM
- F. PSU2
- G. ESM
- H. PSU1

1.5.2.1 bullx blade chassis

The rear side of the bullx blade chassis provides bays for bullx blade system PSUs, CMM, Quad Switch Module, UCM, and the ESM modules.

1.5.2.2

Power Supply Unit module

There are four PSU modules in the bullx blade system, each of 2900W rating. These take in the AC input of 180VAC to 264VAC and provide 12V main and 3.3V standby outputs. The four PSU modules provide N+1 redundancy. The typical system power dissipation is around 7900W depending on the configuration and the customer's applications. The PSU modules occupy the rear of the bullx blade system.

The high-level features of the PSU module are as below:

- Power Supply 2900 W
- Has two outputs including 12V and a 3.3V stand-by
- AC input power factor corrected
- Hot swappable, up to four parallel supplies
- AC input of 180 to 264V AC
- PSMI compliant

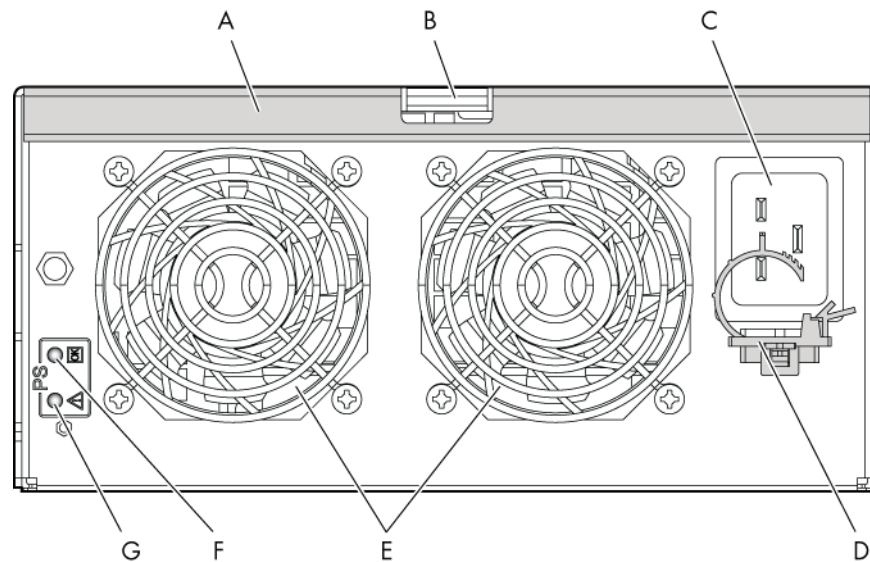


Figure 1-9. Power Supply Unit

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

LED indicators

- **Fault LED**

The Fault LED indicator is amber.

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 also that the 3.3V stand by voltage is available. Once 12V is enabled this LED becomes steady.

1.5.2.3 Chassis Management Module

The CMM's primary function is to provide the bullx blade chassis-level management functionality for the bullx blade system. This includes detection, power On/Off, management status monitoring for the bullx B500 compute blades and other hardware modules within the bullx blade chassis, PSU management status monitoring, and system fan controls. The CMM is also used to manage and display the LCD 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 OPMA service processor (internal)
- Eighteen Ethernet ports to bullx B500 compute blades through backplane connector (internal)
- Three Ethernet ports to RJ45 connectors on the rear side for external access

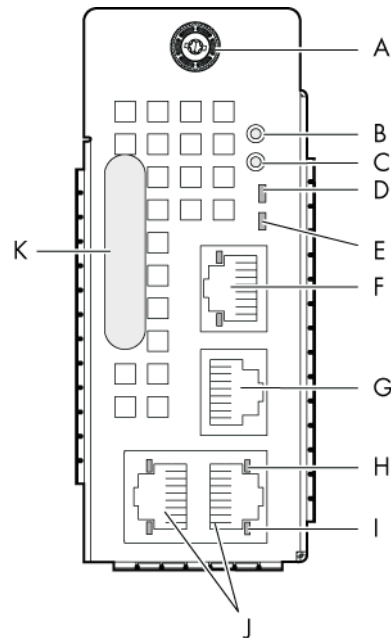


Figure 1-10. Chassis Management Module

- A. Thumb screw
- B. Reset button
- C. Default 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

The other CMM features and functionalities are:

- bullx B500 compute blade execution can proceed when the CMM is down
- The Ethernet switch supports VLANs
- Has three dynamically configurable stacking or Ethernet ports
- An external COM port
- LED for status indication
- Displays status information on the LCP display panel
- Ethernet switch firmware can be loaded in-band over the Ethernet links

LED indicators

- **Identification LED**

The identification LED indicator is blue.

This indicator is a unit identifier dedicated to the maintenance operations to localize physically bullx blade chassis from the rear side. This LED is switched On simultaneously with the LCP identification LED indicator (for the front side).

The switching On/Off of this indicator is driven by the maintenance operator through the CMC (external remote SNMP command to the bullx blade chassis) or locally through the identification button of the LCP.

- **Power LED**

The power LED indicator is amber.

This indicator indicates the stand-by power presence as well as the CHC activity:

- Solid amber: 3.3V stand-by power presence
- Blinking amber: the CMC firmware is alive

- **LAN activity and status LED**

Two LEDs are integrated in each of the three Ethernet connectors: One for the link status, the second for the link activity.

1.5.2.4

Quad Switch Module

The system supports a Quad Switch Module (QSM), based on a 36 port QDR switch Board (QSB) to provide the quad switching function between the 18 blades and the external QSFP ports. The QSM plugs into the Midplane from the rear side of the bullx blade chassis.

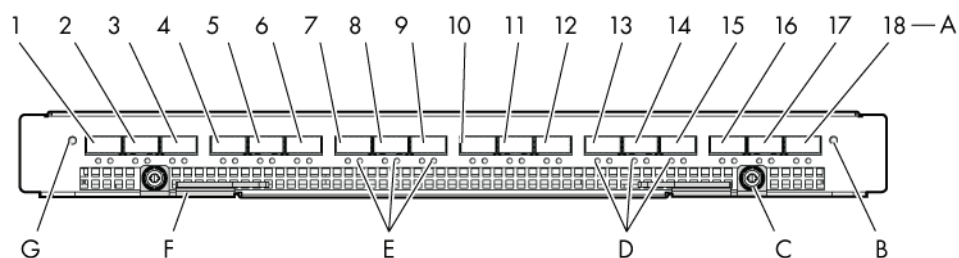


Figure 1-11. Quad Switch Module

- 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

Some of the QSM features are:

- Thirty six ports InfiniBand Switch: 18 internal and 18 external ports
- Support to QDR IB
- Ability to support passive and active cables per IB standard
- The QSM has LEDs in front for status indication
- Switch management is performed in-band on IB connections

LED indicators

- **Identification LED**
In the CHC web interface, select Maintenance tab and click Identification LED. This gives you an option to switch On/Off the identification LED of QSM.
- **Power LED**
The power LED indicator is bicolor: Amber/green indicating the power state:
 - Amber: 3.3V stand-by power presence
 - Green: 12V main power presence
- **IB link activity LED**
There are two LEDs:

- **Physical link** -green indicates a good physical link. Blinking indicates a problem with the physical link data activity.
- **Logical link** -Amber blinking indicates data transfer.

1.5.2.5 Ultra Capacitor Module

The UCM is an optional module that can ride through AC outages of a maximum of 250ms. During normal operation, the module gets charged by the 12V from the Midplane and stores the charge it in its Ultra capacitors. During outage, these capacitors discharge to provide the required power to the other modules like the NCB and the Quad Switch Module board (QSB). For 3v3 stand-by voltage, the PSU module has a hold time of 1000ms. Hence, the PSU module itself takes care of the 3v3 during the 250ms AC outage.

The UCM connects to the Midplane through bus bars. In addition, there is control and monitoring logic that is controlled by the CMM. The control/monitoring logic operates in 3v3 standby voltage from the PSU module.

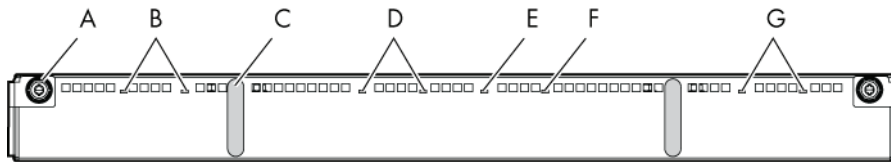


Figure 1-12. Ultra Capacitor Module

- A. Thumb screw
- B. Charge LEDs
- C. Handle
- D. Charge LEDs
- E. Identification LED
- F. Fault LED
- G. Charge LEDs

Following are the other features of the UCM:

- Able to offset power outages up to 250 ms
- Max hold-up time 480 ms

LED indicators

- **Identification LED**

The identification LED indicator is blue.

This indicator is a unit identifier dedicated to the maintenance operations to localize physically the module.

The switching On/Off of this indicator is driven by the maintenance operator (external SNMP remote command to the bullx blade chassis).

- **Charge LED**

The charge LED indicators are tricolor: green, amber, and red.

The green color means that the Ultra capacitor is fully charged, the amber color that it is being charged, the red color that it is in the process of discharging.

Each Ultra capacitor stack has its own LED indicator.

These indicators are managed by the hardware.

- **Fault LED**

The fault power LED indicator is amber.

This indicator indicates the detection of an Ultra capacitor failure.

This indicator is managed by the CHC firmware.

1.5.2.6

Ethernet Switch Module

The ESM, an optional module, is present only to provide the Ethernet switching function through the three external Ethernet ports.

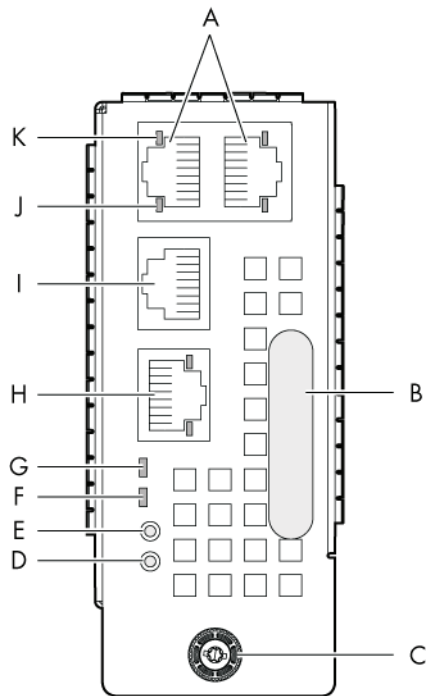


Figure 1-13. Ethernet Switch Module

- A. Dynamically configurable stacking or Ethernet ports
- B. Handle
- C. Thumb screw
- D. Reset button
- E. Default button
- F. Power and health status LED
- G. Identification LED
- H. Dynamically configurable stacking or Ethernet port
- I. Computer port
- J. Activity LED
- K. Link LED

Following are the other features of the ESM:

- Can be hot replaced
- The Ethernet switch supports VLANs
- The 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
- Has LEDs for status indication
- Ethernet switch firmware can be loaded in-band over the Ethernet links

LED indicators

- **Identification LED**

The identification LED indicator is blue.

This indicator is a unit identifier dedicated to the maintenance operations to localize physically the module.

The switching On/Off of this indicator is driven by the maintenance operator (external SNMP remote command to the bullx blade chassis).

- **Power LED**

The power LED indicator is amber.

This indicator indicates the presence of 3.3V stand-by power in the module.

This indicator is managed by the hardware.

- **LAN activity and status LED**

Two LEDs are integrated in each of the three Ethernet connectors: One for the link status, the second for the link activity.

Note The LAN activity for the buried links of the embedded Ethernet switch (between the Ethernet switch and each bullx B500 compute blade) are displayed on a LED in the front of each bullx B500 compute blade.

Chapter 2. Introducing the Chassis Hardware Console

This chapter deals with the Chassis Hardware Console and explains how to start and stop the console from a Microsoft Internet Explorer or Mozilla Firefox browser. This chapter includes following topics:

- Starting the Chassis Hardware Console
- Chassis Hardware Console overview
- Logging off Chassis Hardware Console

2.1 Starting the Chassis Hardware Console

Prerequisites

- The server 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.



Important:

INITIAL START

Enter the IP address that you have just configured using the DHCP server.

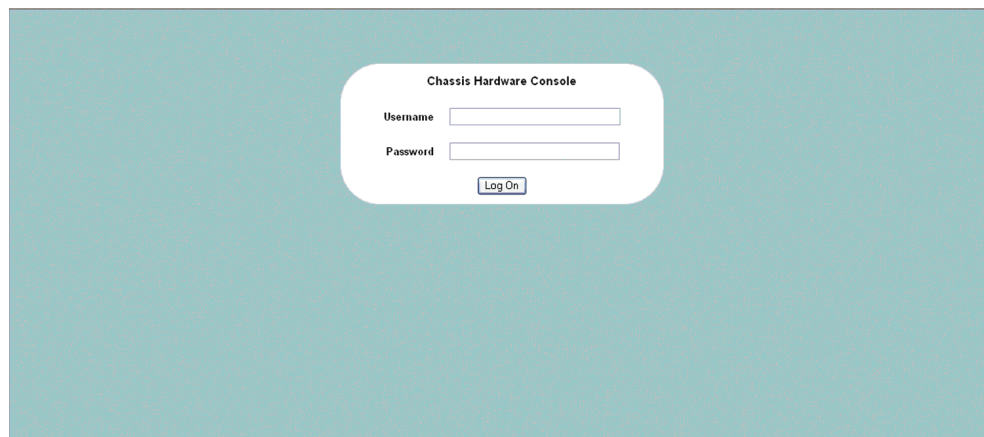


Figure 2-1. Authentication page

Chassis Hardware Console	
User name	super
Password	bull

Table 2-1. Factory-default authentication

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

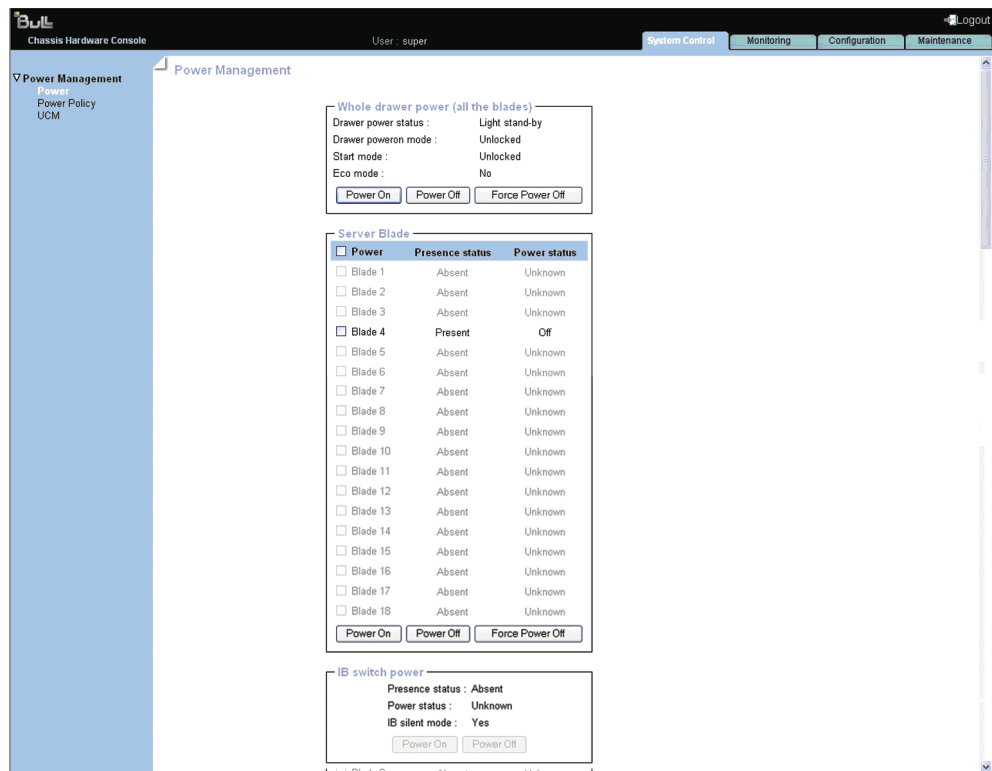


Figure 2-2. Chassis Hardware Console page

Important

It is strongly recommended 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 and is unable to connect to the console, contact your Customer Service Representative.

What to do if an incident occurs?

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

- Network failure
- Incorrect network settings
- Incorrect browser settings

2.2 Chassis Hardware 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 and configure your bullx blade system via the enterprise LAN using a Microsoft Internet Explorer or a Mozilla Firefox browser.

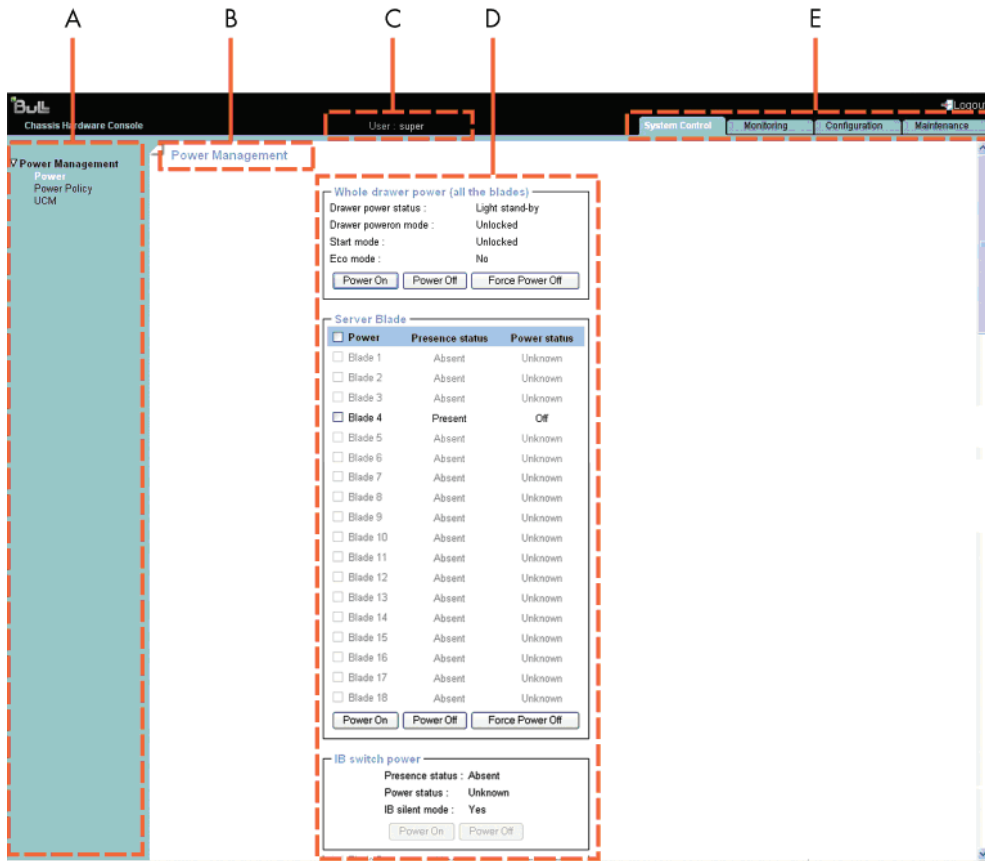


Figure 2-3. Chassis Hardware Console overview

Chassis Hardware console	
A	The navigation tree provides access to console features. Note that displayed features differ according to the tab selected.
B	Name of the selected navigation tree menu.
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 four families of features accessible from the associated navigation trees: System Control, Monitoring, Configuration, and Maintenance.

Table 2-2. Chassis Hardware Console overview

2.3 Chassis Hardware Console interface 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	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Power Policy	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		UCM	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
Monitoring	Cabinet Status & Logs	Sensor Status	Viewing: All users
		System Event Log	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Messages	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
Configuration	General Settings	Chassis	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		CMC Network	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		BMC Network	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Date-time	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		SNMP	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Messages	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
	User Management	Users	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Groups	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Password	<ul style="list-style-type: none"> Viewing: All users Operations: Root users

Tab	Tree node	Features	Permission
	Security Management	Encryption	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		SSL Certificate	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Access Control	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		User Logon Policy	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Authentication	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Power Button Lockout	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		User Lockout	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
	Alert Settings	Filters	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Policies	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		LAN Destination	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		General	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
Maintenance	Hardware Information	Management Board	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		FRU	<ul style="list-style-type: none"> Viewing: All users Operation: Root users
		Firmware	Viewing: All users
		Drawer Information	Viewing: All users
	Firmware Updates	CMC	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
	Maintenance Operations	Unit reset	<ul style="list-style-type: none"> Viewing: All users Operations: Root users

Tab	Tree node	Features	Permission
		Identification LED	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Hardware Exclusion	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Server Blade Change	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		CMM Change	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		ESM Change	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		IBSW Change	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		LCP Change	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Power Management	<ul style="list-style-type: none"> Viewing: All users Operations: Root users
		Connected Users	<ul style="list-style-type: none"> Viewing: All users Operations: Root users

Table 2-3. Chassis Hardware Console interface features and permissions

2.4 Logging off the Chassis Hardware Console

Procedure

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

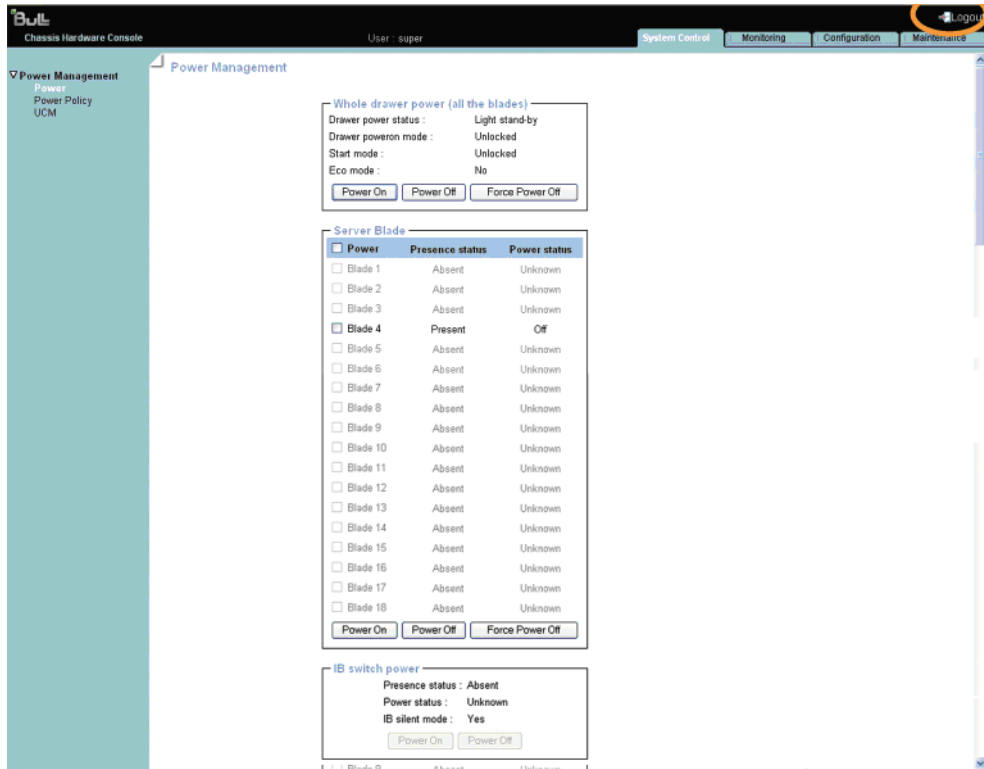


Figure 2-4. Logging off Chassis Hardware Console

Chapter 3. Using chassis power controls

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

- Using Chassis Power Management Features
- Power
- Power policy
- UCM

3.1 Using bullx blade chassis power management features

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

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

From the **System Control** tab, expand **Power Management**, and click **Power** to open the Power Management page.

