bullx B5xx System

Chassis Hardware Console User's Guide

extreme computing

REFERENCE
86 A1 50FB 07

bullx B5xx System

Chassis Hardware Console User's Guide

Hardware

August 2011

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

REFERENCE
86 A1 50FB 07

Trademarks and Acknowledgements

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

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

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

Table of Contents

List of Figures

List of Tables

Legal Information

Regulatory Declarations and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with:

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

Safety Compliance Statement

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

European Community (EC) Council Directives

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

Electromagnetic Compatibility

- 2004/108/EC

Low Voltage

- 2006/95/EC

EC Conformity

- 93/68/EEC

Telecommunications Terminal Equipment

- 1999/5/EC

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

Compliance with these directives requires:

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

Mechanical Structures

- IEC 60297
- EIA-310-E

FCC Declaration of Conformity

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

Federal Communications Commission (FCC) Statement

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

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

Pursuant to Part 15.21 of the FCC Rules, any changes or modifications to this equipment not expressly approved by the manufacturer may cause harmful interference and void the FCC authorization to operate this equipment. An FCC regulatory label is affixed to the equipment.

Canadian Compliance Statement (Industry Canada)

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

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

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

- ICES-003
- NMB-003

VCCI Statement

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

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

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

Laser Compliance Notice (if applicable)

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

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

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

Safety Information

Definition of Safety Notices

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

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

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

Electrical Safety

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

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

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

Laser Safety Information (if applicable)

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

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

CAUTION

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

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

Data Integrity and Verification

WARNING

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

Waste Management

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

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

Safety Recommendations

Danger and Warning Notices

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

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

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

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

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

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

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

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

Important Notices

LABELING

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

HANDLING STATIC-SENSITIVE DEVICES

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

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

Preface

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

Notes

- In this guide, the Chassis Hardware Console is also referred to as Hardware Console.
- The Bull Support Web site may be consulted for product information, documentation, updates and service offers: http://support.bull.com

Intended Readers

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

Highlighting

The following highlighting conventions are used in this guide:

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

Related Publications

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

- *Site Preparation Guide,* 86 A1 40FA
  explains how to prepare a Data Processing Center for Bull Systems, in compliance with the standards in force. This guide is intended for use by all personnel and trade representatives involved in the site preparation process.
- *bullx B500 System Hardware Installation Guide*, 86 A1 48FB
  explains how to install and start the system for the first time. This guide is intended for use by qualified support personnel.
- *bullx B500 System Blade Hardware Console User's Guide*, 86 A1 49FB
  explains how to use the bullx B500 compute blades. This guide is intended for use by customer administrators and operators.
- *bullx B500 System Service Guide*, 86 A7 51FB
  explains how to service the system. This guide is intended for use by qualified support personnel.
- *bullx B505 System Hardware Installation Guide*, 86 A1 79FG
  explains how to install and start the system for the first time. This guide is intended for use by qualified support personnel.
- *bullx B505 System Blade Hardware Console User's Guide*, 86 A1 49FE
  explains how to use the bullx B505 accelerator blades. This guide is intended for use by customer administrators and operators.
- *bullx B505 System Service Guide*, 86 A7 80FG
  explains how to service the system. This guide is intended for use by qualified support personnel.
- *bullx B510 System Hardware Installation Guide*, 86 A1 81FG
  explains how to install and start the system for the first time. This guide is intended for use by qualified support personnel.
- *bullx B510 System Blade Hardware Console User's Guide*, 86 A1 49FG
  explains how to use the bullx B510 dual-nodes blades. This guide is intended for use by customer administrators and operators.
- *bullx B510 System Service Guide*, 86 A7 82FG
  explains how to service the system. This guide is intended for use by qualified support personnel.
- *Resource and Documentation CD*
  contains the tools and documentation required to configure, operate and maintain the equipment.

Chapter 1. Getting to Know the System

This chapter gives an overview of the blade system and its components. It includes the following topics:

1.1. System Overview

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

The bullx blade system is a high-density server system providing cluster architecture. It can be equipped with eighteen bullx B500 compute blades, nine bullx B505 accelerator blade or nine bullx B510 dual-node blades, making it ideally suited for extreme computing cluster environments requiring a large number of high-performance servers in a small space. The bullx blade chassis provides common resources that are shared by the blades, such as power, cooling, system management, network connections, and I/O switch. The use of common resources reduces blade size, minimizes cabling, and also reduces the time / likelihood of idle resources.

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

This guide provides information on how to:

- install the system
- connect and test the system

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

- Up to eighteen dual processor (DP) bullx B500 compute blades (NCB), with two processors, two fans for cooling, and an HDD/SSD disk.
- Up to nine bullx B505 accelerator blades (GPU), with two processors, two Nvidia cards and four fans for cooling.
- Up to nine bullx B510 dual-node blades (SCB) with two common fans, each node with two processors and an HDD/SSD disk.
- A Quad Switch Module (QSM).
- An optional Ultra Capacitor Module (UCM).
- A Chassis Management Module (CMM).
- An optional 1 Gigabit Ethernet Switch Module (ESM).
- An optional 10 Gigabit Ethernet Switch Module (TSM).
- A Local Control Panel (LCP) providing an LCD display and power and reset buttons.
- Up to four Power Supply Unit modules (PSU) providing N+1 power redundancy.
- Two fan blades to cool the QSM, CMM, and ESM / TSM modules.

Serial and part numbers are indicated on a label (A) on the top of the chassis. The following table can be used to record system information.

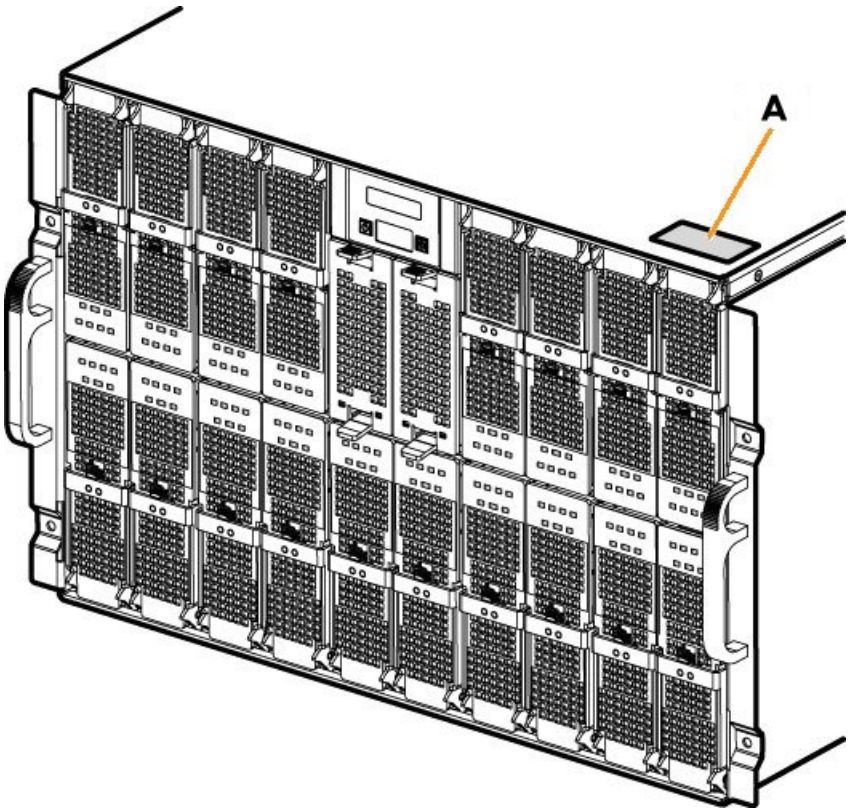


Figure 1-1. bullx information label

System	Data
Product Name	
Model Type	
Serial Number (XAN)	