The Power Management page is divided into three areas:

- Whole drawer power (all the blades) is used to check system power status
- Server blade is used to perform routine power on/off sequences
- IB switch power is used to perform power on/off sequences

Whole drawer power	
Drawer power status	<p>Provides the status of drawer power.</p> <ul style="list-style-type: none">• Deep stand-by: It is the lowest power consumption waking state for the drawer• Light stand-by: It is moderate consumption working state for the drawer• Main power: It is the functional state of the drawer
Drawer power on mode	<p>Provides the status of drawer power on mode.</p> <ul style="list-style-type: none">• Full power on: All the blades and other boards are powered on during the drawer powering on• Unlocked: All the blades and other boards are unlocked (12 V hot swap enabled) during the drawer powering on
Start mode	<p>Provides the status of start mode.</p> <ul style="list-style-type: none">• Deep Stand-by: The bullx B500 compute blade stays in stand-by off state (i.e. BMC is not running)• Light Stand-by: The bullx B500 compute blade state becomes stand-by on (i.e. the BMC will be running)• Unlocked Power: The bullx B500 compute blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)

Whole drawer power	
Eco mode	<p>Provides the status of Eco mode.</p> <ul style="list-style-type: none"> • Yes: This forces drawer to silent mode. (The drawer can be configured to save the energy when the bullx B500 compute blades are not extensively used. The drawer will be in awakened state with very low power consumption (deep stand-by state) as soon as blades inactivity is detected) • No: This forces drawer to off
Server blade	
Power	bullx B500 compute blade number.
Presence status	<ul style="list-style-type: none"> • Present: The corresponding bullx B500 compute blade is present • Absent: Server corresponding bullx B500 compute blade is absent
Power status	<ul style="list-style-type: none"> • Off: The corresponding bullx B500 compute blade is powered Off • On: The corresponding bullx B500 compute blade is powered On • Unknown: The corresponding bullx B500 compute blade is absent
IB switch power	
Presence status	<p>Indicates the status of the Quad Switch Module.</p> <ul style="list-style-type: none"> • Absent: The Quad Switch Module is absent • Present: The Quad Switch Module is present
Power status	<p>Indicates the power status of the Quad Switch Module.</p> <ul style="list-style-type: none"> • 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	<p>Indicates the status of IB silent mode.</p> <ul style="list-style-type: none"> • Yes: The IB switch silent mode is set to silent • No: The IB switch can be explicitly powered on/off

Table 3-1. bullx blade chassis Power Management page features

3.1.1 Viewing bullx blade chassis whole drawer power

bullx blade chassis power status can be checked at all times from the CHC.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

From the **System Control** tab, expand **Power Management**, and click **Power** to open the Power Management page.

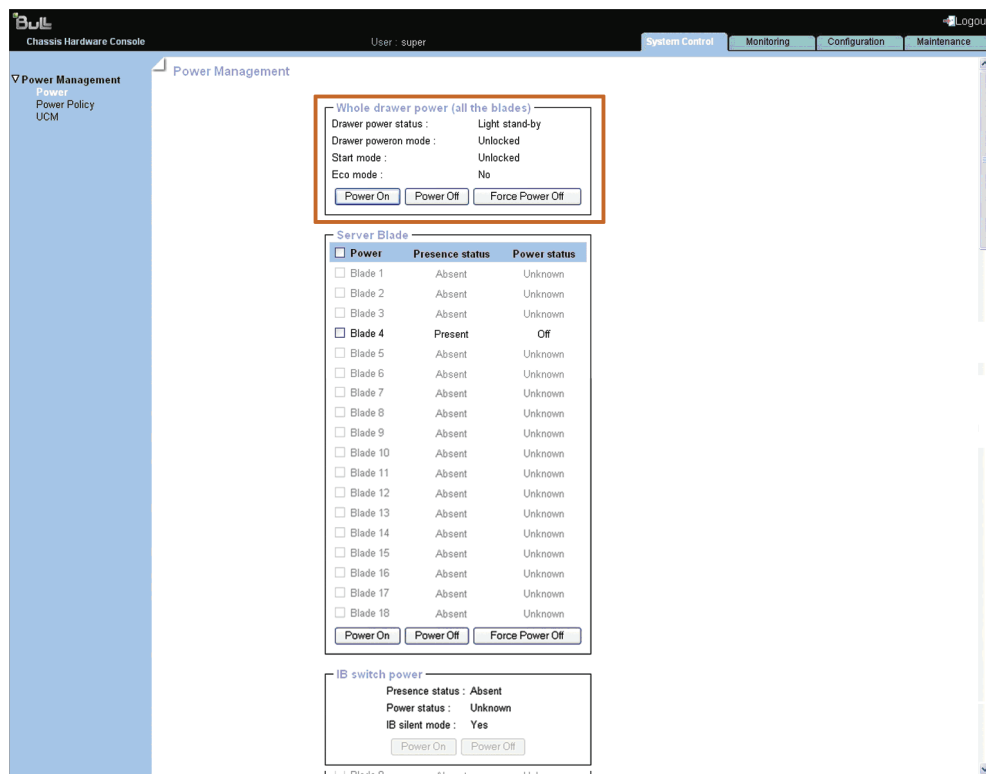


Figure 3-1. Whole drawer power page

Power Information	
Drawer power status	<p>Indicates the status of drawer power.</p> <ul style="list-style-type: none"> • 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 the moderate power consumption waking state for the drawer • Main power: This state is the functional state of the drawer
Drawer power on mode	<p>Indicates the status of drawer power on mode.</p> <ul style="list-style-type: none"> • 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	<p>Indicates the status of start mode.</p> <ul style="list-style-type: none"> • Deep Stand-by: The bullx B500 compute blade stays in stand-by off state (i.e. BMC is not running) • Light Stand-by: The bullx B500 compute blade state becomes stand-by on (i.e. the BMC will be running) • Unlocked Power: The bullx B500 compute blade state becomes Off (i.e. the BMC will be running and the 12V power is enabled)
Eco mode	<p>Indicates the status of Eco mode.</p> <ul style="list-style-type: none"> • Yes: This forces drawer to silent mode. (The drawer can be configured to save the energy when the bullx B500 compute blades are not more used. The drawer will be in awakened state with very low power consumption (deep stand-by state) as soon as blades inactivity are detected) • No: This forces drawer to off

Table 3-2. Whole drawer power page description

3.1.2 Powering on the bullx blade chassis

The bullx blade system can be powered on from the CHC.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **System Control** tab, expand **Power Management**, and click **Power** to open the Whole drawer power page.

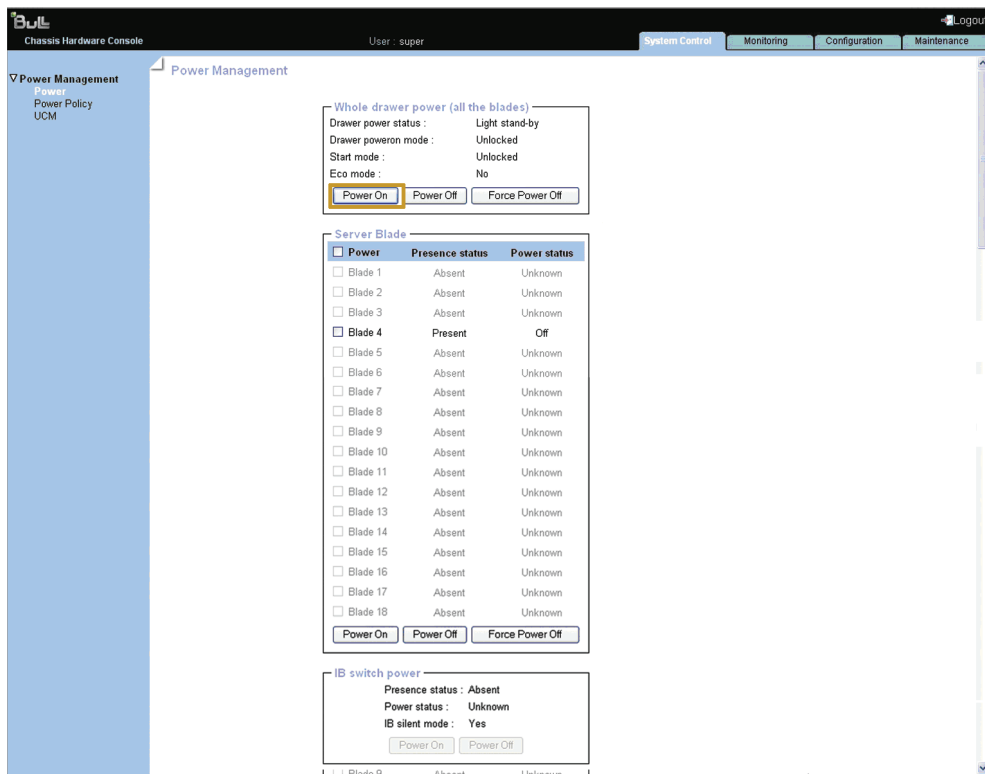


Figure 3-2. Powering on the bullx blade chassis

Power on information	
Power on	<p>Launches the power up sequence. The final state of bullx B500 compute blades depends on the setting Drawer Poweron mode.</p> <p>If the Drawer Poweron mode is Full Power On, the blade is powered up and the OS is booted.</p> <p>If the Drawer Poweron mode is Unlocked, the blade reaches the Off (unlocked) power state.</p>

Table 3-3. Power on features

- From the **Whole drawer power** box, 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.
- Connect to the **Remote System Console** to follow the power on sequence.

3.1.3 Powering off the bullx blade chassis

The system can be powered off from the CHC.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

- From the **System control** tab, expand **Power Management**, and click **Power** to open the Power Management page.

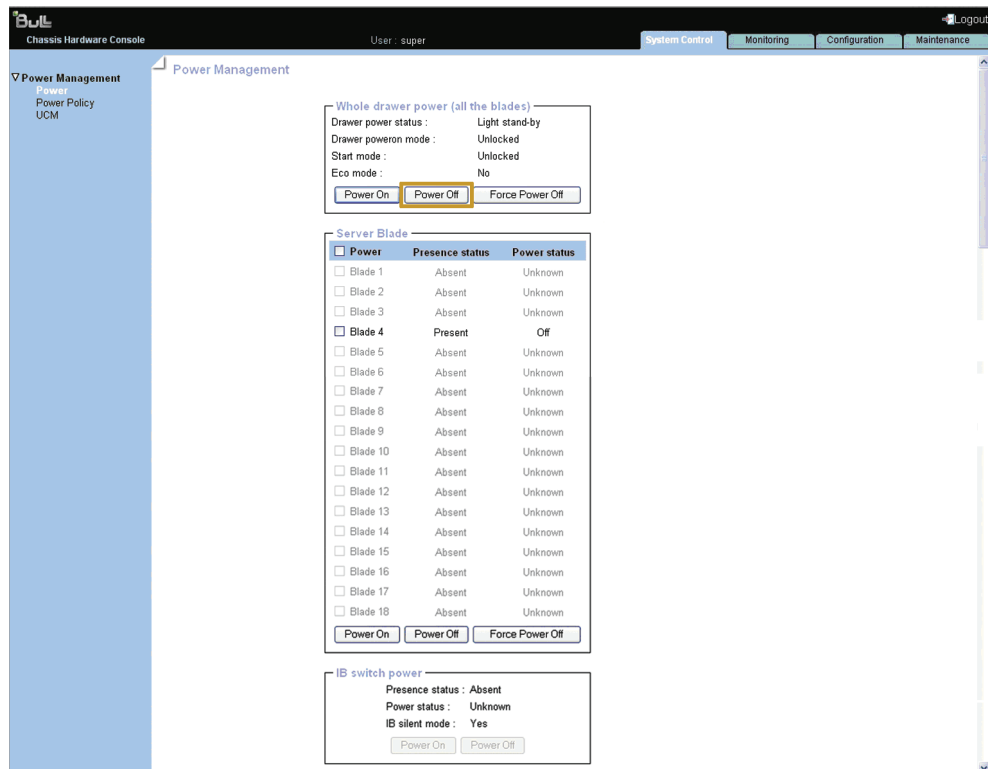


Figure 3-3. Powering off the bullx blade chassis

Power off Information	
Power Off	The hardware is powered down from the main power mode to the Power Off (Unlocked) mode.

Table 3-4. Powering Off

- From the **Whole drawer power box**, click **Power Off** to launch the routine power down sequence, which may take a few minutes to complete. This powering off causes a graceful shutdown of each bullx B500 compute blade.
Once the power down sequence is completed, the **Power State** value switches from **On** to **Off**.
- Connect to the **Remote System Console** to follow the power off sequence.

If the system remains in the **Power On** state after a **Power Off** operation, it may be due to:

- The power sequence has not completed
- The system is frozen or does not respond to the **Power Off** request (you can check the Operating System settings)

You may need to forcibly power down the system using the **Force Power Off** button.

3.1.4 Forcibly powering off the bullx blade chassis

In the event of a system crash or freeze, the system can be forcibly powered Off from the CHC.

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. From the **System Control** tab, expand **Power Management**, and click **Power** to open the Power Management page.

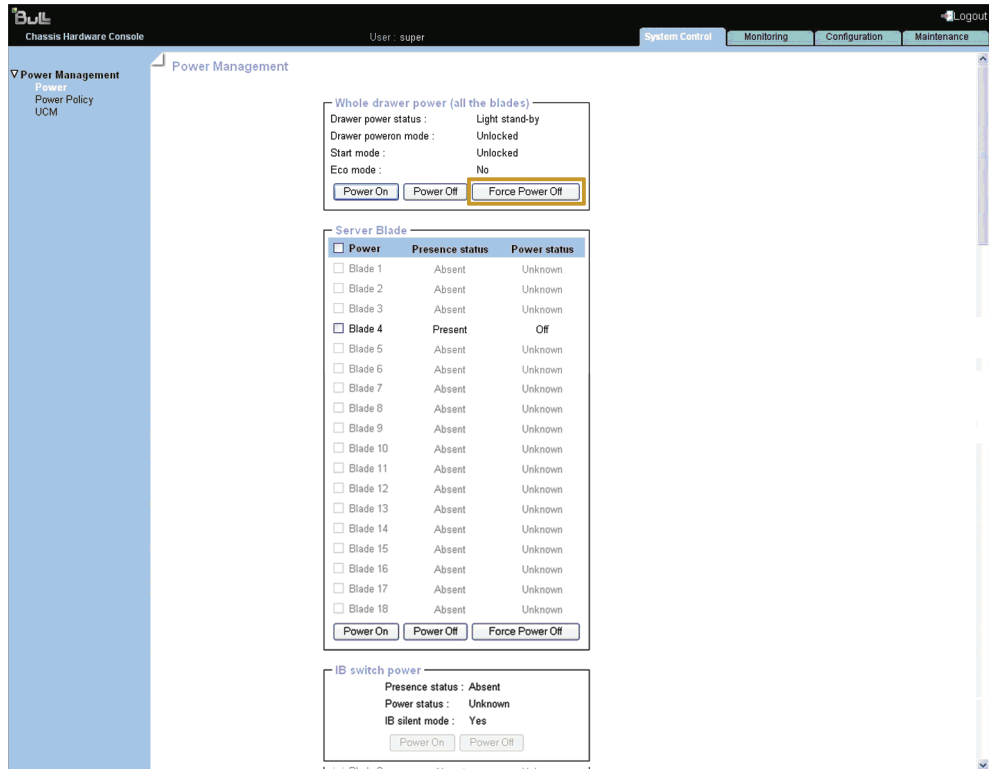


Figure 3-4. Forcibly powering off the bullx blade chassis

Force power off	
Force Power Off	Performs a power down sequence independently of the Operating System. If the Power Off operation fails, you can forcibly power Off by clicking the Force Power Off button.

Table 3-5. Forcibly powering off the bullx blade chassis

2. From the **Whole drawer power box**, click **Force Power Off** to launch the selected sequence, which may take a few minutes to complete.

3.1.5 Viewing bullx B500 compute blade information

The bullx B500 compute blades information such as Power status and Presence status are displayed in this interface. Also, you can perform **Power On**, **Power Off**, and **Forcibly Power Off** tasks for the bullx B500 compute blades.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **System control** tab, expand **Power Management**, and click **Power** to open the Power Management page.

In the Power Management page the second information box is the Server blade.

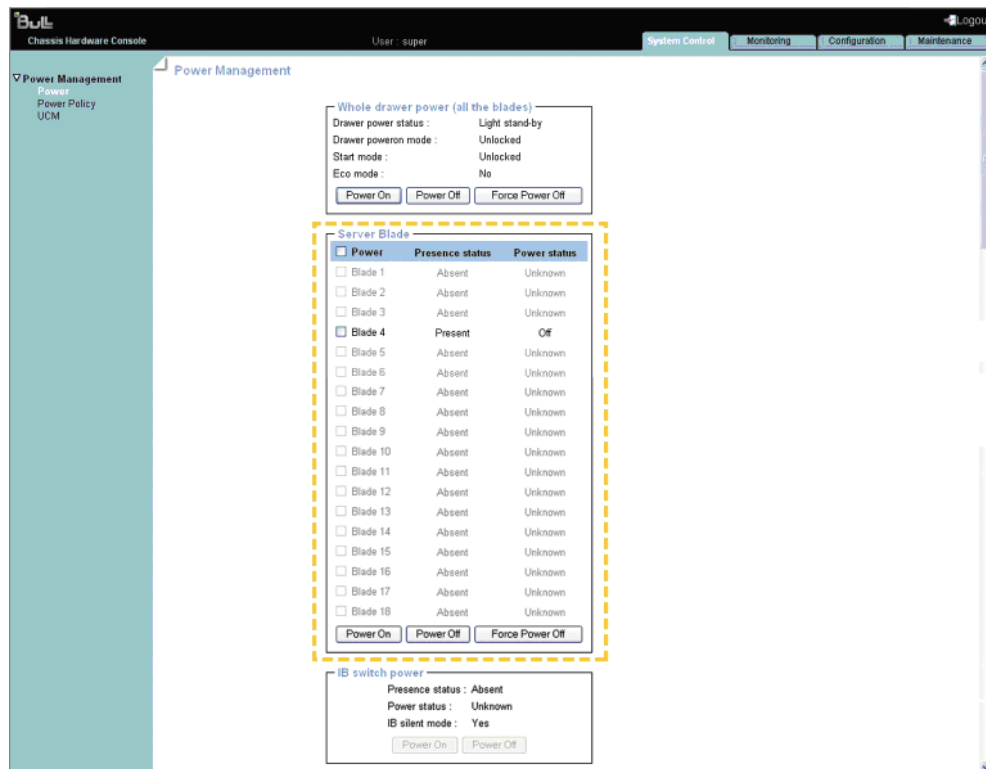


Figure 3-5. Server blade page

Server blade	
Power On	Accessible only when the system is powered Off. This button powers On the corresponding bullx B500 compute blade.
Power Off	Accessible only when the system is powered On. This button powers Off the corresponding bullx B500 compute 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.

Table 3-6. Server blade page description

3.1.6 Viewing IB switch module policies

IB switch policies provide the information of **Presence status**, **Power status**, and **IB silent mode**.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **System control** tab, expand **Power Management**, and click **Power** to open the Power Management page.
In the power management page the third box is the **IB switch power**.

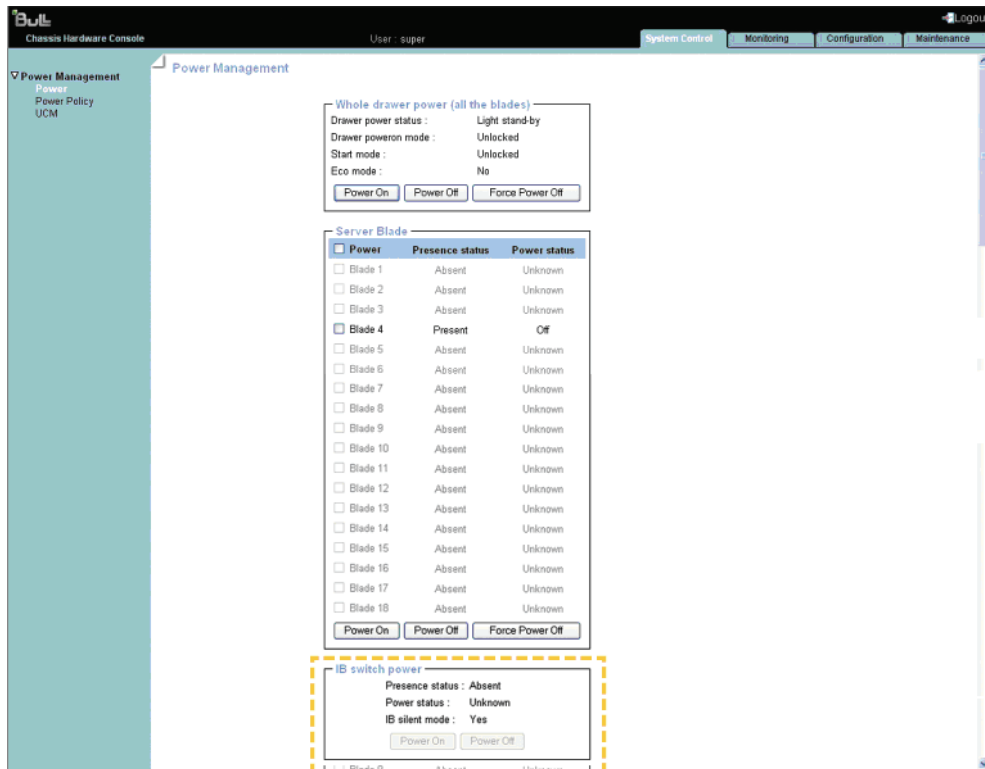


Figure 3-6. IB switch policies

IB switch policies	
Presence status	<p>Indicates the status of Quad Switch Module.</p> <ul style="list-style-type: none"> • Absent: The Quad Switch Module is absent • Present: The Quad Switch Module is present
Power status	<p>Indicates the Power status.</p> <ul style="list-style-type: none"> • 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	<p>Provides the status of IB silent mode.</p> <ul style="list-style-type: none"> • Yes: The IB switch silent mode is set to silent • No: The IB switch can be explicitly powered on/off

Table 3-7. IB switch policies

3.2 Applying power policies

The Power Policies page provides the following information on Power policy and you can set the policies accordingly.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **System Control** tab, expand **Power Management**, and click **Power Policy** to open the Power Policy page.

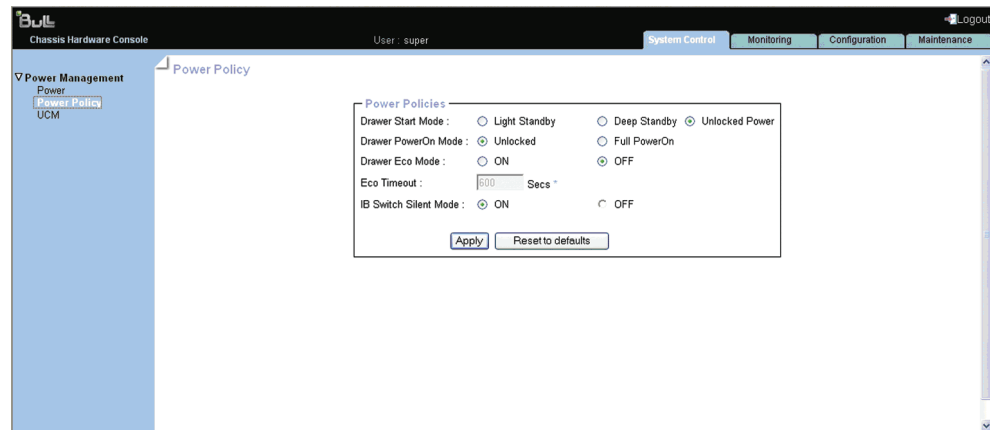


Figure 3-7. Power Policy page

Feature	Option
Drawer start mode	<ul style="list-style-type: none"> • Light stand by: The Light stand-by state is the moderate power consumption waking state for the drawer (the bullx B500 compute blades are operational) • Deep stand by: The Deep stand-by state is the lowest power consumption waking state for the drawer • Unlocked power: In this mode 12V is enabled at the entry of each blade
Drawer power on mode	<ul style="list-style-type: none"> • Unlocked: This means all the blades and other boards are unlocked (12 V hot swap enabled) when the drawer powering on is launched • Full power on: This means all the blades and other boards are powered on when the drawer powering on is launched

Feature	Option
Drawer ECO mode	<ul style="list-style-type: none"> • ON: This forces drawer to eco mode to be On. (The drawer can be configured to save the energy when the bullx B500 compute blades are not used extensively. The drawer will be in an awakened state with very low power consumption – Deep stand-by state – when blades inactivity is detected after time defined in setting eco time out. This mode forces automatically the IB switch silent mode to be ON) • OFF: This forces drawer eco mode to be off
Eco time out	Sets the time for eco mode in seconds.
IB Switch Silent Mode	<ul style="list-style-type: none"> • ON: This forces IB switch silent mode to be silent (The IB switch is implicitly powered. The IB switch is powered on when the first bullx B500 compute blade is powered on. The IB switch is powered off when the last bullx B500 compute blade is powered off) • OFF: This forces IB switch silent mode to be not silent. (The IB switch can be explicitly powered on/off.)

Table 3-8. Power policy description

2. Once the power policies page appears you can click the necessary information buttons to enable the bullx blade chassis.
3. Click **Apply** to apply the changes.

3.3 Viewing Ultra Capacitor Module

UCM is an optional device. The UCM information page provides information of the UCM device.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

From the **System Control** tab, expand **Power Management**, and click **UCM** to get Ultra Capacitor Module Information page.

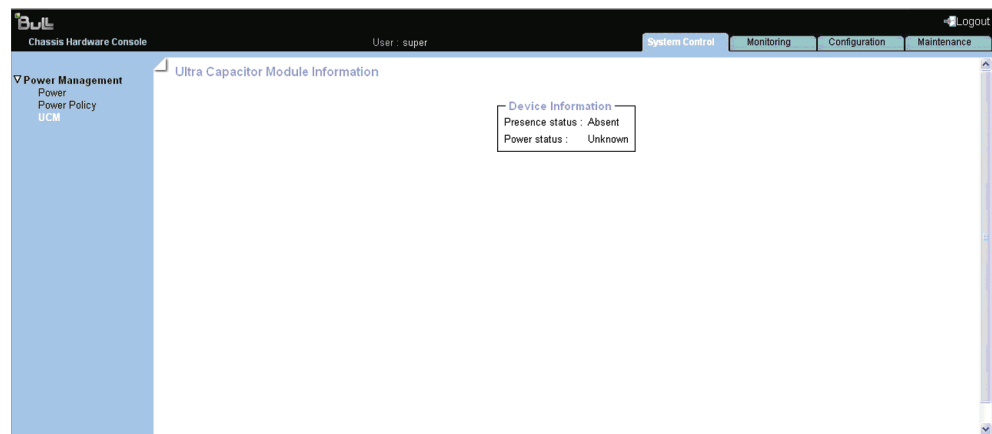


Figure 3-8. Ultra Capacitor Module page

Ultra Capacitor Module Information	
Presence status	Absent or present depending on the presence of the UCM.
Power status	Provides the power status of the UCM (On/Off).

Table 3-9. UCM description

Chapter 4. Monitoring the bullx blade chassis

The monitoring tab provides access to CMC status, logs, and messages.

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

- Sensors status
- System Event Log (SEL)
- Board and Security Messages

4.1 Viewing sensor status

The server is equipped with various sensors that monitor:

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

Procedure

1. From the **Monitoring** tab, expand **Cabinet Status & Logs**, and click **Sensor** to display the Sensor Status page.

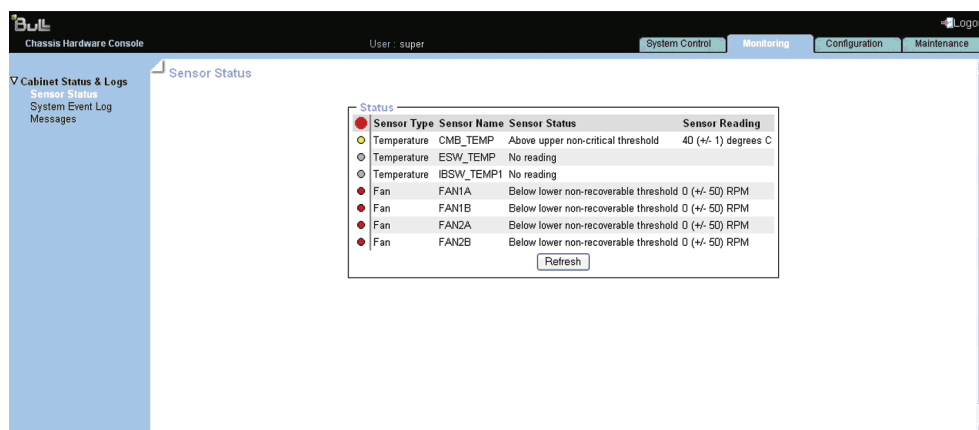


Figure 4-1. Sensor Status page

2. Click **Refresh** and check if all component icons are green.

Icon	Type	Name	Status	Reading
	Power Supply	PS_X	<ul style="list-style-type: none"> • Device Present • Device Absent 	-
	Power Unit	Pwr Redundancy	<ul style="list-style-type: none"> • No reading • Fully redundant • Redundancy Lost 	-
	Power	Pwr Consumption	-	Value in Watts
	Processor	PROC_X	No reading	-
Green Red Yellow Grey	Temperature	CMB_TEMP ESW_TEMP IBSW_TEMP1	<ul style="list-style-type: none"> • Above upper non-critical threshold • No reading 	Value in °C
Green Red Yellow Grey	Fan blade	FAN X	<ul style="list-style-type: none"> • Below power non recoverable threshold • Ok 	Value in RPM

Table 4-1. Sensor status page description

Status Icon Description	
Green	NORMAL This component is operating correctly.
Yellow	NON-CRITICAL
Red	CRITICAL This component is not operating correctly. A problem has been detected. Immediate preventive or corrective action is required.
Grey	NOT-AVAILABLE

Table 4-2. Sensor status icons description

4.2 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. From the **Monitoring** tab, expand **Cabinet Status & Logs**, and click **System Event Log** to open the System Event Log page.

The screenshot displays the System Event Log page. The interface includes a navigation menu on the left with 'Cabinet Status & Logs', 'Sensor Status', 'System Event Log', and 'Messages'. The main content area shows a table of event logs. The table has the following columns: Event Type, Date, Time, Sensor Name, Description, and Direction. The table is divided into two sections by a dashed line. The top section contains 15 entries, and the bottom section contains 20 entries. The interface includes a 'Log' header with 'Clear' and 'Refresh' buttons, and a 'Used Entries: 512 / 512' indicator.

Event Type	Date	Time	Sensor Name	Description	Direction
SEL record 02	Pre-Init	00:00:43	FAN2B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN2B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN2A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN2A	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN2A	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1B	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1A	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:00:43	FAN1A	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:05:46	FAN2B	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:05:46	FAN2B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:05:46	FAN2B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:05:46	FAN2A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN2A	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1B	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1A	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:29:56	FAN1A	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2B	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2A	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN2A	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1B	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1B	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1B	Lower Non-critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1A	Lower Non-recoverable going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1A	Lower Critical going low	Assertion Event
SEL record 02	Pre-Init	00:01:50	FAN1A	Lower Non-critical going low	Assertion Event

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.

4.3 Viewing board and security messages

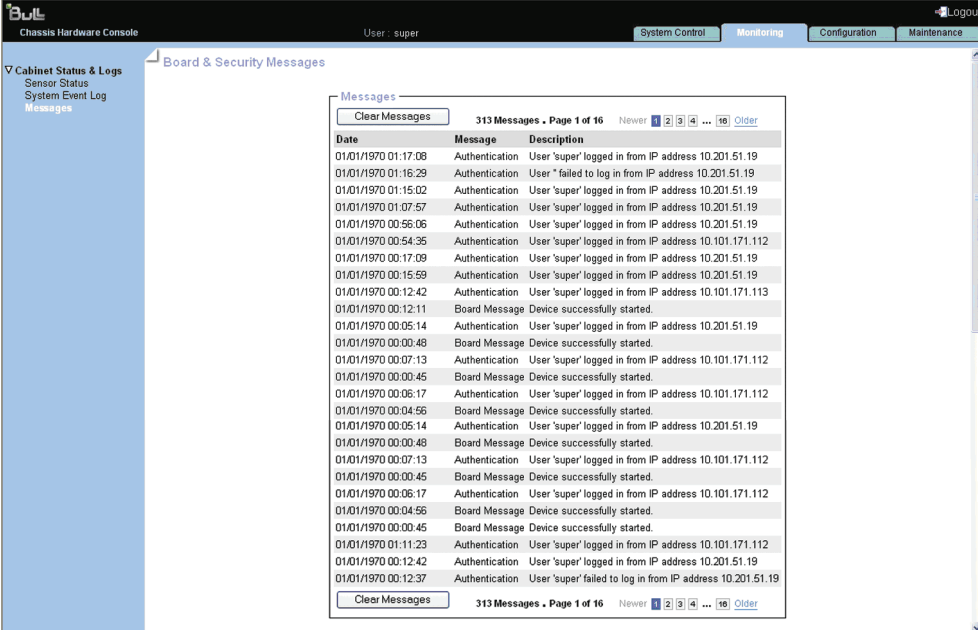
The Board and Security Messages record non-hardware-related events, such as user authentication, connection to the remote console, security violation, log deletion or firmware upgrade. However, hardware-related events are recorded in the SEL.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Monitoring** tab, expand **Cabinet Status & Logs**, and click **Messages** to open the Board & Security Messages page.



The screenshot displays the 'Board & Security Messages' page. The interface includes a navigation menu on the left with 'Messages' selected. The main content area shows a table of messages with the following columns: Date, Message, and Description. The messages are sorted by date, showing a sequence of authentication events and board messages. The table is paginated, showing 'Page 1 of 16' and '313 Messages'.

Date	Message	Description
01/01/1970 01:17:08	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 01:16:29	Authentication	User ' failed to log in from IP address 10.201.51.19
01/01/1970 01:15:02	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 01:07:57	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:56:06	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:54:35	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:17:09	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:15:59	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:12:42	Authentication	User 'super' logged in from IP address 10.101.171.113
01/01/1970 00:12:11	Board Message	Device successfully started.
01/01/1970 00:05:14	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:00:48	Board Message	Device successfully started.
01/01/1970 00:07:13	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:00:45	Board Message	Device successfully started.
01/01/1970 00:06:17	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:04:56	Board Message	Device successfully started.
01/01/1970 00:05:14	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:00:48	Board Message	Device successfully started.
01/01/1970 00:07:13	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:00:45	Board Message	Device successfully started.
01/01/1970 00:06:17	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:04:56	Board Message	Device successfully started.
01/01/1970 00:00:45	Board Message	Device successfully started.
01/01/1970 01:11:23	Authentication	User 'super' logged in from IP address 10.101.171.112
01/01/1970 00:12:42	Authentication	User 'super' logged in from IP address 10.201.51.19
01/01/1970 00:12:37	Authentication	User 'super' failed to log in from IP address 10.201.51.19

Figure 4-3. Board & Security Messages page

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



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 bullx blade chassis

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

- Configuring the general settings
- Managing users
- Configuring security management
- Configuring alert settings

5.1 Configuring the general settings

The **Configuration** tab provides access to General Setting page.

5.1.1 Configuring the bullx blade chassis

The Chassis Settings page allows you to set in the bullx blade chassis name.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Configuration** tab, expand **General Settings**, and click **Chassis** to open the Chassis Settings page.

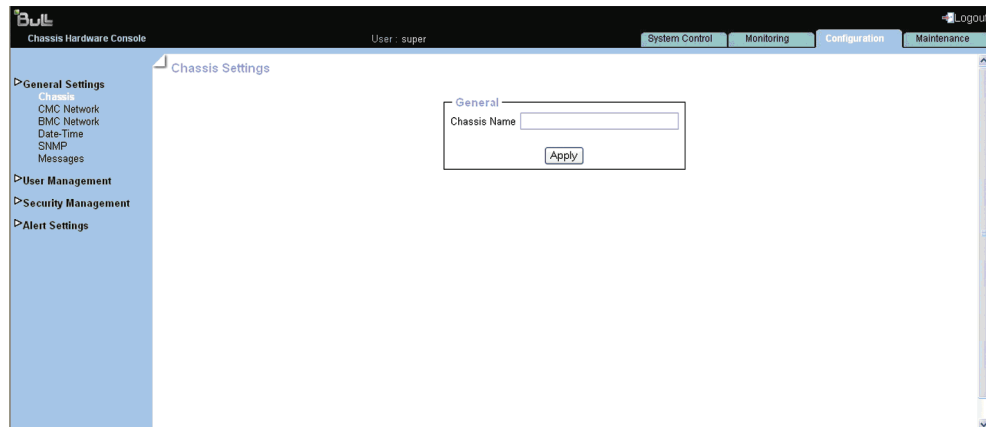


Figure 5-1. Chassis Settings page

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

5.1.2 Configuring the CMC network

The CMC Network Settings allow you to remotely connect to CMC.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Configuration** tab, expand **General Settings**, and click **CMC Network** to open the CMC Network Setting page.

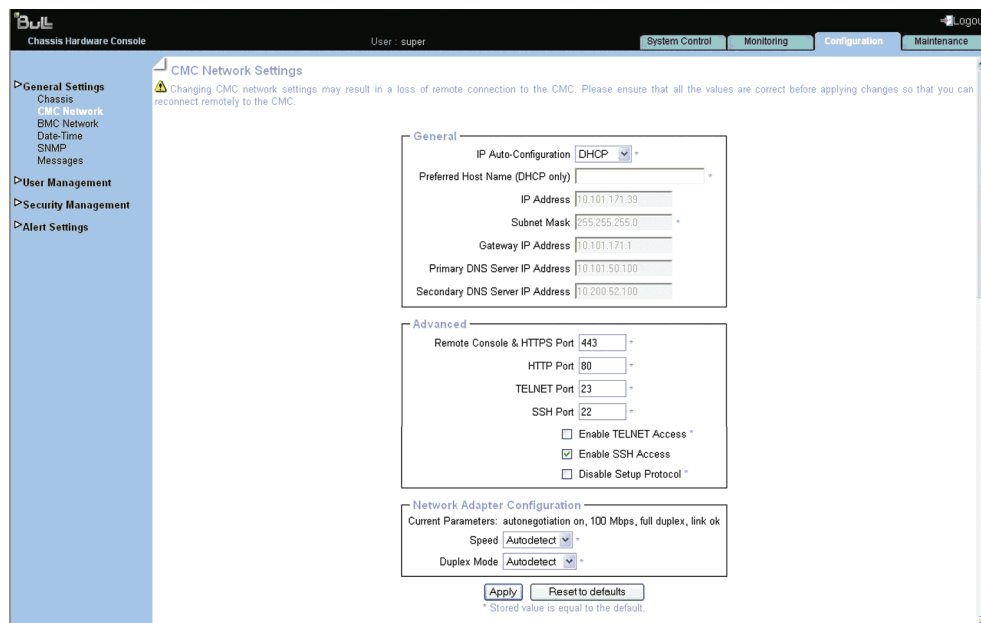


Figure 5-2. CMC Network Settings page

General box	
IP Auto-Configuration	This drop-down list allows you to enable or disable network auto-configuration via a DHCP or BOOTP server: <ul style="list-style-type: none"> • None: Auto-configuration is disabled • DHCP: Network settings are retrieved from a DHCP server (factory-default value) • BOOTP: Network settings are retrieved from a BOOTP server
Preferred Host Name (DHCP only)	Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if 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.

General box	
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 used for secure HTTPS connections and for the remote console (Factory-default: 443).
HTTP Port	The port number used for standard HTTP connections (Factory-default: 80).
TELNET Port	The Telnet port number (Factory-default: 23).
SSH Port	The Secure Shell (SSH) port number (Factory-default: 22).
Enable TELNET Access	Select this option to 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 the <i>psetup (Windows)/mc-setup (Linux) tool</i> , used to discover the bullx blade system on the LAN during initial setup, from re-detecting this bullx blade system when installing other devices.
Network Adapter Configuration Box	
Current Parameters	Displays current network adapter settings.
Speed	LAN interface speed. <ul style="list-style-type: none"> • Autodetect: Automatically adjusts the interface speed (factory-default value). • 10Mbps: fixed speed according to network. • 100Mbps: fixed speed according to network. Autodetect is selected by default. If you encounter connection problems, select the fixed speed required by your network infrastructure.
Duplex Mode	LAN interface duplex mode. <ul style="list-style-type: none"> • 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 field 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 CHC.

5.1.3 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 from a computer or workstation with a web browser.

Prerequisites

- Viewing: All users
- Operations: Root users



CAUTION

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

Procedure

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

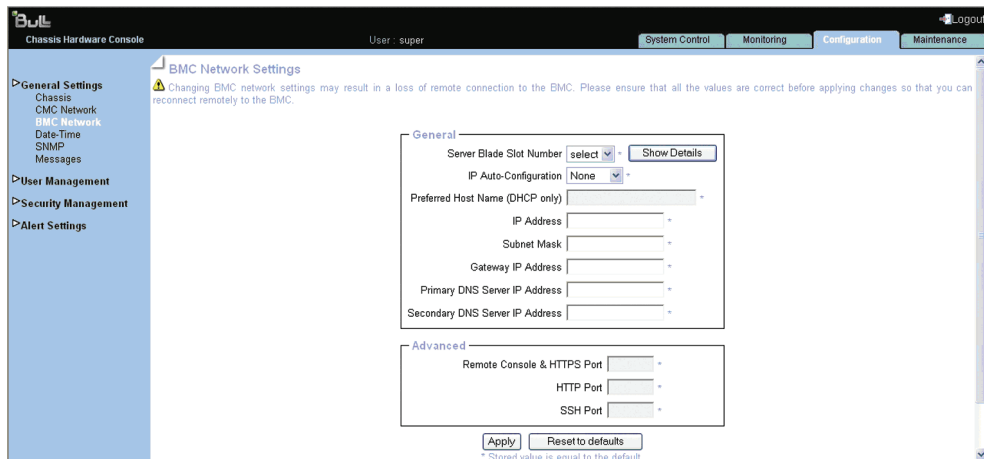


Figure 5-3. BMC Network Settings page

General box	
Server Blade Slot Number	This drop-down lists all the bullx B500 compute blades. Show Details: Provides the information of the bullx B500 compute blade.
IP Auto-Configuration	This drop-down list allows you to enable or disable network auto-configuration via a DHCP or BOOTP server: <ul style="list-style-type: none"> • None: Auto-configuration is disabled. • DHCP: Network settings are retrieved from a DHCP server (Factory-default value). • BOOTP: Network settings are retrieved from a BOOTP server.
Preferred Host Name (DHCP only)	Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if 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.

General box	
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.

5.1.4 Configuring date and time

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 a 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. From the **Configuration** tab, expand **General Settings**, and click **Date-Time** to display the Date/Time Settings page.

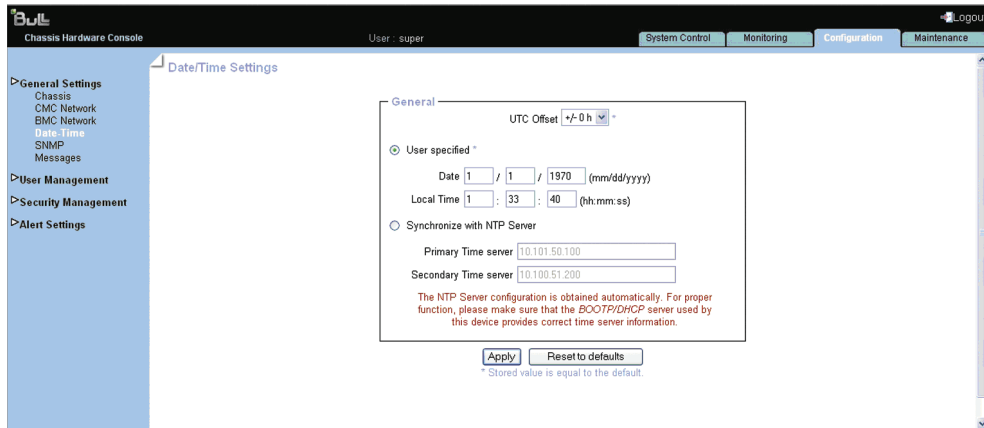


Figure 5-4. Date/Time Settings page

General	
UTC Offset	UTC Offset allows you to set the difference between local and universal time. You must use this drop-down list if you select Synchronize with NTP Server.
User specified	This option allows you to manually set the bullx 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	This option allows you to enter the IP addresses of the NTP servers that you want to use. You must use the UTC Offset drop-down list.
View Defaults	Allows you to display factory-default values (Stored value is equal to the default).