Table 1-1. System product data

1.2. What the Blade System offers

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

Innovative technology

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

Expansion capabilities

Blades can be added to the blade system as needed. The system can be equipped with a maximum of eighteen compute blades / nine accelerator blades / nine dual-node blades. All these blades can be mixed in the same chassis.

Hot-swap / Hot-plug capabilities

The compute, accelerator and dual-node blades, the fan blades, the Chassis Management Module (CMM), the 1 Gigabit Ethernet Switch Module (ESM), the 10 Gigabit Ethernet Switch Module (TSM), the Quad Switch Module (QSM) the Local Control Panel (LCP) and the Power Supply Units (PSU) are hot-pluggable / hot-swappable for optimum uptime and easy maintenance.

Redundancy capabilities

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

Redundant network connection capabilities

The optional 1 Gigabit Ethernet Switch Module (ESM) / 10 Gigabit Ethernet Switch Module (TSM) provides a redundant Ethernet interface to the blades.

System management capabilities

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

Each blade is equipped with a service processor which provides blade system monitoring, event recording, and alert capabilities.

Network environment support

The blade system supports up to two Ethernet Switches, one in the Chassis Management Module (CMM) and the second in the 1 Gigabit Ethernet Switch Module (ESM) / 10 Gigabit Ethernet Switch Module (TSM). The Ethernet Switch Modules are used for blade communication with the network. The Chassis Management Module (CMM) and 1 Gigabit Ethernet Switch Module (ESM) / 10 Gigabit Ethernet Switch Module (TSM) provide internal connections to each blade.

1.3. Reliability, Availability, and Serviceability (RAS)

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

- Shared key components, such as power, cooling, and I/O
- All components serviced from the front or rear of the blade chassis
- Built-in monitoring for fan blade, power, temperature, and voltage
- Built-in monitoring for module redundancy
- Error codes and messages
- Fault-resistant startup
- Remote system management through the Chassis Management Module (CMM)
- Remote upgrade of Chassis Management Module (CMM) firmware
- Remote upgrade of blade service processor firmware
- Redundant components:
  - Fan blades
  - Power Supply Unit modules
- Hot-plug / hot-swap components:
  - Compute (NCB, accelerator (GPU) and/or dual-node (SCB) blades
  - Fan blades
  - Chassis Management Module (CMM)
  - 1 Gigabit Ethernet Switch Module (ESM) / 10 Gigabit Ethernet Switch Module (TSM)
  - Quad Switch Module (QSM)
  - Local Control Panel (LCP)
  - Power Supply Unit (PSU)
- Ultra Capacitor Module (UCM) (requires full system power down)

1.4. Features and Specifications

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

- AC power redundancy: N+1 (4 PSU modules redundant system, 3 PSU modules non-redundant system)
- Two fan blades cooling the QSM, CMM and ESM / TSM
- Rack-mountable system, using a standard cabinet

1.4.1. Chassis-level Platform Management

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

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

1.4.2. Blade-level Platform Management

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

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

1.4.3. External Connections, Interfaces, Indicators, Buttons and Switches

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

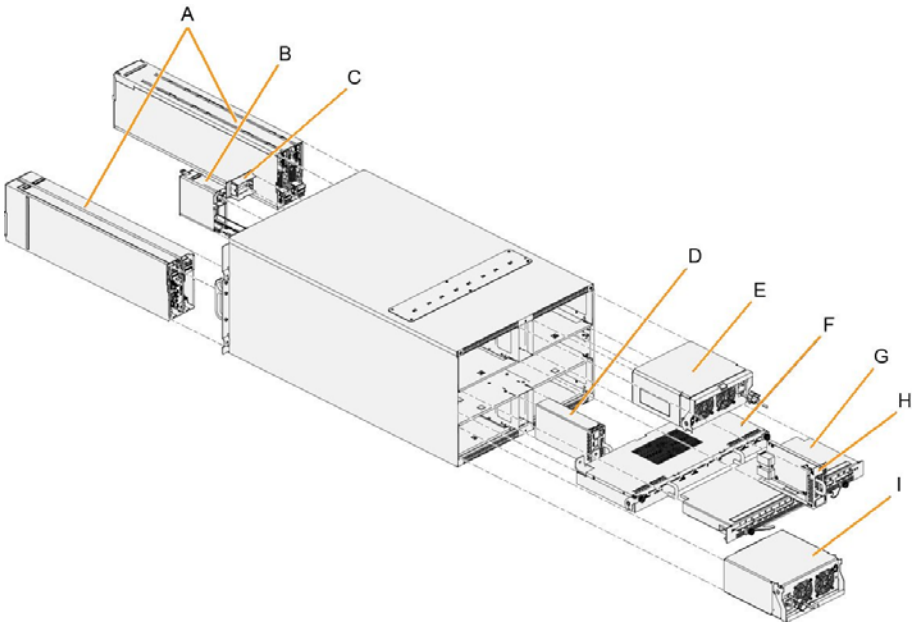
- Eighteen IB QDR connections (QSFP connector with power) on the Quad Switch Module
- Three1Gb Ethernet ports -RJ45 connectors and a serial COM port for maintenance on the ESM
- Four 10Gb Ethernet ports -SFP+ connectors, One 1Gb Ethernet port & a serial COM port for maintenance -Stacked Dual RJ45 connector on TSM.
- Three1Gb Ethernet ports -RJ45 connectors and a serial COM port for maintenance on the CMM
- Local Control Panel (LCP)
- Chassis power On/Off switch
- Chassis power indicator LED
- Chassis blue ID indicator LEDs – front LCP indicator LED, rear CMM indicator LED
- Blade indicator LEDs
- Quad Switch Module indicator LED
- Gbit Ethernet switch indicator LED
- Ultra Capacitor Module indicator LED
- CMM reset pushbutton (CMC reset)