Table 5-3. Date/Time Settings page description

2. If required, change the UTC Offset value.
3. Click either **User Specified** or **Synchronize with NTP Server**, complete the appropriate fields and click **Apply**.

-
- Notes**
- The NTP Server configuration is obtained automatically. For proper function, ensure that the BOOTP/DHCP server used by this device provides correct time server information
 - You can set the factory-default values by clicking **Reset to defaults**
-

5.1.5 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 in your SNMP manager:
 - User logon
 - Access denied
 - Reset
 - Power on/off

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Configuration** tab, expand **General Settings**, and click **SNMP** to display the SNMP Settings page.



Figure 5-5. SNMP Settings page

General	
Area 1	Enable SNMP Agent: When selected, this option allows the SNMP agent to communicate with an SNMP manager.
	System Location bullx blade system name.
	System Contact bullx 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 a SNMP user who has read-only access to the bullx blade system.
	Read Password Read-only user authentication password.
	Write Username Name of an SNMP user who has write access to the bullx 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 bullx blade system (example: public).
	Write Community SNMP write community name for the bullx blade system.
Area 4	Download the SNMP MIB file: This link allows you to save, as a .txt file, the bullx blade system MIB file. This file is required by your SNMP manager to interpret trap messages.

Table 5-4. 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:
 - i. To allow data retrieval and event reporting only, complete the Read User Name and Read Password fields only.

- ii. To allow the performance of actions only, complete the Write User Name and Write Password fields only.
 - iii. 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:



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

- i. To allow data retrieval and event reporting only, complete the Read Community field only.
- ii. To allow the performance of actions only, complete the Write Community field only.

2. Click **Apply**.

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

5.1.6 Saving the message log

This section describes how to record 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 bullx 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. From the **Configuration** tab, expand **General Settings**, and click **Messages** to display the Board, Security & Remote Console Messages Settings page.



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

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	<p>This option allows board and security messages to be written to a file located on a Network File System (NFS) server.</p> <p>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.</p> <p>Do not use the same file name to write messages from more than a system using the same NFS shared directory.</p>
	NFS Server	NFS server hostname or IP address.
	NFS Shares	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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Login failed • Login succeed

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

2. Complete the **Messaging Policy** box.
3. If necessary, modify the **Messaging Filter** box.
4. Click **Apply**.

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

5.2 Managing Users

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

5.2.1 Creating a user account

The bullx 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.



The bullx 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. From the **Configuration** tab, expand **User Management**, and click **Users** to display the User Management page.

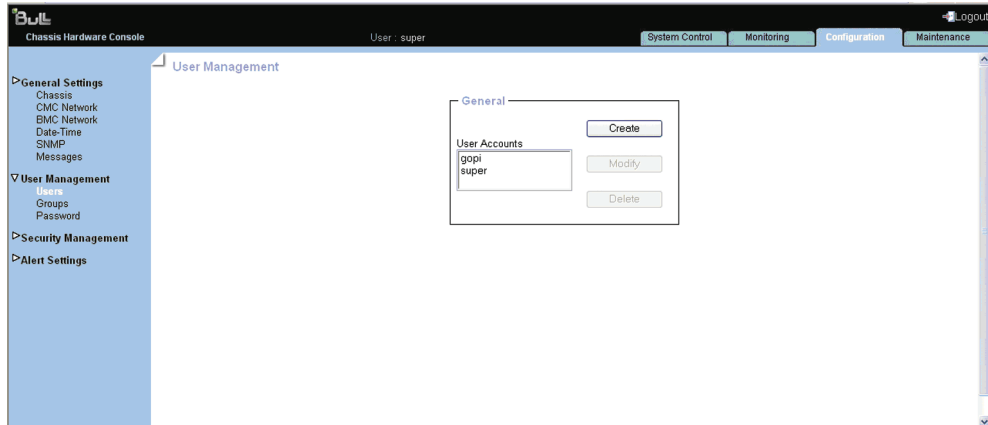


Figure 5-7. User Management page

2. Click **Create** to display the User Creation box.

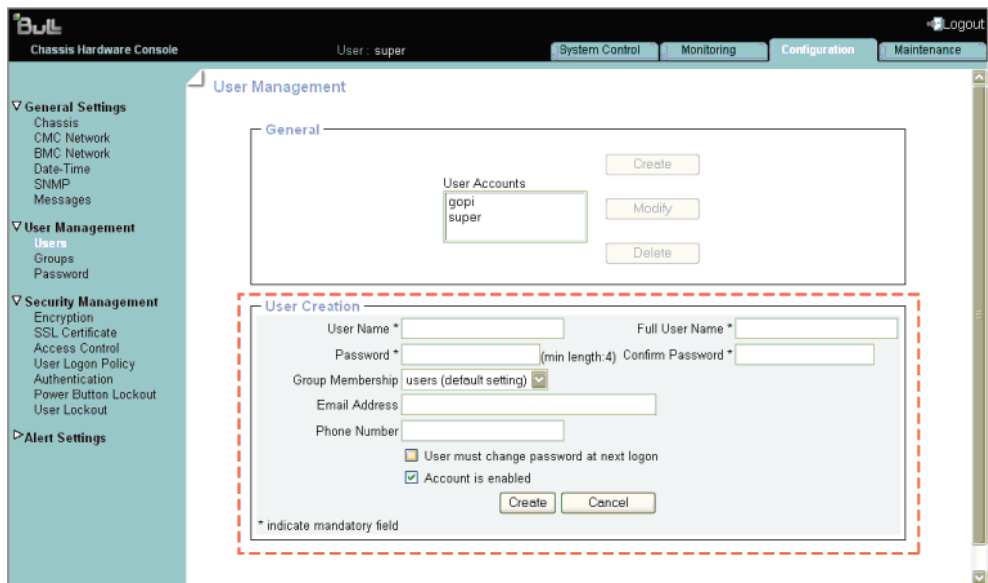


Figure 5-8. User Creation dialog page

3. Complete the fields as required.
4. Click **Apply**.
The user is created and is displayed in the User Accounts box.

5.2.2 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. From the **Configuration** tab, expand **User Management**, click **Users** to display the User Management page.

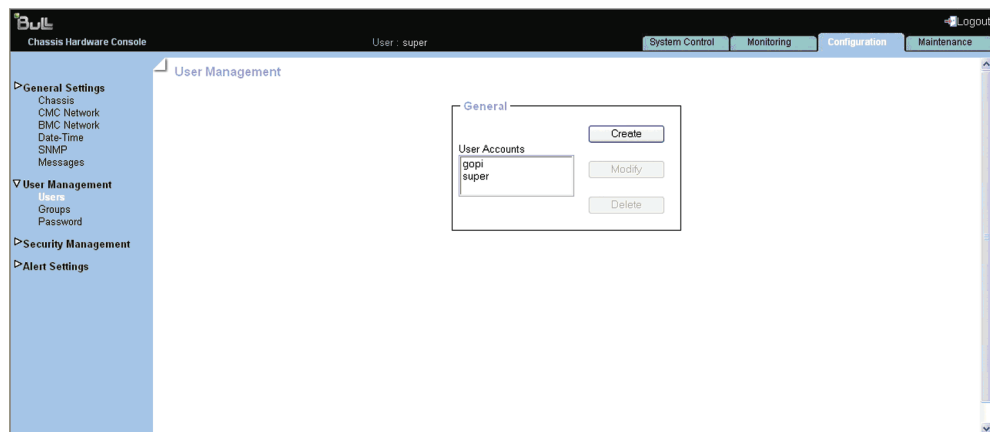


Figure 5-9. User Management page

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.

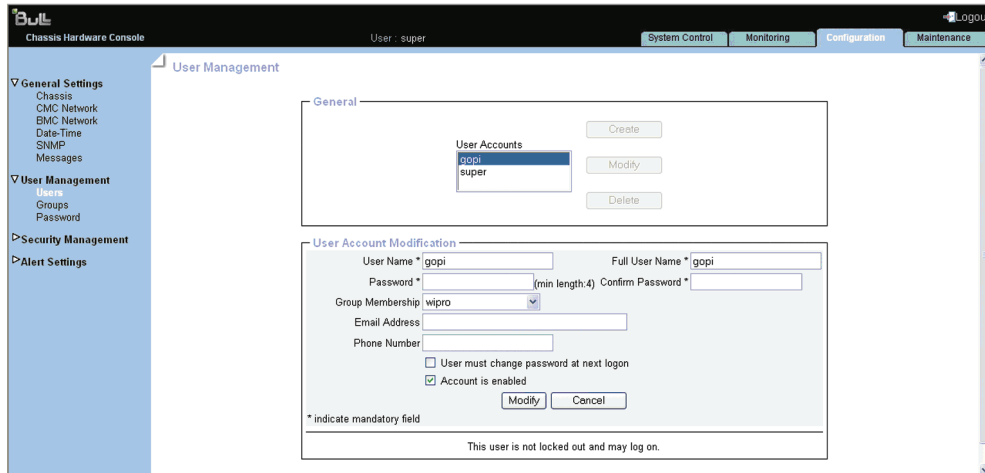


Figure 5-10. User Account Modification box

3. Modify the following fields based on your requirement:
 - **User Name**
 - **Full User Name**
 - **Password and Conform Password**
 - **Group Membership**
 - **Email Address**
 - **Phone Number**
4. Click **Modify**.
User account details have been modified successfully.

5.2.3 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. From the **Configuration** tab, expand **User Management**, and click **Users**. The User Management page appears.

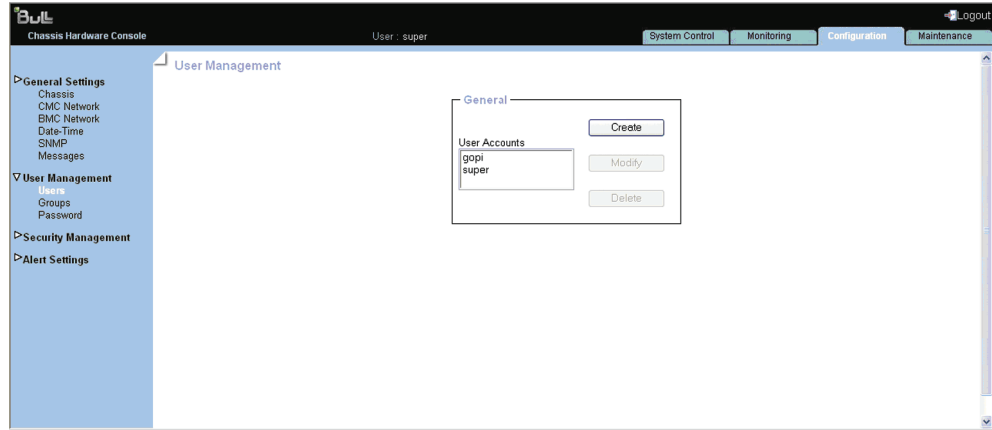


Figure 5-11. User Management page

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

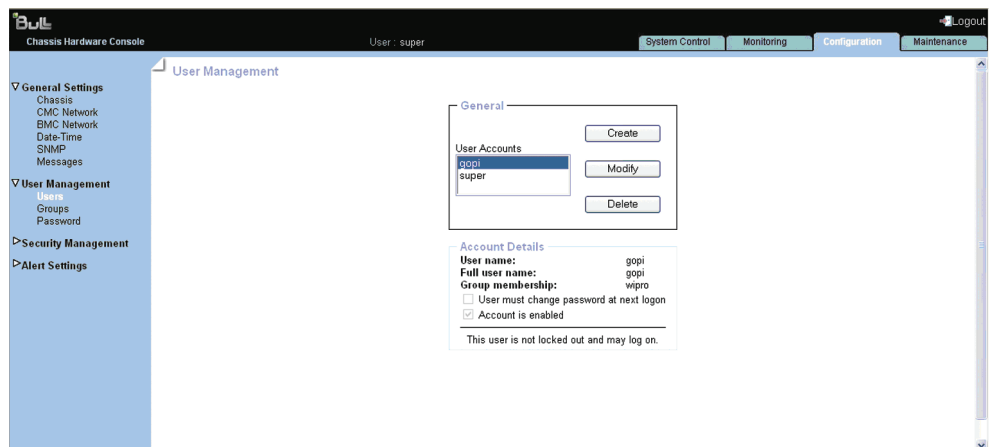


Figure 5-12. Account Details box

5.2.4 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. From the **Configuration** tab, expand **User Management**, and click **Users** to display the User Management page.

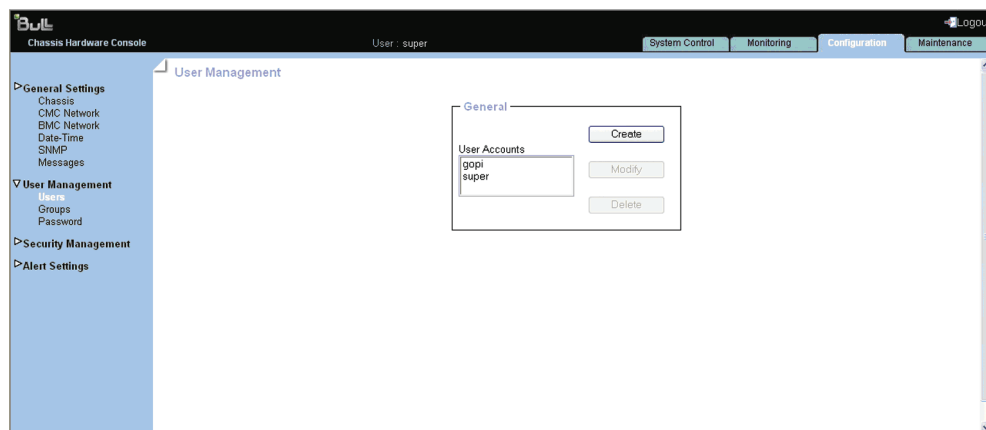


Figure 5-13. User Management page

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

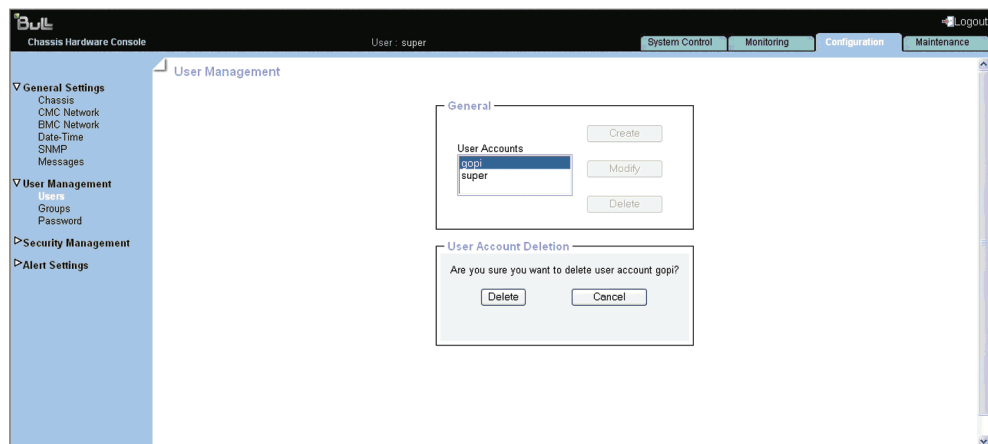


Figure 5-14. Deleting a User Account

3. Click **Delete** to confirm.
The user is removed from the list and from the associated group.

5.2.5 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. From the **Configuration** tab, expand **User Management**, and click **Users** to display the User Management page.

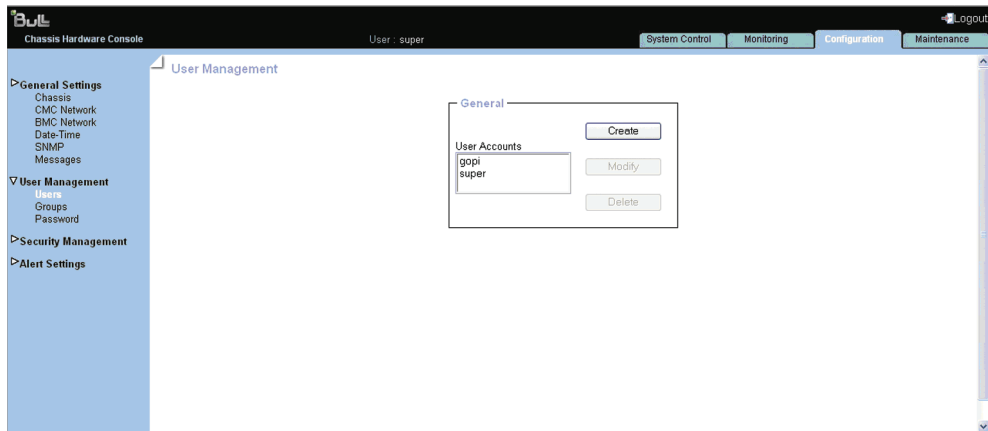


Figure 5-15. User Management page

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.

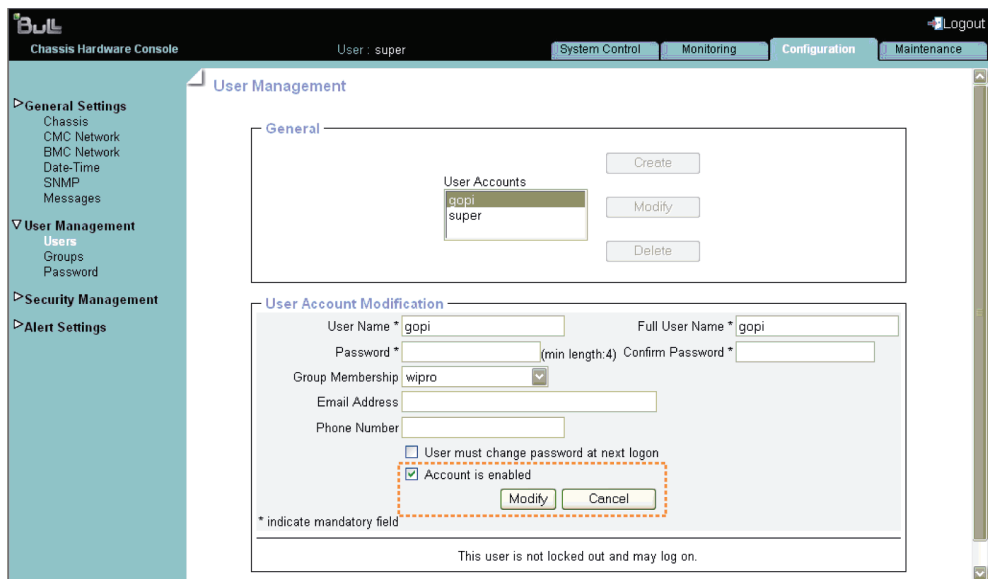


Figure 5-16. User Account Modification

3. To enable/disable the account, check/uncheck the **Account is enabled**.
4. Click **Modify** to update the modification

5.2.6 Creating a group

The bullx 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.



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. From the **Configuration** tab, expand **User Management**, and click **Groups** to open the Group Management page.

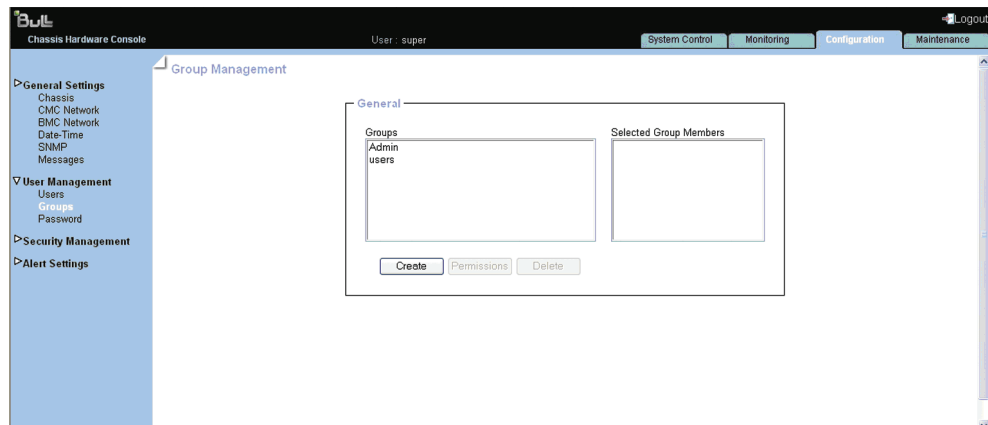


Figure 5-17. Creating a group

2. Click **Create** to open the Group Creation box.

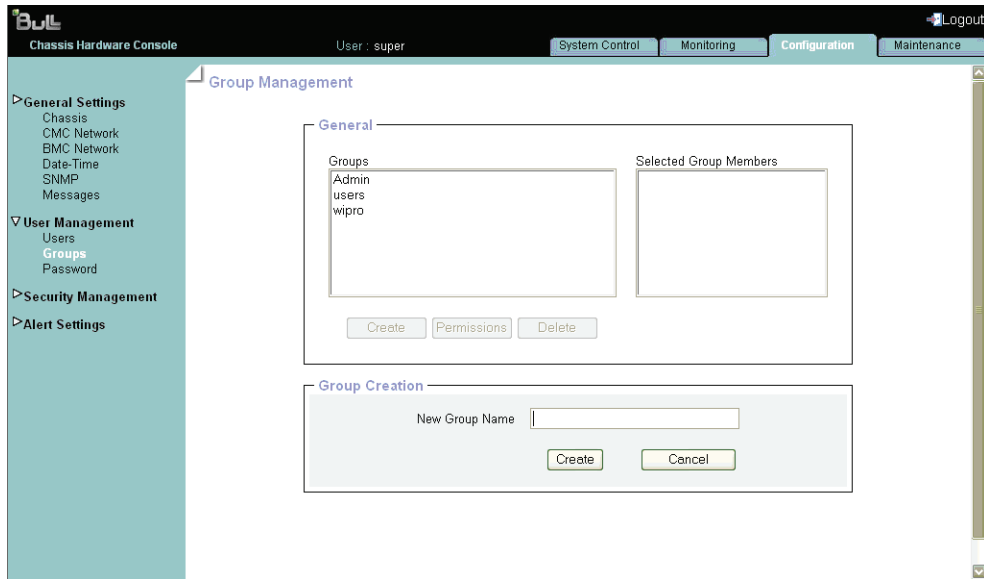


Figure 5-18. Group Creation box

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.

5.2.7 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. From the **Configuration** tab, expand **User Management**, and click **Groups** to open the Group Management page.

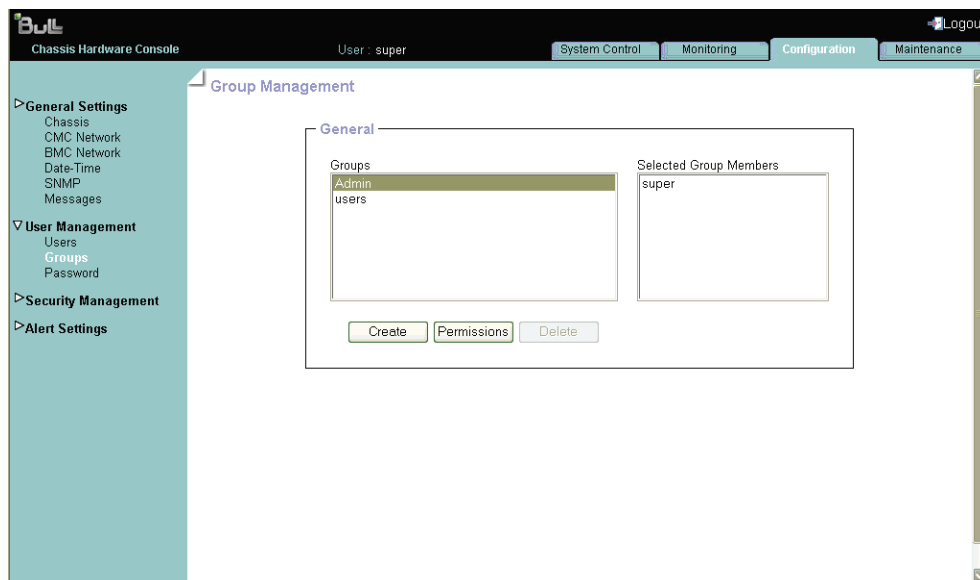


Figure 5-19. Group Management page

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

5.2.8 Deleting a group

You can delete an empty group when no longer needed.



Predefined groups and users cannot be deleted.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Configuration** tab, expand **User Management**, and click **Groups** to open the Group Management page.

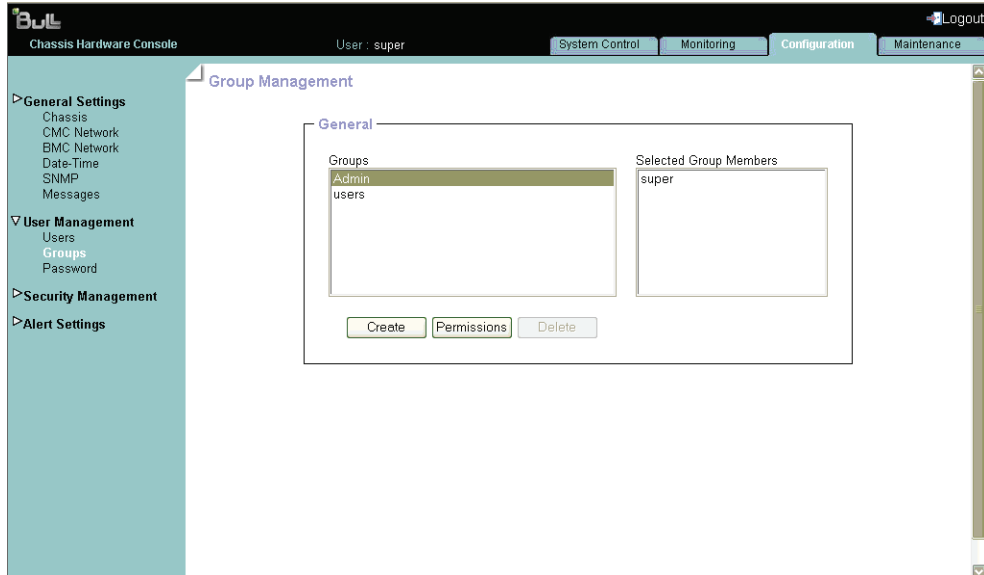


Figure 5-20. Group Management page

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.

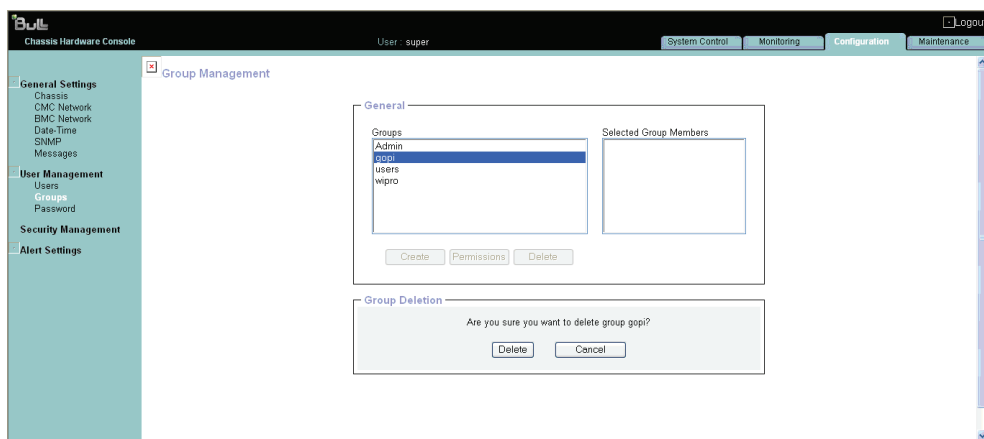


Figure 5-21. Deleting a Group

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

5.2.9 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. From the **Configuration** tab, expand **User Management**, and click **Groups** to display the Group Management page.

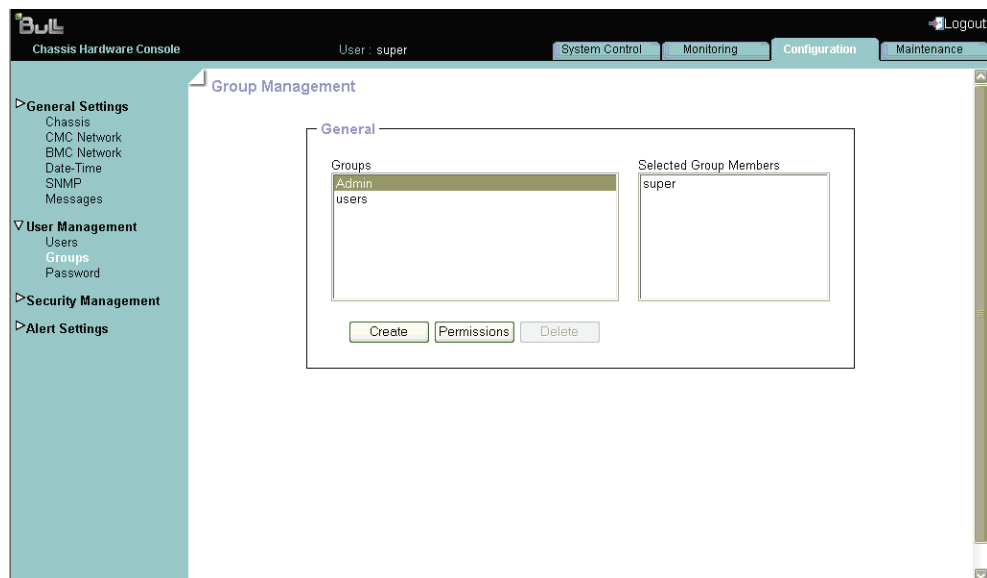


Figure 5-22. Group Management page

2. Select the group and click **Permissions** to display the Group Permissions page.

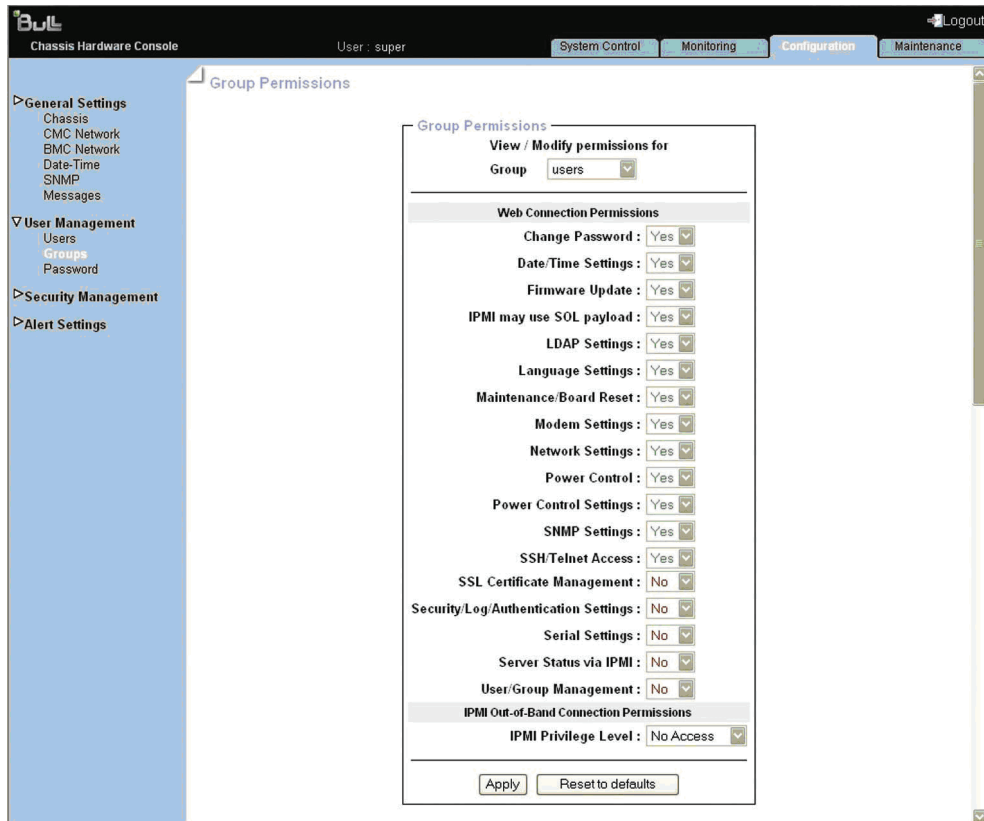


Figure 5-23. Group permission page

5.2.10 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. From the **Configuration** tab, expand **User Management**, and click **Users** to display the User Management page.

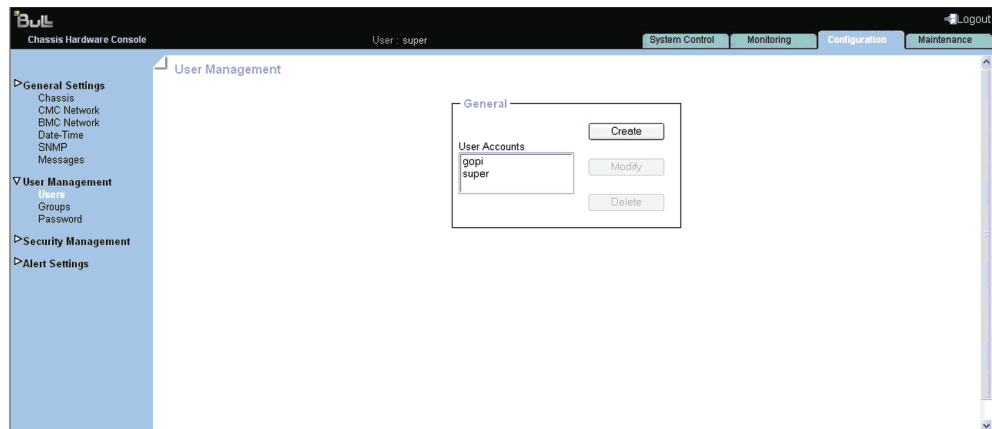


Figure 5-24. User Management page

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.

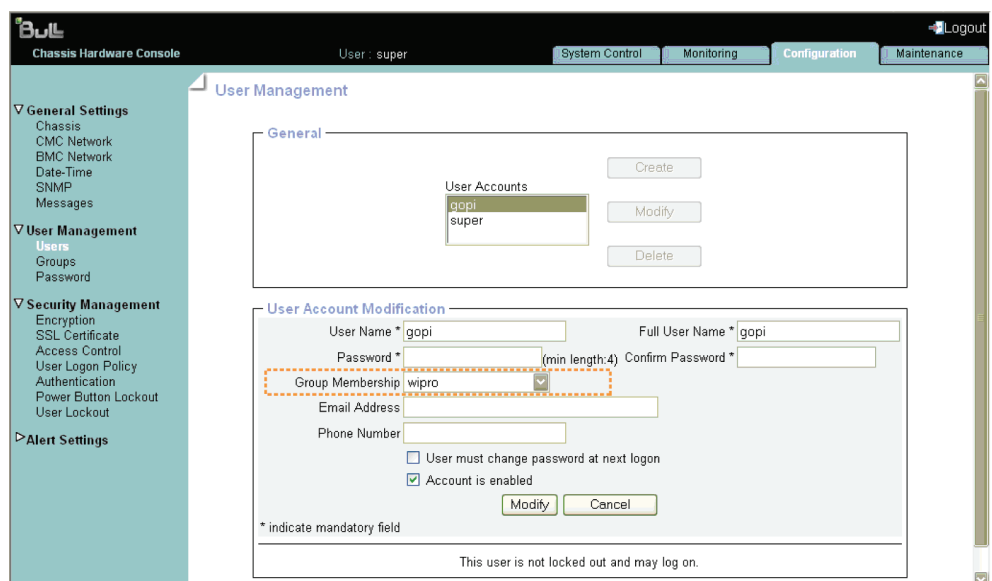


Figure 5-25. User Account Modification box

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

5.2.11 Modifying your password

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

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Configuration** tab, expand **User Management**, and click **Password** to open the Password Management page.

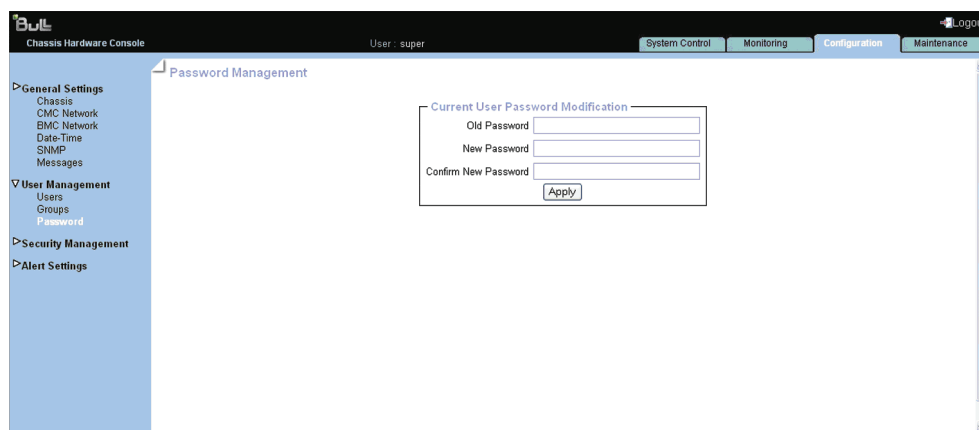


Figure 5-26. Password Management page

2. Complete all the 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.

5.3 Configuring security management

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

5.3.1 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. From then **Configuration** tab, expand **Security Management**, and click **Encryption** to open Encryption Management page.

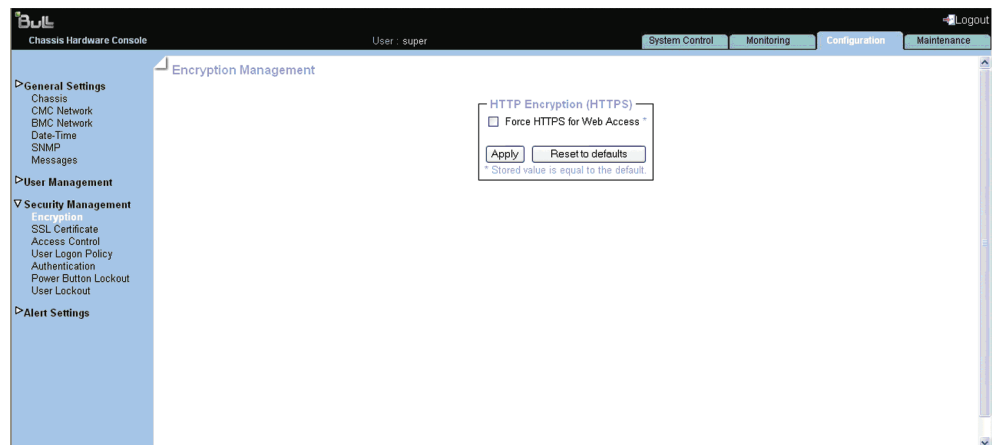


Figure 5-27. Encryption Management page

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

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>

Table 5-6. HTTP Encryption (HTTPS)

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

5.3.2 Installing 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. From the **Configuration** tab, expand **Security Management**, and click **SSL Certificate** to display the SSL Certificate Management page.

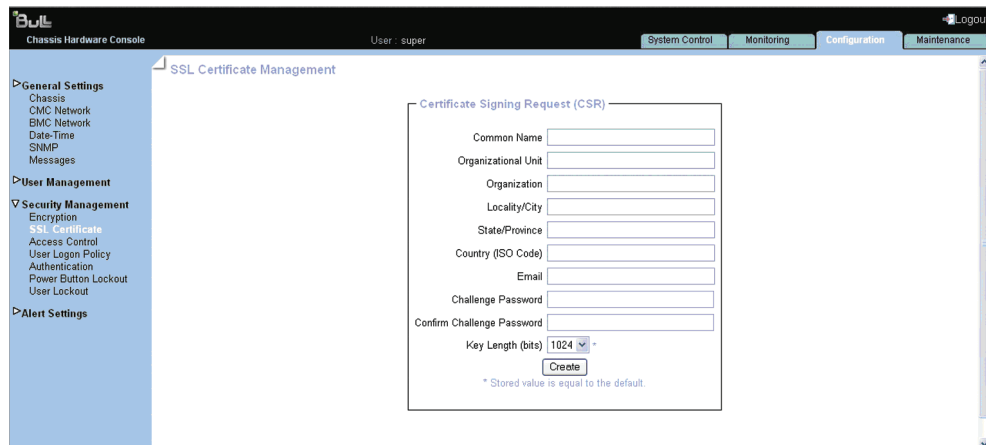


Figure 5-28. SSL Certificate Management page

Certificate Signing Request(CSR)	
Common name	“Fully Qualified Domain Name” (FQDN) (Example: hostName.DomainName.Top-LevelDomain). If the Common Name differs from the network name, a security warning pops up when the bullx blade system is accessed using HTTPS.
Organizational unit	Generally the name of the department (within your organization) using the bullx blade system (or example: Research and Development).
Organization	Name of your organization.
Locality/city	Name of your city.
State/province	Name of your state, province, or region.
Country (ISO Code)	ISO Code for your country (example: FR for France).
Email	Generally the administrator's email address.

Certificate Signing Request(CSR)	
Challenge Password	Depending on your certification authority, you may need to define a challenge password to authorize later changes to the certificate (Example: Revocation of the certificate). The minimal length of this password is four characters.
Confirm Challenge Password	
Key length(bits)	Length of the generated key in bits. Generally 1024 bits. Longer keys may result in slower connection response time.

Table 5-7. SSL Certificate Management page description

2. Complete the fields and click **Create** to generate your CSR.
3. Click **Download** to save the CSR to your computer and send it to the Certification Authority, which 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.

5.3.3 Configuring the logon policy

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

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

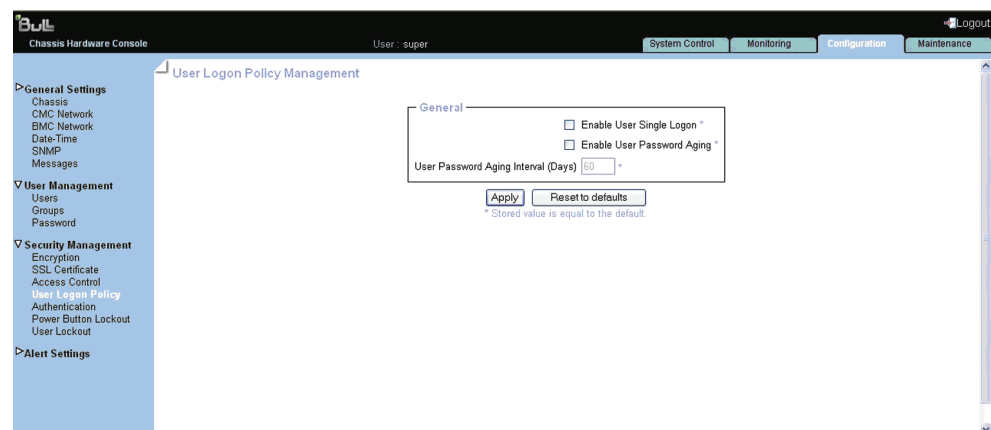


Figure 5-29. User Logon Policy Management page

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 5-8. 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**.

5.3.4 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. From the **Configuration** Tab, expand **Security Management**, and click **Authentication** to display the Authentication Management page.

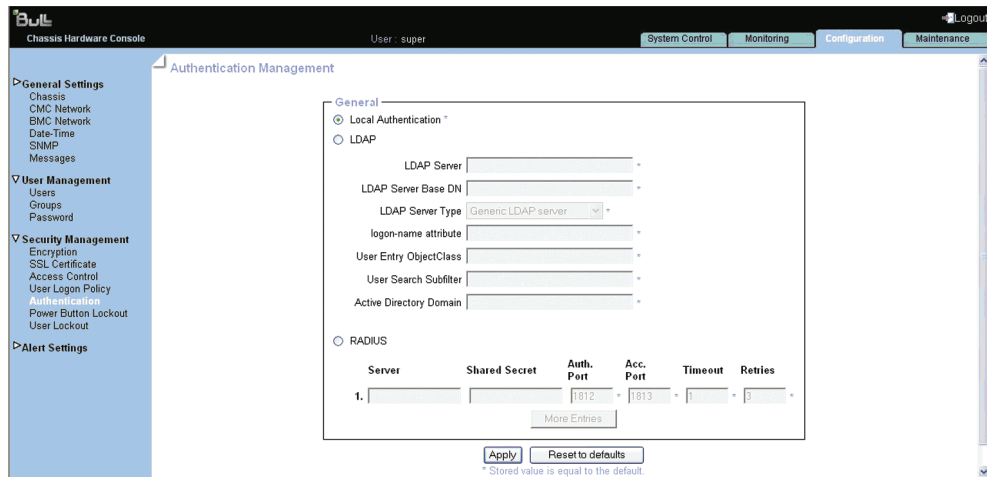


Figure 5-30. Authentication Management page

- Depending on your needs, click **Local Authentication**, **LDAP** or **RADIUS** and 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.
Logon Name Attribute	If you have selected Novell Directory Service or Microsoft Active Directory, leave these fields blank to use the directory's default value. Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory. For example, cn. User Entry Object Class: Object class that identifies a user in the directory. For example, organizationalPerson.
User Entry Object Class	
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.
Retries	Number of retries if a request cannot be completed.
More entries	If you are using several RADIUS servers, click this button to add authentication configurations.