1.5. Blade Drawer Components, Controls, LEDS and Ports

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

1.5.1. Components (Exploded view)

The following diagram shows an exploded view of blade system components:



Mark	Description
A	Blades
B	Fan blade
C	Local Control Panel (LCP)
D	Ethernet Switch Module (ESM/TSM)
E	Power Supply Unit (PSU) (x2)
F	Ultra Capacitor Module (UCM)
G	Quad Switch Module (QSM)
H	Chassis management Module (CMM)
I	Power Supply Unit (PSU) (x2)

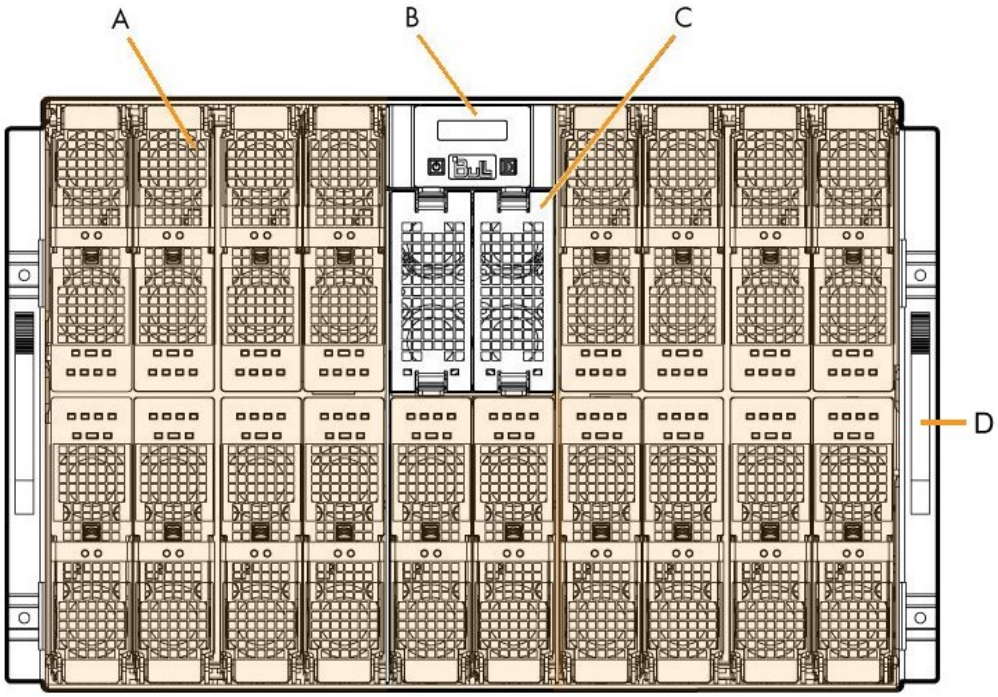
Figure 1-2. Blade drawer components - Exploded view

1.5.2. Blade front components

Blade Chassis

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

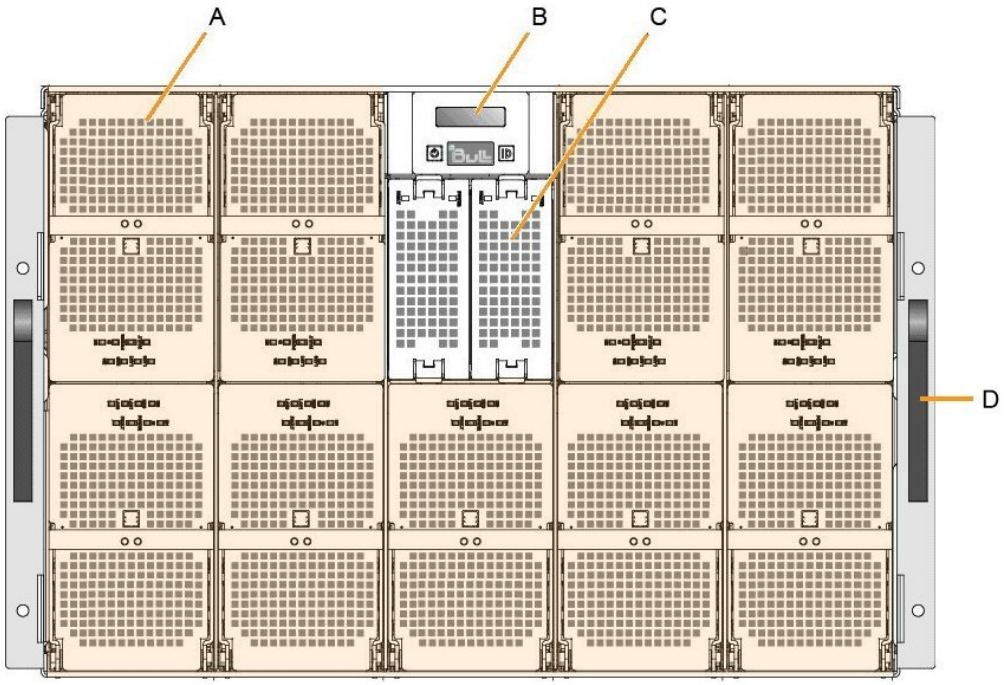
Blade system with compute blades (Front view)



Mark	Description
A	Compute blades (NCB) (x18)
B	Local Control Panel (LCP)
C	Fan blade (x2)
D	Handles (x2)

Figure 1-3. Blade system with compute blades - Front view

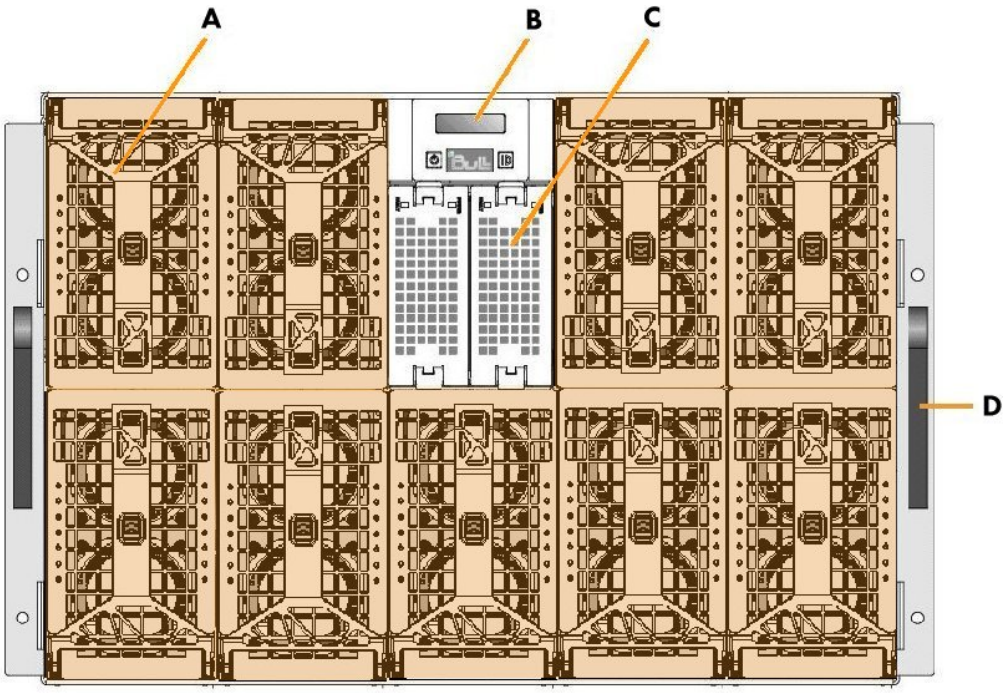
Blade system with accelerator blades (Front view)