Table 5-9. Authentication Management page description

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

5.3.5 Enabling/Disabling power button

The bullx 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. From the **Configuration** tab, expand **Security Management**, and click **Power Button Lockout** to open the Power Button Lockout Management page.

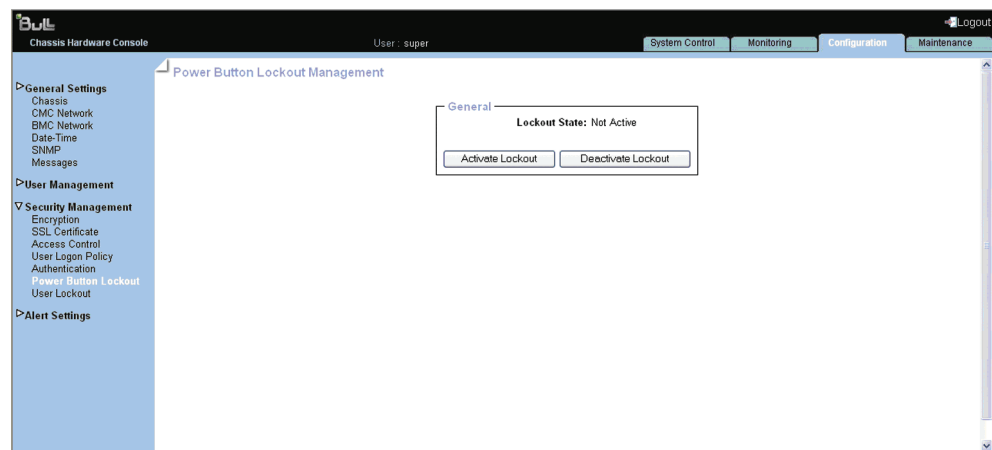


Figure 5-31. Power Button Lockout Management page

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

General	
Activate Lockout	The power button is locked on the LCP.
Deactivate Lockout	The power button is unlocked on the LCP.

Table 5-10. Power Button lockout Management page description

5.3.6 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. From the **Configuration** tab, expand **Security Management**, and click **User Lockout** to display the User Lockout Management page.

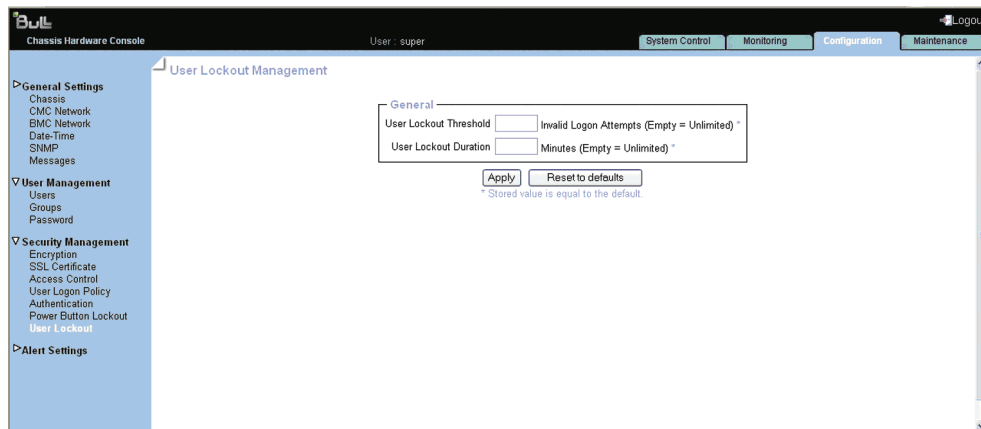


Figure 5-32. User Lockout Management page

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

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.

Table 5-11. User Lockout Management page description

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

5.4 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.

5.4.1 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. From the **Configuration** tab, expand **Alert Settings**, and click **Filters** to display the Filter settings page.

The screenshot displays the 'Filter settings' page in the BMC Chassis Hardware Console. The interface includes a top navigation bar with 'System Control', 'Monitoring', 'Configuration', and 'Maintenance' tabs. A left sidebar lists various configuration categories, with 'Alert Settings' expanded to show 'Filters'. The main content area contains a table with 32 rows of filter configurations. All filters are currently 'Disabled' and 'Configurable'. The table columns are: Index, Status, Filter Type, Action, Policy Set, Severity, Generator ID, Sensor Type, Sensor No., Trigger, Offset Mask, Data 1, Data 2, Data 3, and a 'Modify' link for each row.

Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID	Sensor Type	Sensor No.	Trigger	Offset Mask	Data 1	Data 2	Data 3	
1	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
2	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
3	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
4	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
5	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
6	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
7	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
8	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
9	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
10	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
11	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
12	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
13	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
14	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
15	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
16	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
17	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
18	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
19	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
20	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
21	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
22	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
23	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
24	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
25	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
26	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
27	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
28	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
29	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
30	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
31	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]
32	Disabled	Configurable		0	Unspecified	00 00	00	00	00	00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	[Modify]

Figure 5-33. Filters settings page

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



Figure 5-34. Filter modification page

Filter Modification	
Filter No.	Filter number (read-only field).
Status	Two possible values: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.

Filter Modification	
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 5-12. Configurable filter modification page description

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

5.4.2 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. From the **Configuration** tab, expand **Alert Settings**, and click **Policies** to display the Policy Settings page.

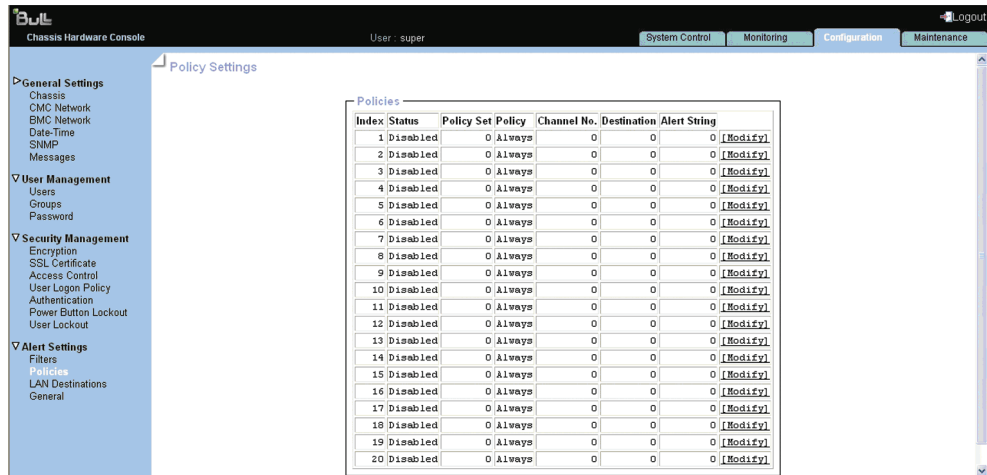


Figure 5-35. Policy Settings page

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

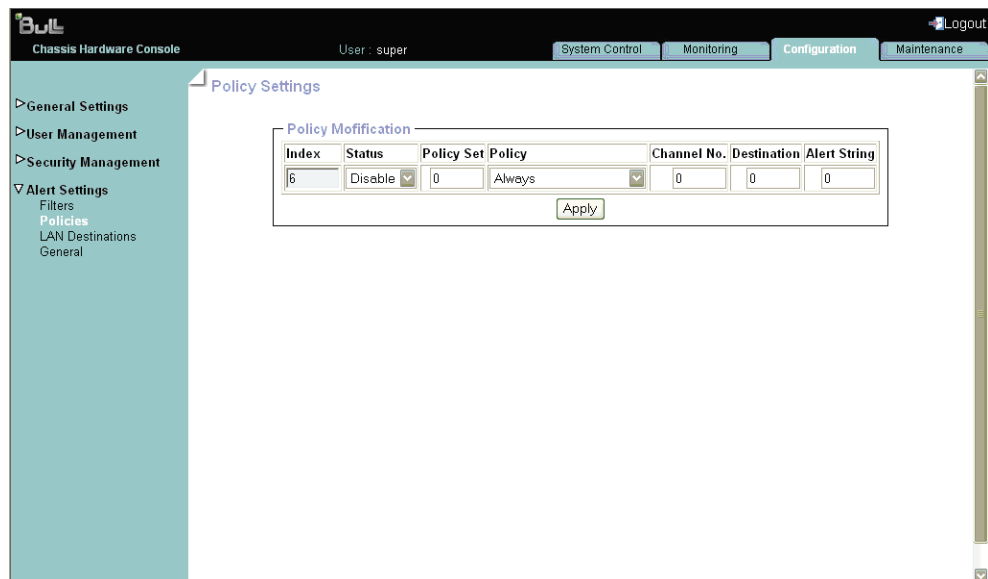


Figure 5-36. Policy Modification page

Policy Modification	
Index	Read-only.
Status	Two possible values: <ul style="list-style-type: none"> • 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	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: <ul style="list-style-type: none"> • 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 transmission 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 5-13. Policy Modification page description

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

-
- 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 in the list.
-

- When several enabled event filters match the event, the filter with the lowest policy set number is selected to transmit the alert
- When several enabled event filters match the event in the selected policy set, the filter with the highest severity is selected to transmit the alert
- When several enabled filters match the event in the selected policy set and they all have the same severity, the filter with the lowest index is selected to transmit the alert

5.4.3 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. From the **Configuration** tab, expand **Alert Settings**, and click **LAN Destinations** to display the LAN Destination Settings page.

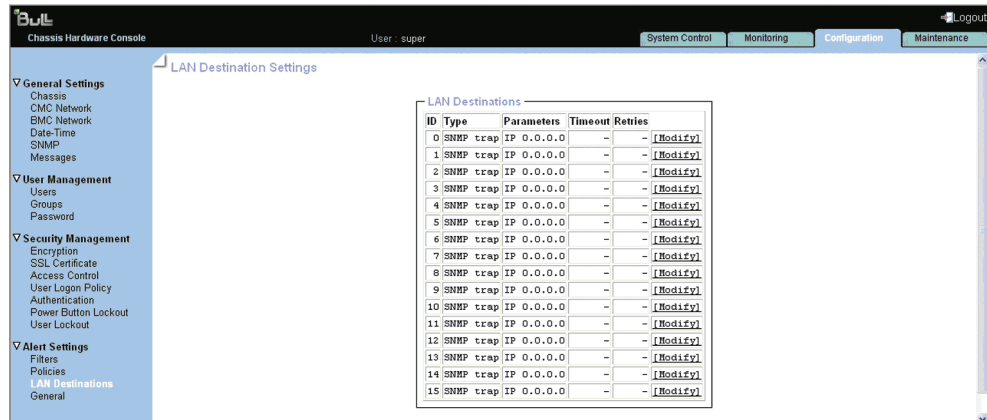


Figure 5-37. LAN destination settings page

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: <ul style="list-style-type: none"> • 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 5-14. Alert Settings: LAN Destination Edit page description

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

5.4.4 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. From the **Configuration** tab, expand **Alert Settings**, and click **General** to display the General Settings page.

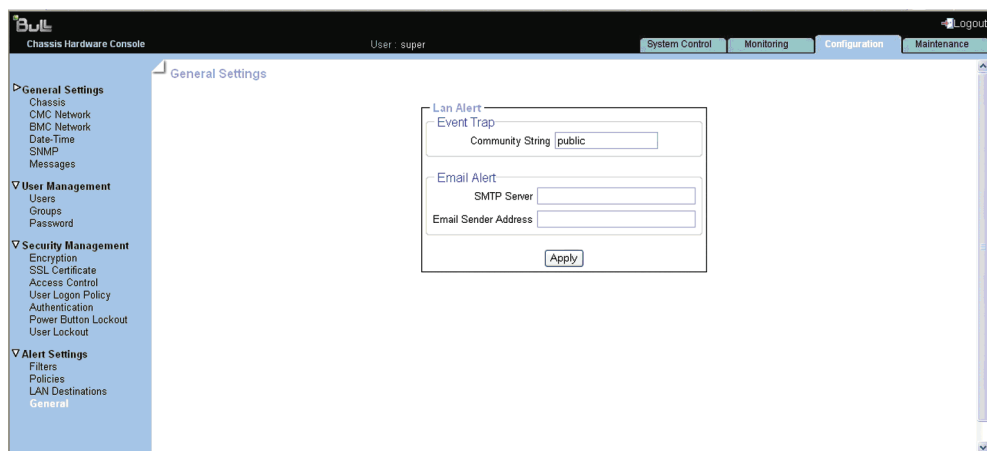


Figure 5-39. General Settings page

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.

Table 5-15. General Settings page description

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 console. The maintenance section contains the following topics:

- Hardware Information
 - Embedded Management Board
 - FRU
 - Firmware Version
 - Drawer
- Firmware Update
 - CMC
- Maintenance operation
 - Unit reset
 - Hardware Exclusion
 - Identification LED
 - Server blade change
 - CMM change
 - ESM change
 - IBSW change
 - LCP change
 - Power Management
 - Connected users

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. From the **Maintenance** tab, expand **Hardware Information**, and click **Management Board** to display the Management Board Information page.

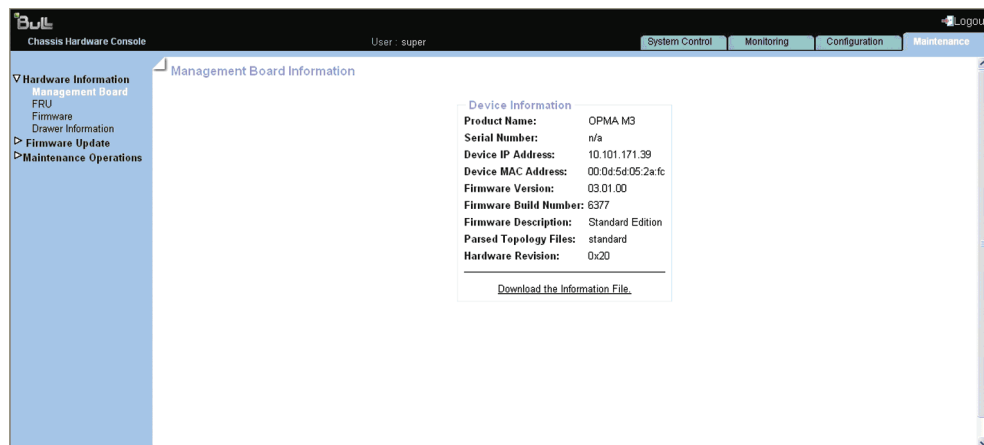


Figure 6-1. Management Board Information page

3. 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.

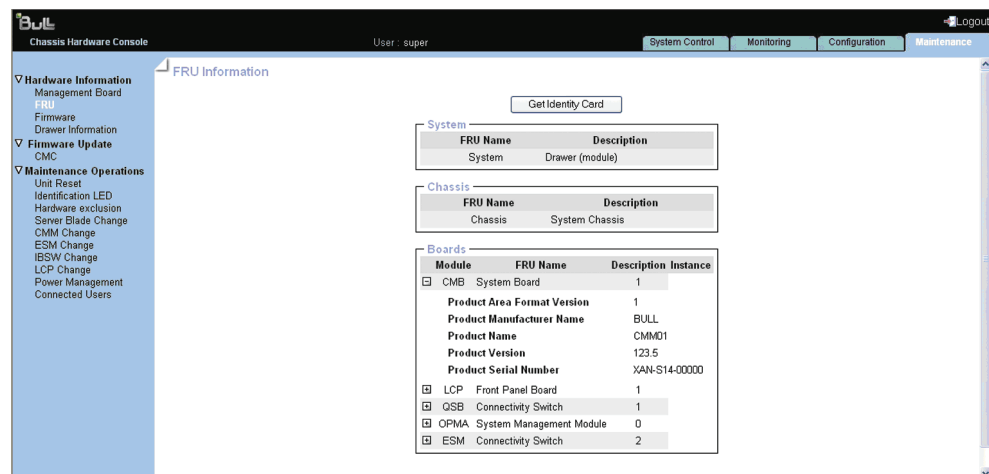
Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Hardware Information**, and click **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.



The screenshot shows the 'FRU Information' page in the 'Chassis Hardware Console'. The interface includes a top navigation bar with tabs for 'System Control', 'Monitoring', 'Configuration', and 'Maintenance'. A left-hand navigation menu is expanded to show 'FRU' under 'Hardware Information'. The main content area is titled 'FRU Information' and features a 'Get Identity Card' button. Below this, there are three sections: 'System', 'Chassis', and 'Boards'. Each section contains a table of FRU information.

FRU Name	Description
System	Drawer (module)

FRU Name	Description
Chassis	System Chassis

Module	FRU Name	Description	Instance
<input type="checkbox"/>	CMB	System Board	1
Product Area Format Version 1			
Product Manufacturer Name BULL			
Product Name CMM01			
Product Version 123.5			
Product Serial Number XAN-S14-00000			
<input type="checkbox"/>	LCP	Front Panel Board	1
<input type="checkbox"/>	QSB	Connectivity Switch	1
<input type="checkbox"/>	OPMA	System Management Module	0
<input type="checkbox"/>	ESM	Connectivity Switch	2

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

From the **Maintenance** tab, expand **Hardware Information**, and click **Firmware** to display the Firmware Information page.

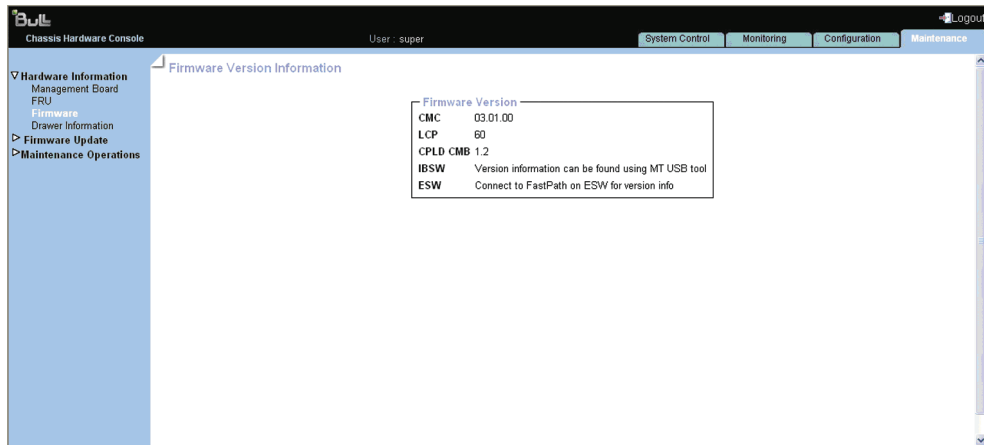


Figure 6-3. Firmware Version Information page

6.4 Viewing drawer information

This section provides information for the following components:

- Server Blade
- LCP
- IB Switch (QSM)
- UCM
- ESM

Procedure

From the **Maintenance** tab, expand **Hardware Information**, and click **Drawer Information** to display the Drawer Information page.

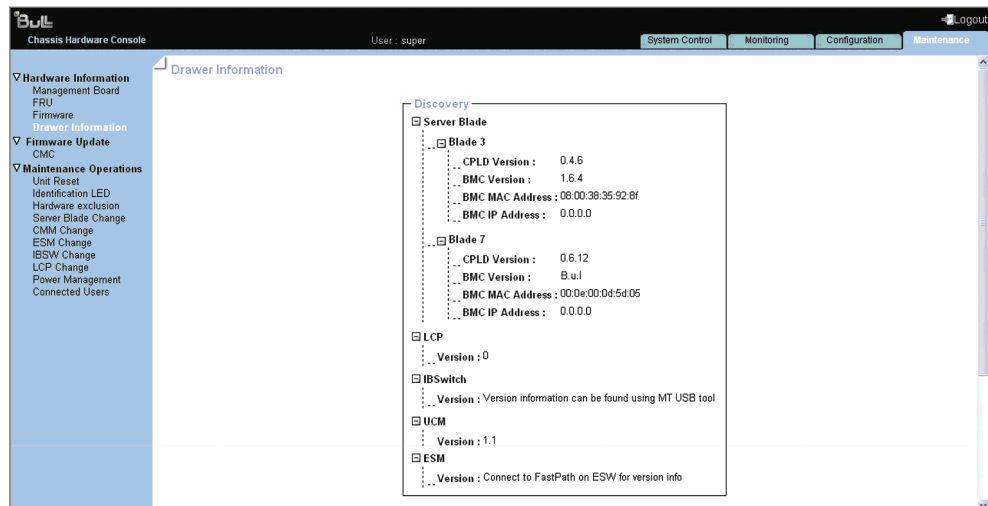


Figure 6-4. Drawer Information page

6.5 Upgrading Firmware

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Firmware Update** and click **CMC** to display the Firmware Upload page.

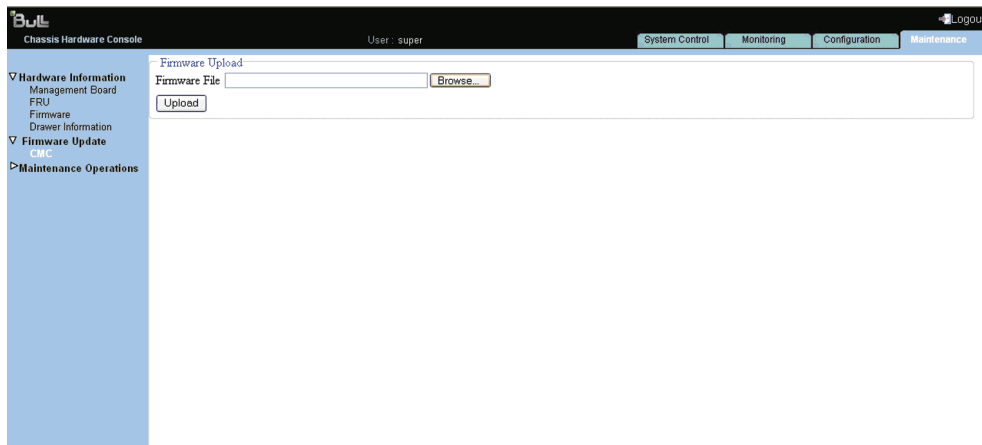


Figure 6-5. Firmware Upload page

2. Click **Browse** to get the new version of the firmware file supplied by Bull (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:

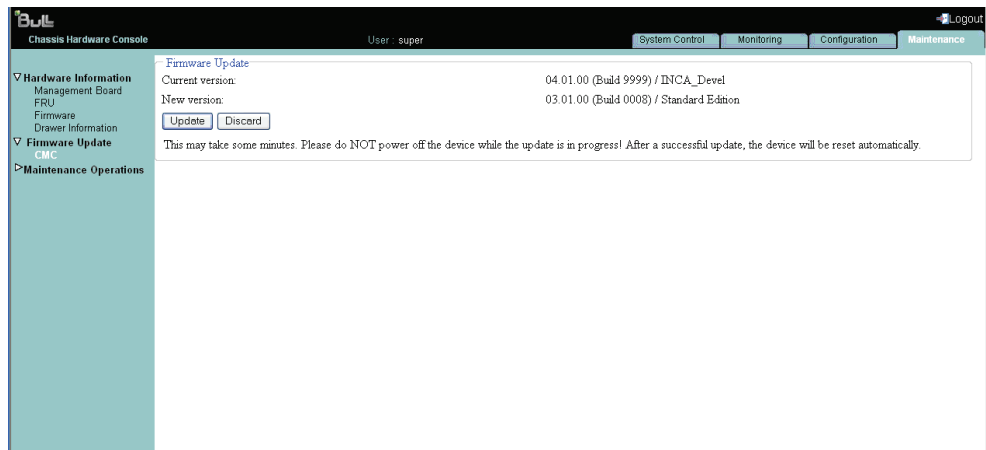


Figure 6-6. Firmware Upload page_Step2

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. From the **Maintenance** tab, expand **Maintenance Operation**, and click **Unit Reset** to display the Management Board Reset page.

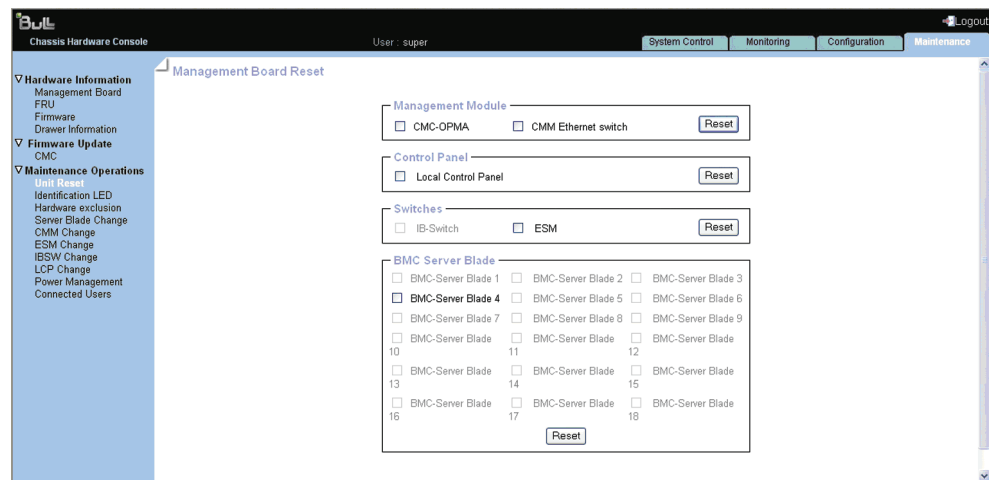


Figure 6-8. Management Board Reset page

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	bullx B500 compute blade numbers

Table 6-1. Management Board Reset page description

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. From the **Maintenance** tab, expand **Maintenance Operations**, and click **Identification LED** to open the Identification LED Management page.

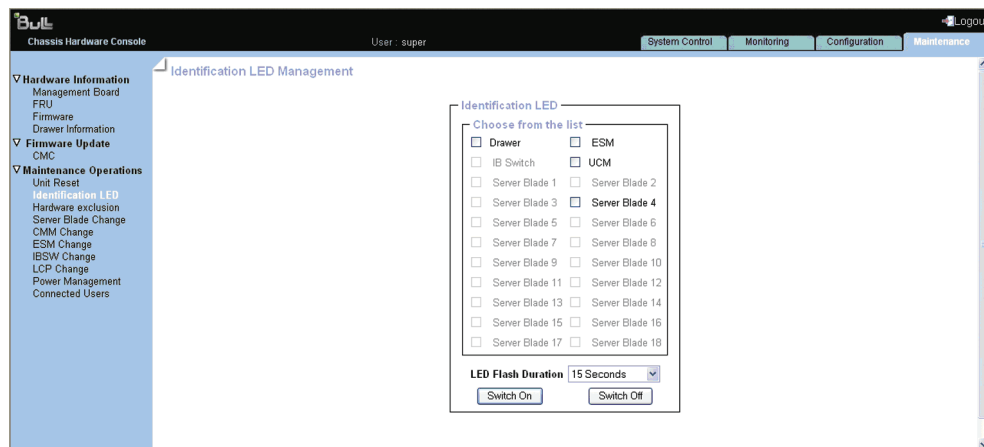


Figure 6-9. Identification LED Management page

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.

6.8 Excluding hardware

The console allows you to exclude bullx B500 compute blades in a static way. 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. From the **Maintenance** tab, expand **Maintenance Operations**, and click **Hardware Exclusion** to open the Hardware Exclusions management page.

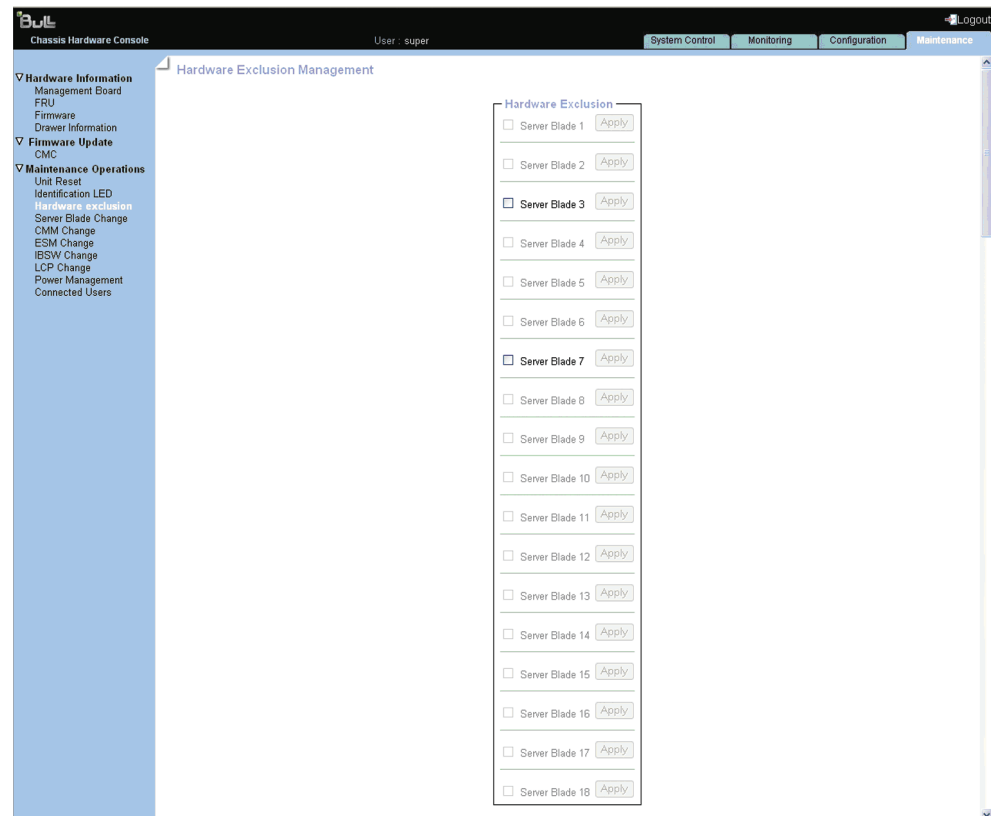


Figure 6-10. Hardware Exclusion Management page

2. Clear the check box(es) corresponding to the bullx B500 compute blade to exclude and click **Apply**.
3. Power on the system to apply the modification.

6.9 Managing bullx B500 compute blades

It allows removal/insertion of bullx B500 compute blades through the Chassis Hardware Console and it is required when servicing the bullx B500 compute blade.

See For information on serving the bullx B500 compute blade, see the section Servicing a bullx B500 compute blade in the *bullx blade system Maintenance and Troubleshooting Guide*.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operations**, and click **Server Blade Change** to open the Server blade Management page.

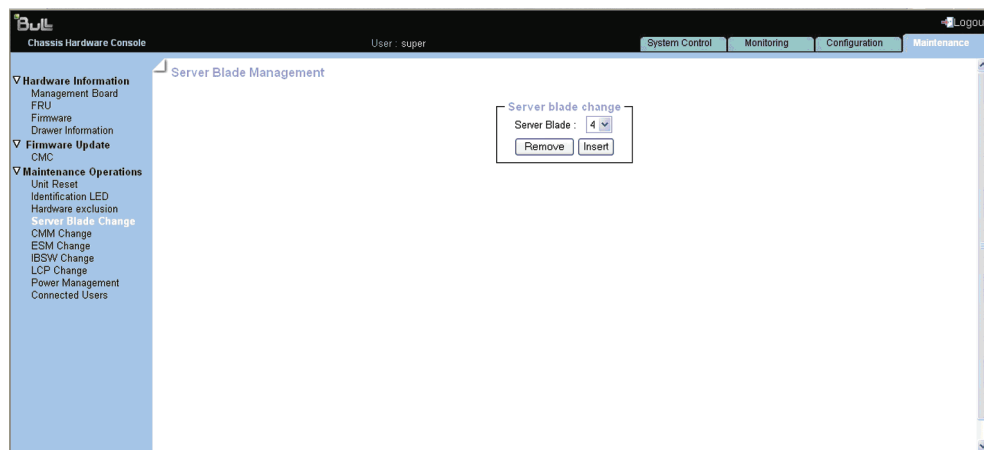


Figure 6-11. Sever Blade Management page

2. Select the **Server Blade** number from the drop-down.
3. Click **Remove/Insert** as required.

6.10 Managing the CMM

It allows removal/insertion of CMM through the Chassis Hardware Console and it is required when servicing the CMM.

See For information on servicing the CMM, see the section Servicing the Chassis Management Module in the *bullx blade system Maintenance and Troubleshooting Guide*.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operations**, and click **CMM Change** to open the CMM Management page.

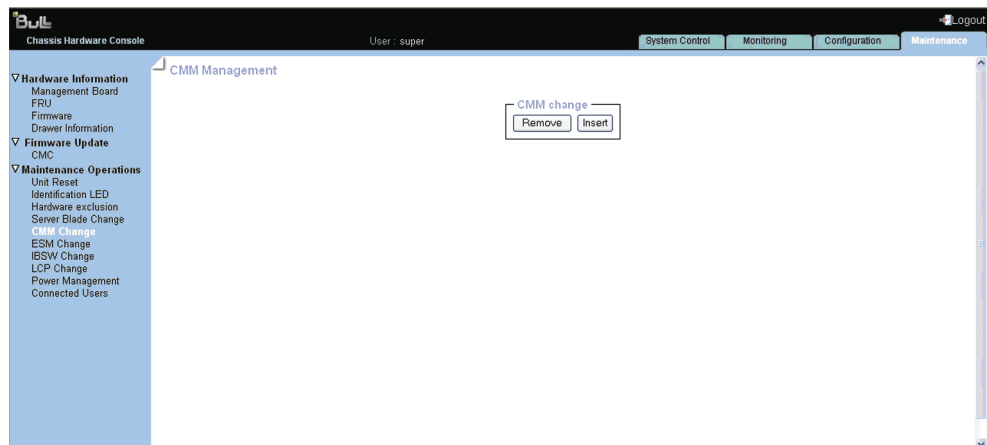


Figure 6-12. CMM Management page

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

6.11 Managing the ESM

It allows removal/insertion of ESM through the Chassis Hardware Console and it is required when servicing the ESM.

See For information on servicing the ESM, see the section Servicing the Ethernet Switch Module in the *bullx blade system Maintenance and Troubleshooting Guide*.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operations**, and click **ESM Change** to open the ESM Management page.

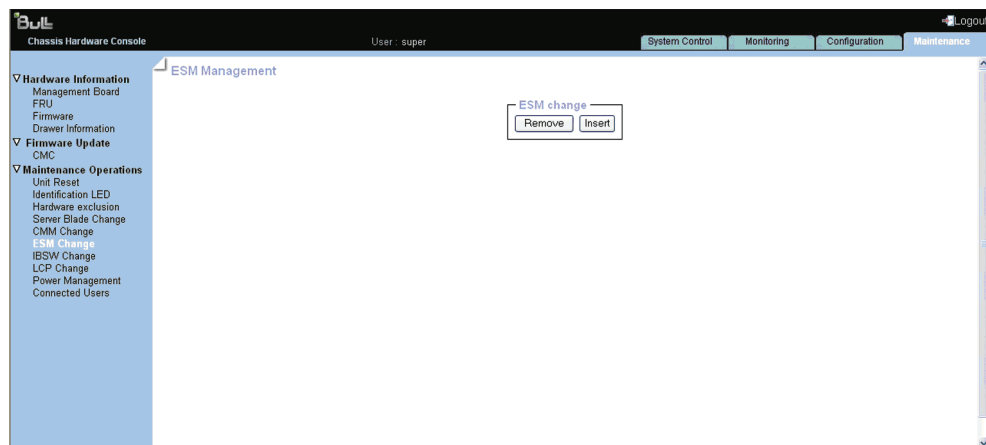


Figure 6-13. ESM Management page

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

6.12 Managing the Quad Switch Module

It allows removal/insertion of Quad Switch Module through the Chassis Hardware Console and it is required when servicing the Quad Switch Module.

See For information on servicing the Quad Switch Module, see the section Servicing Quad Switch Module in the *bullx blade system Maintenance and Troubleshooting Guide*.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operations**, and click **IBSW Change** to open the IBSW Management page.

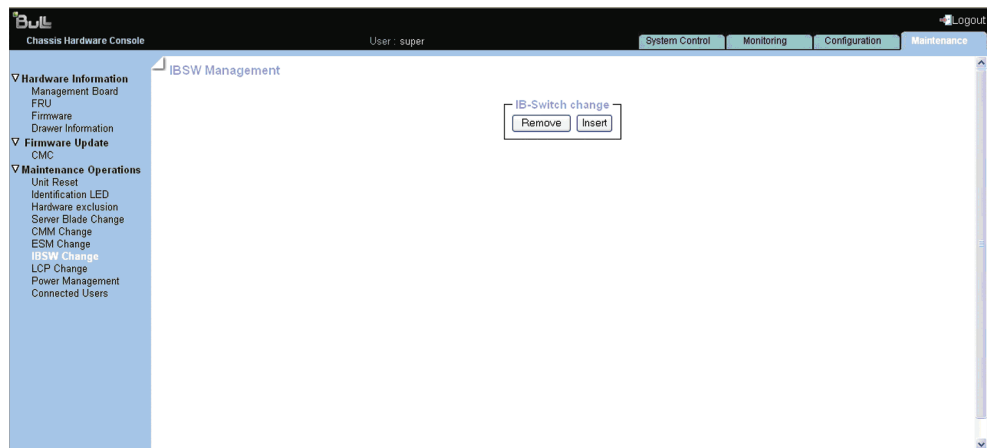


Figure 6-14. IBSW Management page

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

6.13 Managing the LCP

It allows removal/insertion of LCP through the Chassis Hardware Console and it is required when servicing the LCP.

See For information on servicing the LCP, see the section Servicing the Local Control Panel in the *bullx blade system Maintenance and Troubleshooting Guide*.

Prerequisites

- Viewing: All users
- Operations: Root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operation**, and click **LCP Change** to open the LCP Management page.

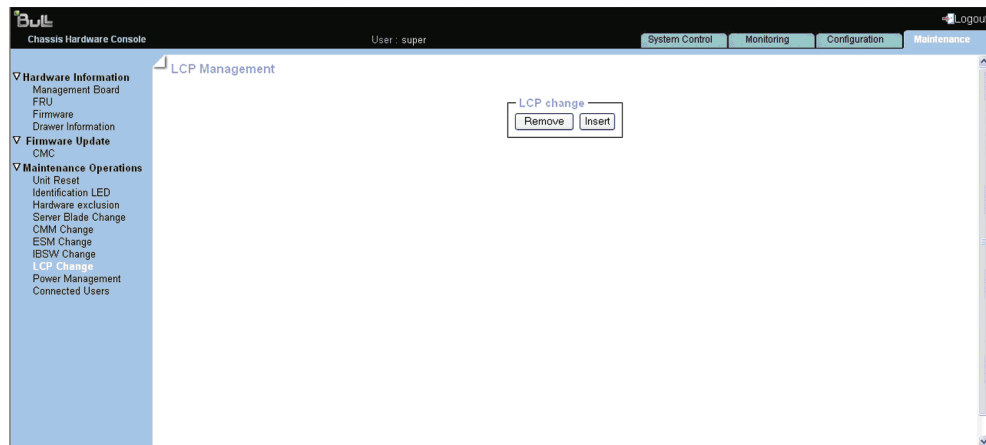


Figure 6-15. LCP Management page

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

6.14 Managing Power

It allows power management through the Chassis Hardware Console.

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. From the **Maintenance** tab, expand **Maintenance Operations**, and click **Power Management** to open the power management page.

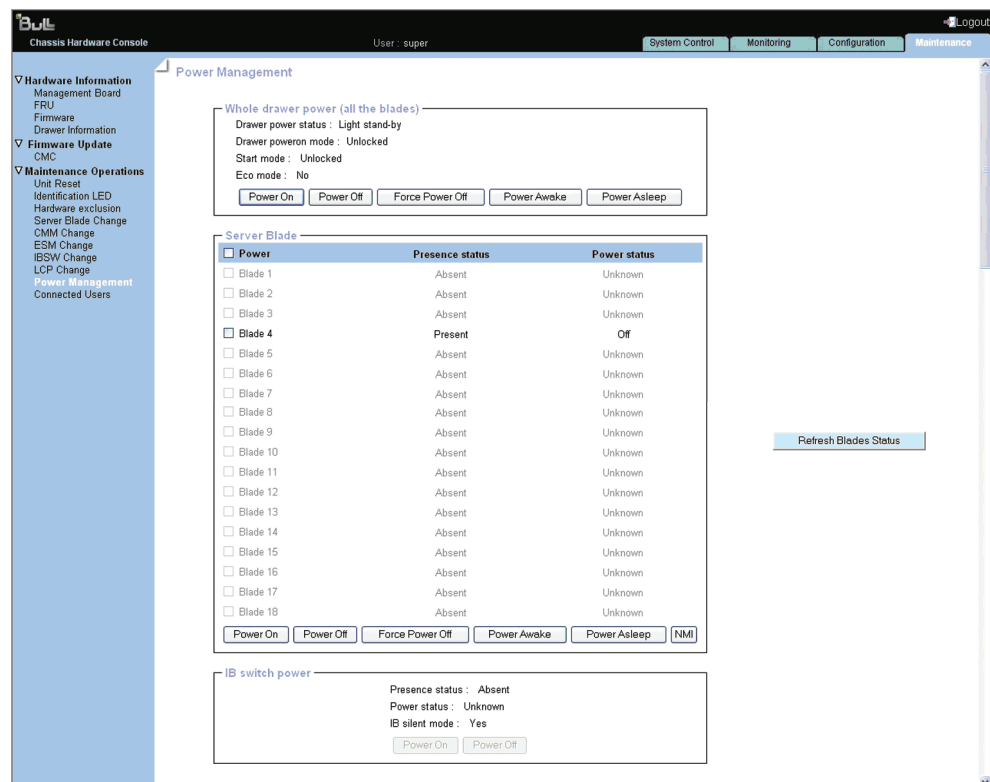


Figure 6-16. Power Management page

Whole drawer power	
Drawer power status	<p>Provides the status of drawer power.</p> <ul style="list-style-type: none"> • 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. • Main power: This state is the functional state of the drawer
Drawer power on mode	<p>Provides the status of drawer power on mode.</p> <ul style="list-style-type: none"> • 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	<p>Provides the status of start mode.</p> <ul style="list-style-type: none"> • Deep Stand-by: In this mode, the bullx B500 compute blade stays in stand-by off state (i.e. BMC not running) • Light Stand-by: In this mode, the bullx B500 compute blade state becomes stand-by on (i.e. the BMC will be running) • Unlocked Power: In this mode, the bullx B500 compute blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)
Eco mode	<p>Provides the status of Eco mode.</p> <ul style="list-style-type: none"> • Yes: This forces drawer to silent mode. (The drawer can be configured to save the energy when the bullx B500 compute 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	bullx B500 compute blade number.
Presence status	<ul style="list-style-type: none"> • Present: The corresponding bullx B500 compute blade is present • Absent: Server corresponding bullx B500 compute blade is absent
Power status	<ul style="list-style-type: none"> • Off: The corresponding bullx B500 compute blade is powered Off • On: The corresponding bullx B500 compute blade is powered On • Unknown: The corresponding bullx B500 compute blade is absent

IB switch power	
Presence status	Provides the presence of Quad Switch Module. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Yes: The IB switch silent mode is set to silent • No: The IB switch can be explicitly powered on/off.

Table 6-2. Power Management page description

2. Click the buttons as required.

You can refresh status of bullx B500 compute blade by clicking **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

From the **Maintenance** tab, expand **Maintenance Operations**, and click **Connected Users** to display the Connected Users Information page.