Mark	Description
A	Accelerator blades (GPU) (x9)
B	Local Control Panel (LCP)
C	Fan blade (x2)
D	Handles (x2)

Figure 1-4. Blade system with accelerator blades - Front view

Blade system with dual-node blades (Front view)



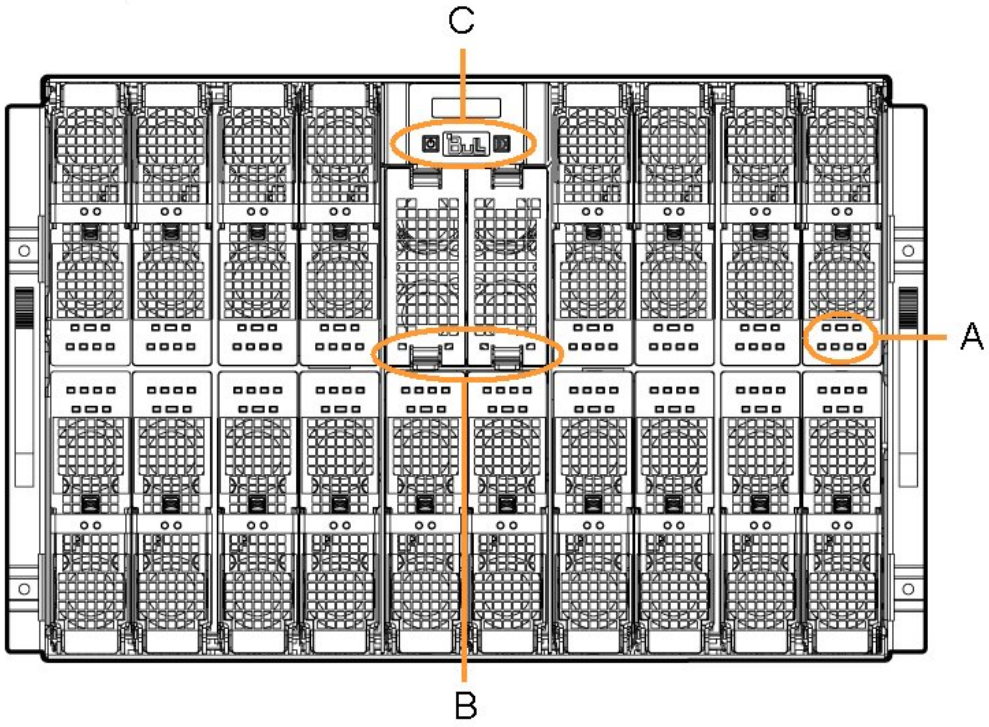
Mark	Description
A	Blades (SCB) (x9)
B	Local Control Panel (LCP)
C	Fan blade (x2)
D	Handles (x2)

Figure 1-5. Blade system with dual-node blades - Front view

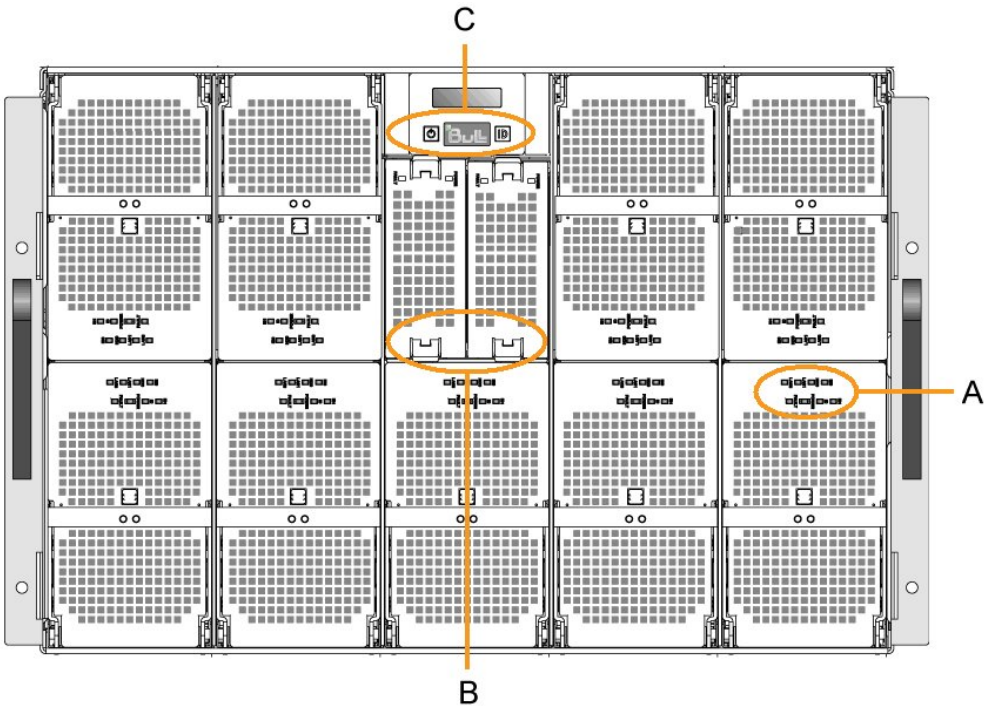
1.5.3. Controls and LEDs (Front view)