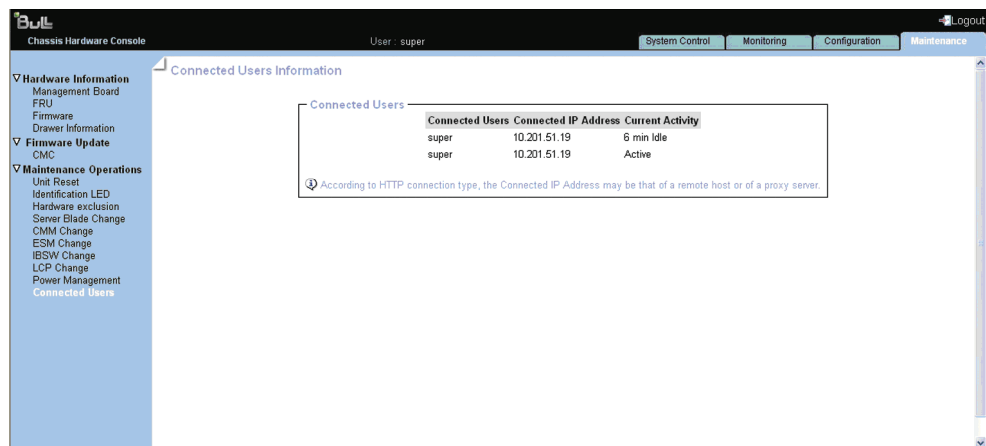


Figure 6-17. Connected Users Information page

Appendix A. bullx blade system specifications

bullx blade system is delivered rack-mounted in 42U cabinet.

You may consult the following web site for general site preparation information:

<http://www.cs.bull.net/aise>.

Cabinet Dimensions /Weight	
Unpacked	Unpacked
Height: 30.7 cm (12 in) Width: 44.6 cm (17.55 in) Depth: 74.7 cm (29.4 in) Weight (max): 125 kg (275 lb) (Approximate with UCM)	Height: 62 cm (24.4 in) Width: 60 cm (23.62 in) Depth: 90 cm (35.43 in) Weight (max): 155 kg (341 lb) (Approximate with UCM)
Service Clearance	
Front	150 cm
Rear	100 cm
Side (free side)	100 cm
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)
Max. wet bulb temperature	+16 °C (60.8 °F)
Moisture content	0.019 kg water/kg dry air
Pressure / Elevation	Sea level < 2500 m
Optimum Operational Reliability	
Temperature	+ 10 °C to 35 °C (50 °F to 95 °F) Gradient 5° /h
Hygrometry	50% (+ 5%)
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 %)
Max. 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° /h
Relative humidity (non-condensing)	5 to 95 % Gradient 30 % / h

Acoustic Power at Room Temperature +20°C (+68°F)	
System Running	System Idle
85 dBA	82 dBA
Power Cable	
Three pin, 250 V AC, 16 A	
AC 16 A per PSU Cable type Connector type	4 per bullx blade system Normal power cables with 16 A rating IEC C19 outlet on PSU side and IEC C20 on the main side.
It is mandatory for power lines and terminal boxes to be located within the immediate vicinity of the system and to be easily accessible.	
Electrical Specifications	
Current draw Power consumption Thermal dissipation Input ratings	12.5 A 10000 VA (max power drawn from mains per bullx blade system) 8500 W (max power dissipated per bullx blade system) 210-240VAC, 50/60Hz
Europe	
Nominal voltage Voltage range Frequency	230VAC (Phase / Neutral) 210 to 240V AC 50Hz
United States of America	
Nominal voltage Voltage range Frequency	230 VAC (Phase / Neutral) 210 to 240 V AC 60 Hz 0.3%
Breaker Protection (Mains Power)	
PDU Maximum inrush current	16A per PSU 210A / per quarter period

Table A.1. bullx blade system specifications

Appendix B. Predefined alert filters description

This appendix lists predefined event filters. A set of 67 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.

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

The use and configuration of event filters is explained in the section 5.4.1 Configuring filters.

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	<ul style="list-style-type: none"> • 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.
71	PSU-X	<ul style="list-style-type: none"> PSU-1 Input Volt(0x47) PSU-2 Input Volt(0x48) 	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.

Sensor No.	Component	Source	Event/Description	Severity	Meaning
		<ul style="list-style-type: none"> PSU-3 Input Volt(0x49) PSU-4 Input Volt(0x4A) 	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	<ul style="list-style-type: none"> 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 bullx B500 compute blade
 - SYSPG (SYStem Power Good) means the 12V power is running in the bullx B500 compute blade
-

Appendix C. SEL messages description

This appendix contains additional information about messages that appear in the System Event Log. It includes the following topics:

- Local Control Panel SEL messages
- Chassis Management Module SEL messages
- Ethernet Switch Module SEL messages
- Quad Switch Module SEL messages
- Ultra Capacitor Module SEL messages
- Power Supply Unit module SEL messages
- Fan blade SEL messages
- bullx B500 compute blade SEL messages

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.

IBSW Presence (0x1D)

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 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.

Fan blade 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.

bullx B500 compute blade SEL messages

Blade1 Presence (0x0B)

Description	bullx B500 compute 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 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	bullx B500 compute blade 3 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 3.
Comments	This log corresponds to sensor number 13. For more information on filters, see Configuring filters.

Blade3 Presence (0x0D)

Description	bullx B500 compute blade 3 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	bullx B500 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	bullx B500 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	bullx B500 compute blade 5 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 5.
Comments	This log corresponds to sensor number 15. For more information on filters, see Configuring filters.

Blade5 Presence (0x0F)

Description	bullx B500 compute blade 5 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	bullx B500 compute blade 6 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 6.
Comments	This log corresponds to sensor number 16. For more information on filters, see Configuring filters.

Blade6 Presence (0x10)

Description	bullx B500 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	bullx B500 compute blade 7 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 7.
Comments	This log corresponds to sensor number 17. For more information on filters, see Configuring filters.

Blade7 Presence (0x11)

Description	bullx B500 compute blade 7 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	bullx B500 compute blade 8 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 8.
Comments	This log corresponds to sensor number 18. For more information on filters, see Configuring filters.

Blade8 Presence (0x12)

Description	bullx B500 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	bullx B500 compute blade 9 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 9.
Comments	This log corresponds to sensor number 19. For more information on filters, see Configuring filters.

Blade9 Presence (0x13)

Description	bullx B500 compute blade 9 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	bullx B500 compute blade 10 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 10.
Comments	This log corresponds to sensor number 20. For more information on filters, see Configuring filters.

Blade10 Presence (0x14)

Description	bullx B500 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	bullx B500 compute blade 11 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 11.
Comments	This log corresponds to sensor number 21. For more information on filters, see Configuring filters.

Blade11 Presence (0x15)

Description	bullx B500 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	bullx B500 compute blade 12 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 12.
Comments	This log corresponds to sensor number 22. For more information on filters, see Configuring filters.

Blade12 Presence (0x16)

Description	bullx B500 compute blade 12 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	bullx B500 compute blade 13 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 13.
Comments	This log corresponds to sensor number 23. For more information on filters, see Configuring filters.

Blade13 Presence (0x17)

Description	bullx B500 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	bullx B500 compute blade 14 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 14.
Comments	This log corresponds to sensor number 24. For more information on filters, see Configuring filters.

Blade14 Presence (0x18)

Description	bullx B500 compute blade 14 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	bullx B500 compute blade 15 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 15.
Comments	This log corresponds to sensor number 25. For more information on filters, see Configuring filters.

Blade15 Presence (0x19)

Description	bullx B500 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	bullx B500 compute blade 16 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 16.
Comments	This log corresponds to sensor number 26. For more information on filters, see Configuring filters.

Blade16 Presence (0x1A)

Description	bullx B500 compute blade 16 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	bullx B500 compute blade 17 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 17.
Comments	This log corresponds to sensor number 27. For more information on filters, see Configuring filters.

Blade17 Presence (0x1B)

Description	bullx B500 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	bullx B500 compute blade 18 is not present. Device removed/Device absent.
Severity	Information.
Direction	Assertion.
Action	Insert bullx B500 compute blade 18.
Comments	This log corresponds to sensor number 28. For more information on filters, see Configuring filters.

Blade18 Presence (0x1C)

Description	bullx B500 compute blade 18 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 bullx B500 compute blade
 - SYSPG (SYStem Power Good) means the 12V power is running in the bullx B500 compute blade
-

Appendix D. Error dictionary

This appendix lists errors for all the hardware components that may occur during the system operation. All the errors are based on event filters. The use and configuration of event filters is explained in the section 5.4.1 Configuring filters.

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

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.
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.

Component	Event/Description	Severity	Meaning	Corrective action
	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 is not present.	Insert the corresponding bull B500 compute 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 below lower critical threshold (going low).	Critical	PSU input voltage lesser than expected.	AC input supply may be improper, check the AC input.
	At or above upper critical threshold (going high).	Critical	PSU input voltage greater 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.

Table D-1. Error dictionary

Glossary

A

ABR: Automatic BIOS Recovery

This invention describes a recovery method for a computer system that has corrupted initialization, or boot code. This is done using checksum for detecting the corruption and a backup copy of the boot code for recovery.

AC: Alternate Current

Alternating Current generated by the power supply. See also DC.

ACPI: Advanced Configuration and Power Interface

Open industry specification co-developed by Hewlett-Packard, Intel, Microsoft, Phoenix, and Toshiba, ACPI establishes industry-standard interfaces enabling OS-directed configuration, power management, and thermal management of server platforms.

Address

A label, name or number that identifies a location in a computer memory.

Archive: (Archive file)

A file that is a copy of a history file. When a history file is archived, all messages are removed from the history file.

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

Backup

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

BHC: Blade Hardware Console

Web based GUI, used to control and monitor an individual bullx B500 compute blade in a bullx blade chassis.

BIOS: Basic Input Output System

A program stored in flash EPROM or ROM that controls the system startup process.

BIST: Built - In Self Test

It is a mechanism that permits a machine to test itself.

Blade fans

The two counter rotating fans that are mounted in each bullx B500 compute blade to cool the bullx B500 compute blade.

BMC: Baseboard Management Controller

It is an embedded microcontroller surrounded by memory, interfaces, and sensors.

BOOTP

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

Byte

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

C

CENELEC: Comité européen de normalisation en électronique et en électrotechnique

Certificate Authority

It is an entity that issues digital certificates for use by other parties.

CFR: Code of Federal Regulations

Channel

A channel is a series of related web pages that provide a range of information on a particular topic.

CHC: Chassis Hardware Controller

Webs based GUI, used to control and monitor the whole of the BULLX BLADE SYSTEM.

Chipset

The term chipset is commonly used to refer to a set of specialized chips on a computer's motherboard or an expansion card.

CISC: Complex Instruction-Set Computer

A computer instruction set architecture (ISA) in which each instruction can execute several low-level operations, such as a load from memory, an arithmetic operation, and a memory store, all in a single instruction. The term was retroactively coined in contrast to reduced instruction set computer (RISC).

CLP: Command Line Protocol

The command line protocol will specify 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 daughter card, M3-G4 from Raritan, based on OPMA.

CMM: Chassis Management Module

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

COM: Complementary Metal Oxide Semiconductor

It is a major class of integrated circuits. CMOS technology is used in microprocessors, microcontrollers, static RAM, and other digital logic circuits.

COM1 or COM2:

The name assigned to a serial port to set or change its address. See Serial Port.

CPU: Central Processing Unit

It is an electronic circuit that can execute computer programs.

CRU: Customer Replaceable Unit**CSR: Certificate Signing Request**

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

D**DC: Direct Current**

Direct Current generated by the power supply. See AC.

DDR3: Double Data Rate 3

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

Default Gateway

A Default Gateway is the node on the computer network that is chosen when the IP address does not belong to any other entities in the Routing Table.

Default setting

The factory setting that your server uses unless instructed otherwise.

Density

The capacity of information (bytes) that can be packaged into a storage device.

DES: Data Encryption Standard

A block cipher (a form of shared secret encryption) that is based on a symmetric-key algorithm that uses a 56-bit key.

DHCP: Dynamic Host Configuration Protocol

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

Disk Drive or HDD

A device that stores data on a hard or floppy disk. A floppy disk drive requires a floppy disk to be inserted. A hard disk drive has a permanently encased hard disk.

Diskless

Personal computer without disk drives, which employs network booting to load its operating system from a server.

DIMM: Dual In-line Memory Module

The smallest system memory component.

DIMM socket

The socket used in Bullx blade system is for 240-pin DDR-3 memory modules.

DN: Distinguished Name

A distinguished name (DN) is a LDAP entry that uniquely identifies and describes an entry in a directory (LDAP) server

DNS: Domain Name System

It's a hierarchical naming system for computers, services, or any resource participating in the Internet.

DOS: Disk Operating System

It is a shorthand term for several closely related operating systems.

DRAM: Dynamic Random Access Memory

It is the most common type of random access memory (RAM).

DP: Dual Processor

Systems in which the two processors can either be located on the same motherboard or on separate boards.

E

ECC: Error Correcting Code

An error-correcting code is an algorithm for expressing a sequence of numbers such that any errors which are introduced can be detected and corrected (within certain limitations) based on the remaining numbers.

EP: Efficient Performance

ESM: Ethernet Switch Module

The hardware is same as that of 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

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

F

Fan blade

Refers to the *bullx blade system* fan modules which are located at the front of the system, below the LCP.

FC-LGA: Flip-Chip Land Grid Array

Nehalem CPU socket connectors on the Blade Server

FCC: Federal Communications Commission

Firmware

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

FQDN: Fully Qualified Domain Name

A domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS).

FRU: Field Replaceable Unit

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

Full Duplex

A Full Duplex system provides for communication in both directions at a time.

G

GB: GigaByte

One GB equals to 1,073,741,824 bytes.

GT/s: Giga Transfer per second

One GT equals four Gbytes.

GUI: Graphical User Interface

GPU: Graphical Processing Unit

It is a specialized processor that offloads 3D graphics rendering from the microprocessor.

H

Half Duplex

A Half Duplex system provides for communication in both directions at a time.

HDD: Hard Disk Drive

A device that stores data on a hard or floppy disk. A hard disk drive has a permanently encased hard disk.

High Performance Computing cluster

A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer.

HOST name

It is a unique name by which a network-attached device (which could consist of a computer, file server, network storage device, fax machine, copier, cable modem, etc.) is known on a network.

Hot plugging

The operation of adding a component without disturbing the system activity.

Hot swapping

The 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.

HTML: Hyper Text Markup Language

It is the predominant markup language for web pages.

HTTP: Hyper Text Transfer protocol

In the World Wide Web, a protocol that facilitates the transfer of hyper text-based files between local and remote systems.

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

The InfiniBand™ Architecture (IBA) is an 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.

Quad Switch Module

This is same as QSM or Quad.

iBMC: Integrated Baseboard Management Controller

Specialized microcontroller that is integrated in the motherboard of a server. 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.

ID: Identification**IEC: International Electrotechnical Commission**

World's leading organization that prepares and publishes International Standards for all electrical, electronic and related technologies

ILB: I/O Legacy Board

Video, LAN, USB, etc...

INCA

INtegrated Cluster Architecture. It is a high-density server system.

bullx B500 compute blades

Refers to the bullx B500 compute blade or NCB.

bullx blade system

Refers to the overall system including the bullx blade chassis, bullx B500 compute blades, and Modules.

Input – Output

Refers to the communication between an information processing system (such as a computer), and the outside world – possibly a human, or another information processing system.

Intelligent Drive Electronics/Integrated Device Electronics

It is an interface for mass storage devices, in which the controller is integrated into the disk or CD-ROM drive.

Interconnect

It is a point-to-point processor interconnects developed by Intel to compete with Hyper Transport.

IP: Internet Protocol

A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.

IPMI: Intelligent Platform Management Interface

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

ISO: International Organization for Standardization

World's largest developer and publisher of International Standards.

J**JTAG: Joint Test Action Group**

It is the 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**

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

L**LAN: Local Area Network**

A group of computers linked together within a limited area to exchange data.

LCD: Liquid Crystal Display

It is an electronically-modulated optical device shaped into a thin, flat panel made up of any number of color or monochrome pixels filled with liquid crystals and arrayed in front of a light source (backlight) or reflector.

LCP: Local Control Panel

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

LDAP: Lightweight Directory Access Protocol

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

LED: Light Emitting Diode

A small electronic device that glows when current flows through it.

M

MAC: Mandatory Access Control

A type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target.

Memory

Computer circuitry that stores data and programs.

Memory bandwidth

It is the rate at which data can be read from or stored into a semiconductor memory by a processor

MIB: Management Information Base

Type of database used to manage the devices in a communications network.

Microprocessor

An integrated circuit that processes data and controls basic computer functions.

Midplane

Midplane is a passive board that provides the physical and electrical connectivity to all the hardware modules.

MMX: MultiMedia eXtensions

A single instruction, multiple data (SIMD) instruction set designed by Intel, introduced in 1997

MTU: Maximum Transmission Unit

It is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet.

N

Nehalem CPU Board

This refers the bullx B500 compute blade or NCB.

Network interface

A point of interconnection between a user terminal and a private or public network.

NFS: Network File System

Protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed.

NTP server

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

NVRAM: Non-Volatile Random Access Memory

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

O

OPMA board

bullx blade system uses an OPMA based daughter card as the Chassis Management Controller or CMC. The CMC is a plugged into the CMM module.

OPMA: Open Platform Management Architecture

Is an open, royalty free standard for connecting a modular, platform hardware management subsystem (an "mCard") to a computer motherboard.

OS: Operating System

The software which manages computer resources and provides the operating environment for application programs.

Out-of-band compliant interface

It refers to communications which occur outside of a previously established communications method or channel.

P

Password

A security feature that prevents an unauthorized user from operating the system.

PCI - E slots

Slots for add in PCI-E cards. *bullx blade system* does not have any PCI-E slots.

PCI – Express

It is a serial transmission interface established by PCI-SIG. This can replace the conventional parallel PCI bus.

PCI - Express slots

Slots for add in PCI-E cards. *bullx blade system* does not have any PCI-E slots.

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)

Ping

A basic Internet program that lets you verify that a particular IP address exists and can accept requests. The verb 'to ping' means the act of using the ping utility command.

Power consumption

Energy consumption is the consumption of energy or power.

POST: Power On Self Test

When power is turned on, POST is the diagnostic testing sequence that a computer runs to determine if hardware is working properly.

Power redundancy

Preboot execution Environment

It is an environment to boot computers using a network interface independently of available data storage devices (like hard disks) or installed operating systems.

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 *bullx blade system*. It takes in the AC input voltages and converts them to the 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

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

Quad Data Rate

It is a communication signaling technique wherein 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

bullx 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.

RAS: Reliability Availability Serviceability

These factors help to ensure the integrity of the data stored on your bullx B500 compute blade; that your bullx B500 compute blade is available when you want to use it; and that should a failure occur; you can easily diagnose and repair the failure with minimal inconvenience.

RISC: Reduced Instruction-Set Computer

A CPU design strategy emphasizing the insight that simplified instructions that "do less" may still provide for higher performance if this simplicity can be utilized to make instructions execute very quickly.

RJ45

Eight-contact regular jack.

RoHS: Restriction of Certain Hazardous Substances

This Directive bans the placing on the EU market of new electrical and electronic equipment containing more than agreed levels of lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyl (PBB) and polybrominated diphenyl ether (PBDE) flame retardants.

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 of server (512 entries)

Serial Port

Connector that allows the transfer of data between the computer and a serial device. See COM1 or COM 2. Shell is a Unix term for the interactive user interface with an operating system.

bullx B500 compute blade

The blades that provides dual QDR InfiniBand (IB) channel to the InfiniBand Switch.

SIMD: Single Instruction, Multiple Data

Technique employed to achieve data level parallelism.

SKU: Stock Keeping Unit

It is a unique identifier for each distinct product and service that can be ordered from a supplier.

SMASH: System Management Architecture for Server Hardware

It is a suite of specifications that deliver industry standard protocols to increase productivity of the management of a data center.

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

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

SNMP: Simple Network Management Protocol

The protocol governing network management and the monitoring of network devices and their functions.

SO-DIMM: Small Outline Dual In-line Memory Module

Smaller alternative to a DIMM, being roughly half the size of regular DIMMs

SSD: Solid State Drive

It is a data storage device that uses solid-state memory to store persistent data.

SSH: Secured Shell

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

SSL: Secure Socket Layer

They are cryptographic protocols that provide security and data integrity for communications over networks such as the Internet

T**TELNET: Telecommunication network**

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive communications facility.

U**UCM: Ultra Capacitor Module**

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.

URL: Uniform Resource Locator

The address of a file (resource) accessible on the Internet.

USB: Universal Serial Bus

A plug-and-play interface between a computer and add-on device. The USB interface allows a new device to be added to your computer without having to add an adapter card or even having to turn the computer off.

UTC: Coordinated Universal Time

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

V**VLAN: Virtual Local Area Network**

A local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

VT-d: Virtualization for Directed I/O

The VT-d architecture enables system software to assign one or more I/O devices to a protection domain. DMA isolation is achieved by restricting access to a protection domain's physical memory from I/O devices not assigned to it, through address-translation tables.

VT-x: Virtualization Technology for x86

Method by which x86-based "guest" operating systems can run within another "host" x86 operating system, with little or no modification of the guest OS.

W**WOL: Wake-on LAN**

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

Web Service for Management

Is a general Web services protocol based on SOAP for managing systems such as PCs, servers, devices, Web services and other applications, and other manageable entities.

WEEE: Waste Electrical and Electronic Equipment

Loose category of surplus, obsolete, broken, or discarded electrical or electronic devices.

WS-MAN: Web Service Management

Public standard for remotely exchanging management data with any computer device that implements the protocol.

X

XML: eXtended MarkUp Language

General-purpose specification for creating custom markup language

Y

No entries.

Z

No entries.

Index

A

authentication, 90

B

BMC network, 61

bullx B500 compute blade information, 44

C

Chassis

interconnectivity, 10

Chassis Management Module, 3, 18

CMC network, 58

E

Ethernet Switch Module, 24

Identification LED, 25

LAN activity and status LED, 25

Power LED, 25

Expansion, 4

External port, 21

F

Fan blade, 14

filters, 95

Front view, 10

FRU, 107

Functionality, 4

G

Global power, 7

I

IB switch module policies, 45

L

LAN destinations, 101

LED

IB link activity LED, 21

Identification, 15

Power, 15

Local Control Panel, 15

lockout parameters, 94

M

management board, 113

Managing

bullx B500 compute blades, 116

CMM, 117

ESM, 118

LCP, 120

Power, 121

QSM, 119

message log, 68

N

Nehalem CPU blade, 3

O

OPMA service, 19

P

Power LED

bicolor, 21

power management, 36

Power Supply Unit, 17

PSU

hot swappable, 17

Q

Quad Switch Module, 3, 21

R

RJ45, 19

S

security management, 87

security messages, 56

sensor status, 52

Server blade, 10, 13
 Fault LED, 13
 HDD activity LED, 14
 IB activity LED, 13
 LAN 0 activity LED, 13
 LAN1 activity LED, 13
 Power LED, 13
 specific features, 12
SNMP command, 20
SNMP settings, 65

T

Turned On, 15

U

Ultra Capacitor Module, 22
 Charge LED, 23
 Fault LED, 23
 Identification LED, 22

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

REFERENCE
86 A1 50FB 02