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

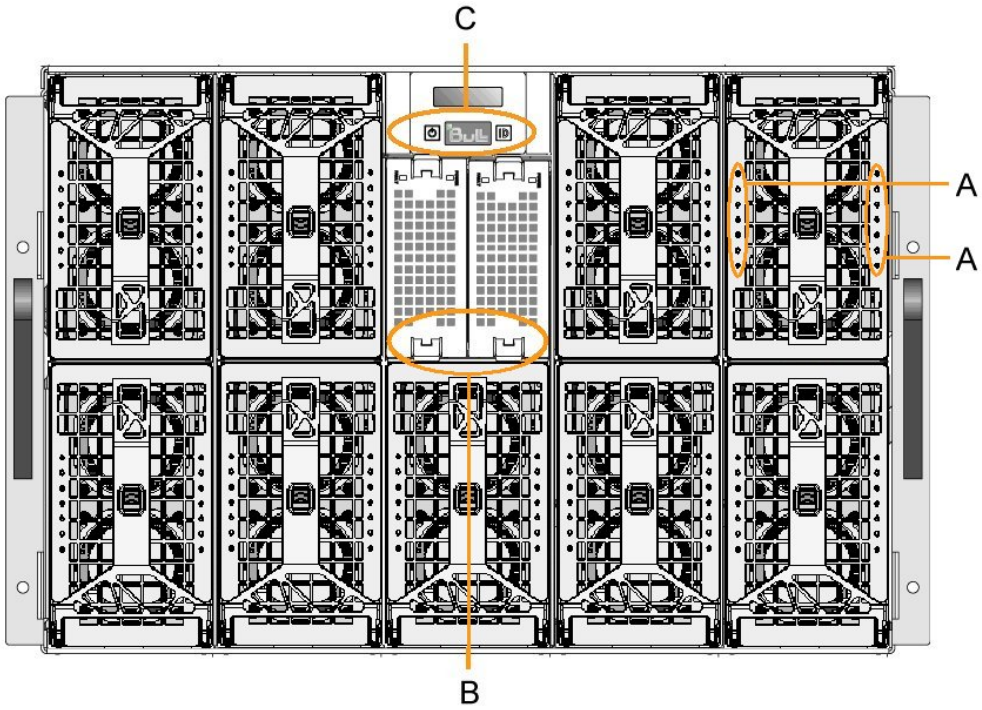
Drawer with compute blades (NCB)



Drawer with accelerator blades (GPU)



Drawer with dual-node blades (SCB)



Mark	Description
A	Blade LEDs
B	Fan LEDs
C	Power and ID LEDs and buttons

Figure 1-6. LEDs and buttons - Front view

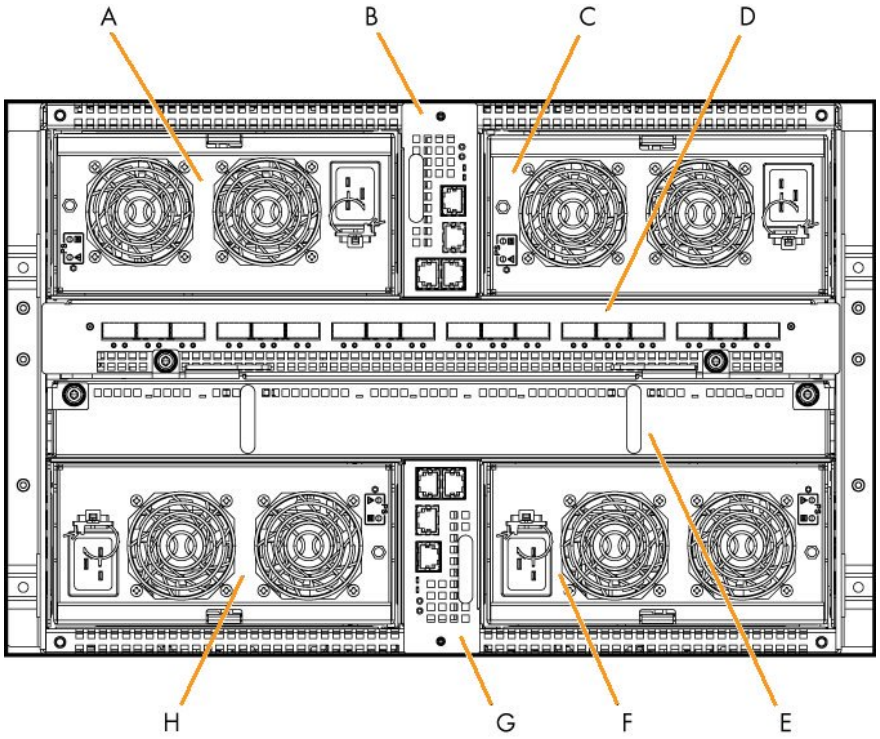
1.5.4. Blade rear components

Blade chassis

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

Blade drawer with ESM - Rear view

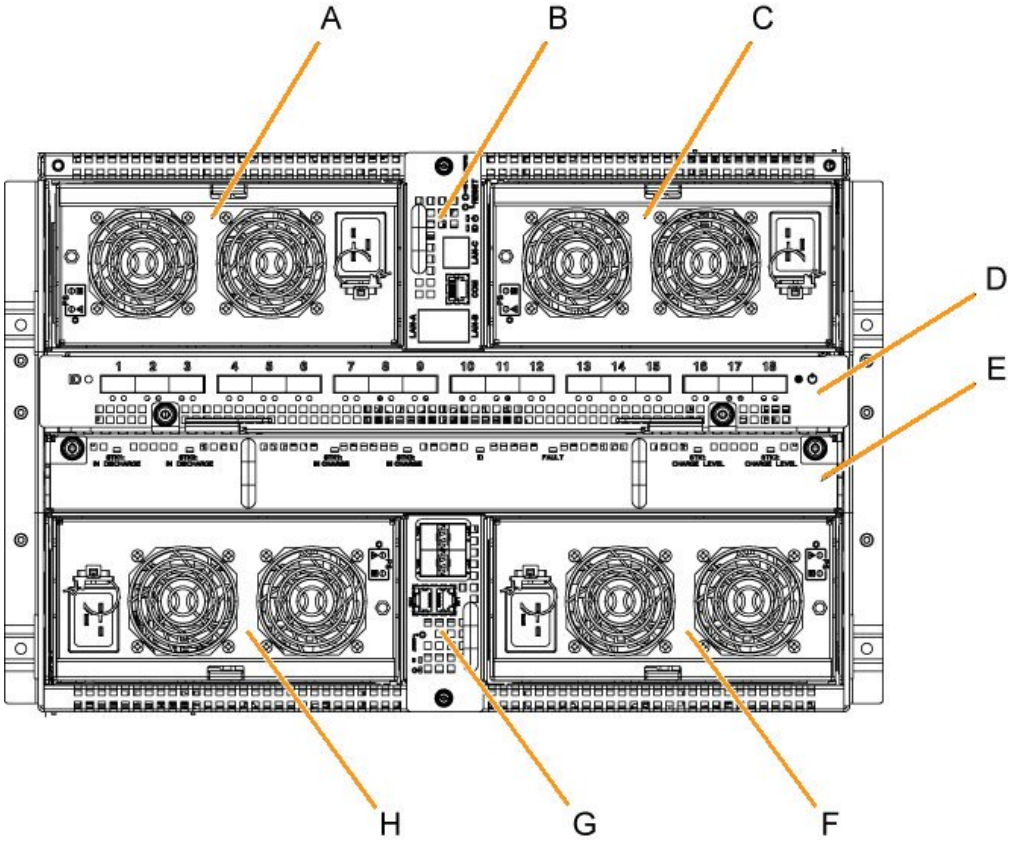
The rear of the blade drawer is equipped with four power supplies, a chassis management module, a Quad Switch Module, an Ultra Capacitor Module, and an Ethernet Module.



Mark	Description
A	Power Supply Unit (PSU) 3
B	Chassis Management Module (CMM)
C	Power Supply Unit (PSU) 4
D	Quad Switch Module (QSM)
E	Ultra Capacitor Module (UCM)
F	Power Supply Unit (PSU) 2
G	1 Gb Ethernet Switch Module (ESM)
H	Power Supply Unit (PSU) 1

Figure 1-7. Blade system with ESM - Rear view

Blade system with TSM - Rear view

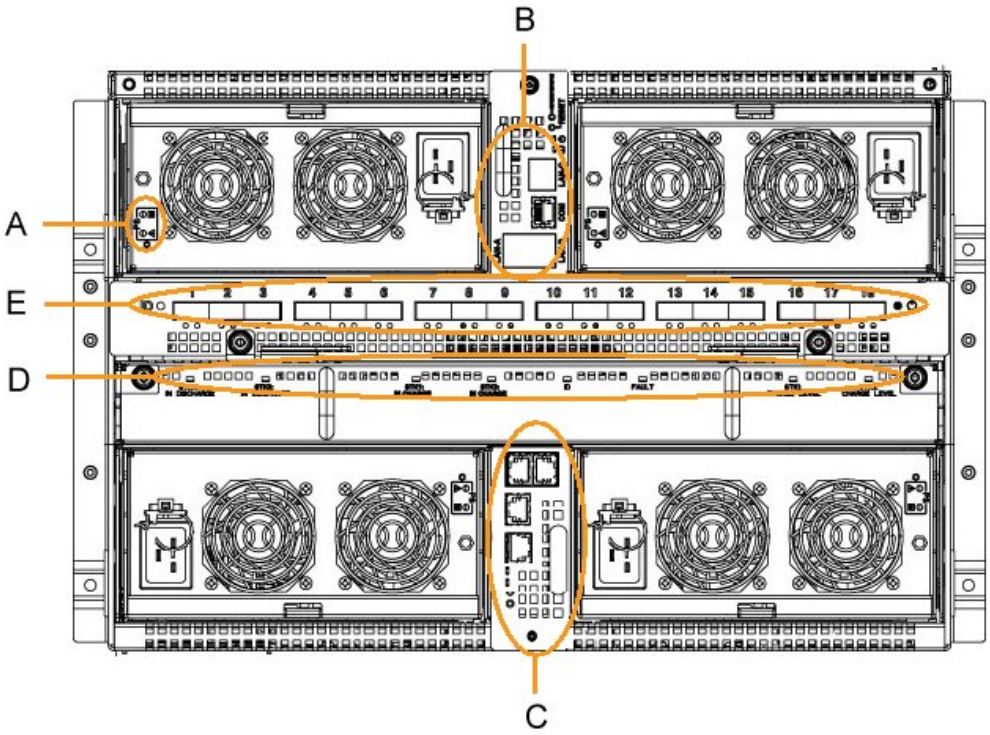


Mark	Description
A	Power Supply Unit (PSU) 3
B	Chassis Management Module (CMM)
C	Power Supply Unit (PSU) 4
D	Quad Switch Module (QSM)
E	Ultra Capacitor Module (UCM)
F	Power Supply Unit (PSU) 2
G	10 Gb Ethernet Switch Module (TSM)
H	Power Supply Unit (PSU) 1

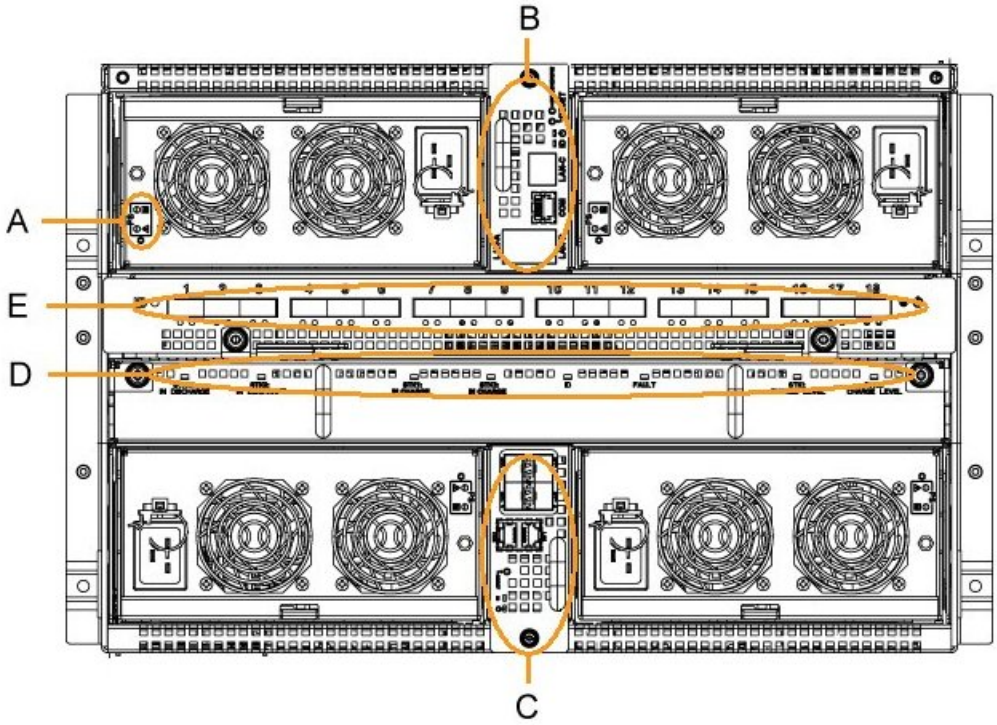
Figure 1-8. Blade system with TSM - Rear view

1.5.5. Controls and LEDs (Rear view)

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



Mark	Description
A	Power Supply Unit (PSU) LEDs
B	Chassis Management Module (CMM) LEDs and controls
C	1 Gb Ethernet Switch Module (ESM) LEDs and controls
D	Ultra Capacitor Module (UCM) LEDS
E	Quad Switch Module (QSM) LEDS

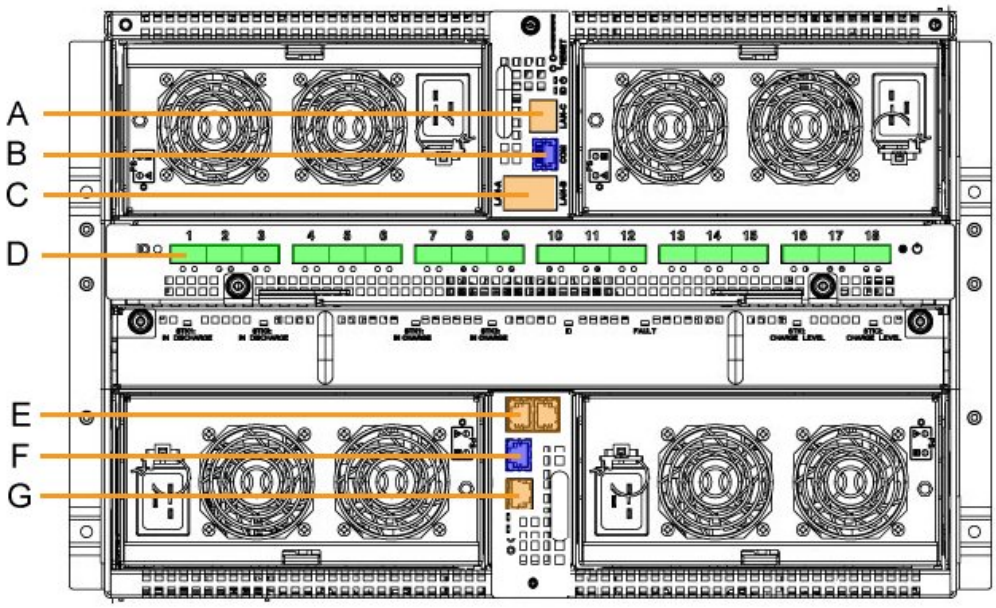


Mark	Description
A	Power Supply Unit (PSU) LEDs
B	Chassis Management Module (CMM) LEDs and controls
C	10 Gb Ethernet Switch Module (TSM) LEDs and controls
D	Ultra Capacitor Module (UCM) LEDS
E	Quad Switch Module (QSM) LEDS

Figure 1-9. Controls and LEDs - Rear view

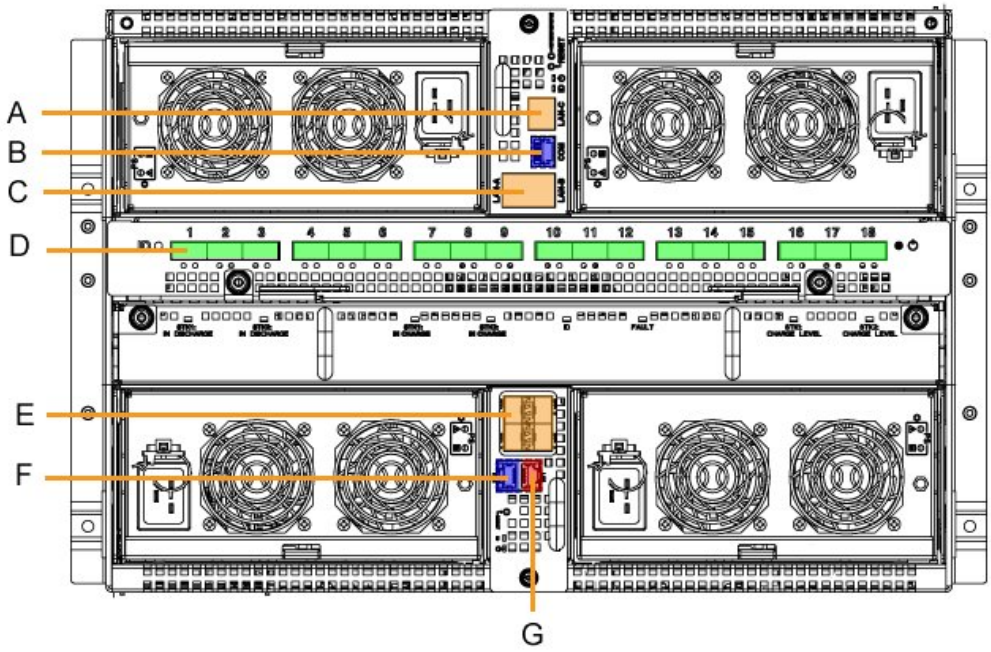
1.5.6. Connection Ports (Rear view)

The following diagrams show the connection ports on the rear of the blade drawer.



Mark	Description
A	CMM dynamically configurable stacking or Ethernet port
B	CMM serial port
C	CMM dynamically configurable stacking or Ethernet ports
D	QSM QSFP ports (1-18)
E	ESM dynamically configurable stacking or Ethernet ports
F	ESM serial port
G	ESM dynamically configurable stacking or Ethernet port

Figure 1-10. Connection ports - Rear view with ESM module



Mark	Description
A	CMM dynamically configurable stacking or Ethernet port
B	CMM serial port
C	CMM dynamically configurable stacking or Ethernet ports
D	QSM QSFP ports (1-18)
E	TSM dynamically configurable stacking or Ethernet ports
F	TSM serial port
G	TSM 1 Gb Ethernet port

Figure 1-11. Connection ports - Rear view with TSM module

Chapter 2. Getting Started

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

2.1. Starting the Hardware Console

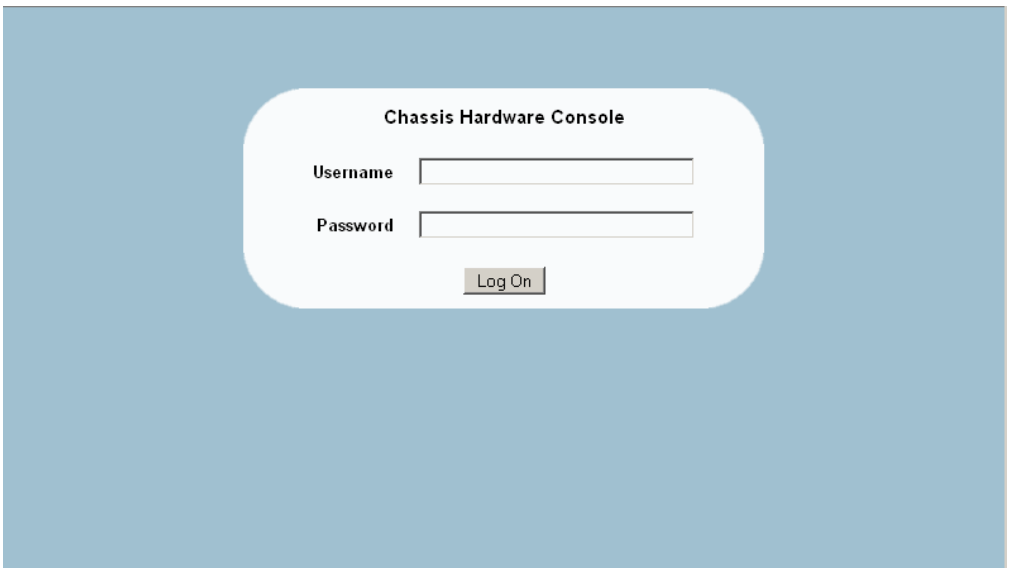
The hardware console is launched from a Web browser using a standard or secure IP address or host name, according to settings.

Prerequisites

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

Your web browser is configured to accept cookies.

Procedure



Hardware Console	
Username	Factory-default name: super
Password	Factory-default password: bull

Figure 2-1. Logon

Important **It is strongly recommended to change the factory-default super user password once initial setup is completed, taking care to record your new account details for subsequent connections.**
If you lose your account details and are unable to connect to the console, please contact your Customer Service Representative.

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

What To Do if an Incident Occurs?

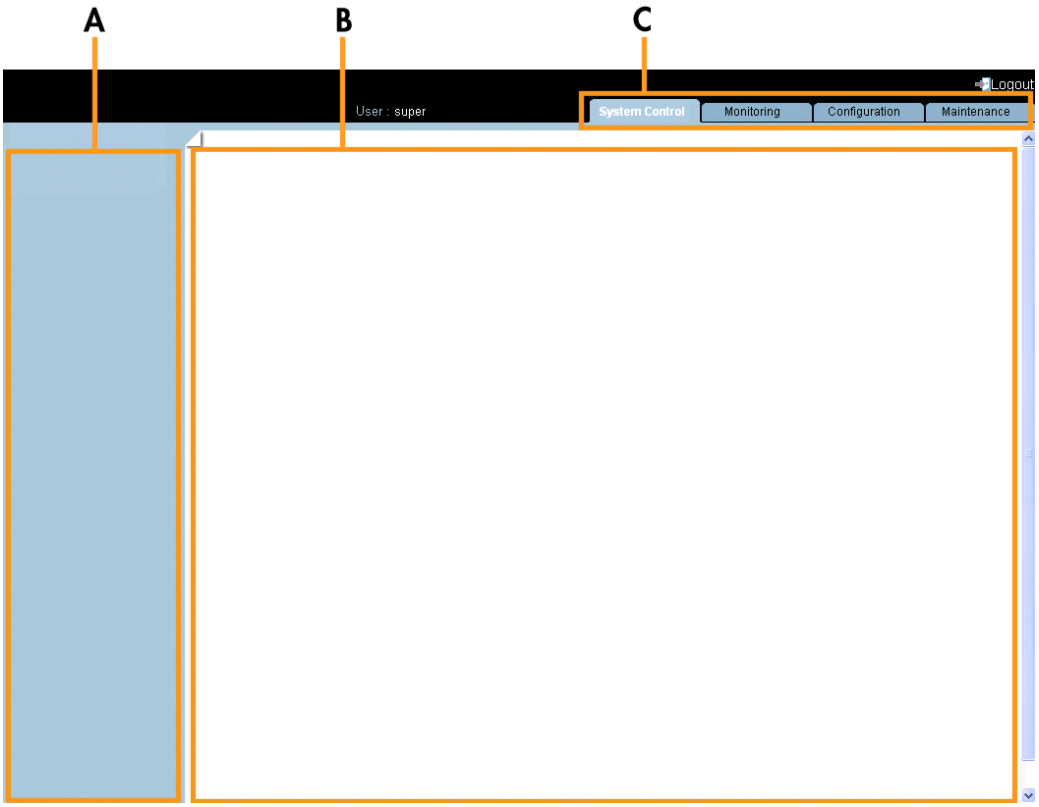
If you cannot connect to the console or if the web pages are displayed incorrectly, one of the following problems may be the cause:

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

2.2. Hardware Console Overview

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

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



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

Figure 2-2. Hardware Console overview

Console Interface Features

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

Tab	Tree node	Features	Permission
System Control	Power Management	Power	Viewing: All users Operations: root users
		Power Policy	Viewing: All users Operations: root users
Monitoring	Cabinet Status & Logs	Sensor Status	Viewing: All users
		System Event Log	Viewing: All users Operations: root users
		Messages	Viewing: All users Operations: root users
Configuration	General Settings	Chassis	Viewing: All users Operations: root users
		CMC Network	Viewing: All users Operations: root users
		BMC Network	Viewing: All users Operations: root users
		Date-time	Viewing: All users Operations: root users
		SNMP	Viewing: All users Operations: root users
		Messages	Viewing: All users Operations: root users
	User Management	Users	Viewing: All users Operations: root users
		Groups	Viewing: All users Operations: root users
		Password	Viewing: All users Operations: root users
	Security Management	Encryption	Viewing: All users Operations: root users
		SSL Certificate	Viewing: All users Operations: root users
		User Logon Policy	Viewing: All users Operations: root users
		Authentication	Viewing: All users Operations: root users
		Power Button Lockout	Viewing: All users Operations: root users
		User Lockout	Viewing: All users Operations: root users

Tab	Tree node	Features	Permission
Configuration	Alert Settings	Filters	Viewing: All users Operations: root users
		Policies	Viewing: All users Operations: root users
		LAN Destinations	Viewing: All users Operations: root users
		General	Viewing: All users Operations: root users
Maintenance	Hardware Information	Management Board	Viewing: All users Operations: root users
		FRU	Viewing: All users Operation: root users
		Firmware	Viewing: All users
		Force New Drawer Discovery	Viewing: All users
		Simple Drawer Information	Viewing: All users
	Firmware Updates	CMC	Viewing: All users Operations: root users
	Maintenance Operations	Unit Reset	Viewing: All users Operations: root users
		Identification LED	Viewing: All users Operations: root users
		Hardware Exclusion	Viewing: All users Operations: root users
		Server Blade Change	Viewing: All users Operations: root users
		CMM Change	Viewing: All users Operations: root users
		ESM / TSM Change	Viewing: All users Operations: root users
		IBSW Change	Viewing: All users Operations: root users
		LCP Change	Viewing: All users Operations: root users
		Power Management	Viewing: All users Operations: root users
		Connected Users	Viewing: All users Operations: root users
		UCM Management	Viewing: All users Operations: root users
		Force Backup BMC Boot	Viewing: All users Operations: root users

Table 2-1. Chassis Hardware Console interface features and permissions

2.3. Stopping the Hardware Console

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

)in the upper-right corner of the console.

2.4. Initial Configuration

When the chassis is first delivered, you will need to perform a few basic configuration tasks to ensure correct operation and identification by management software. These configuration tasks are explained in detail in Chapter 5. Configuring the Chassis Management Controller and are listed below by order of priority:

- Configuring Network Settings for Remote Access, on page 5-3
- Setting the Chassis Name, on page 5-2
- Modifying Internal Clock Settings, on page 5-10

Note The other configuration tasks can be performed when required.

Chapter 3. Using Chassis Power Controls

This chapter explains how to use power controls and check power status. It includes the following topics:

3.1. Using 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

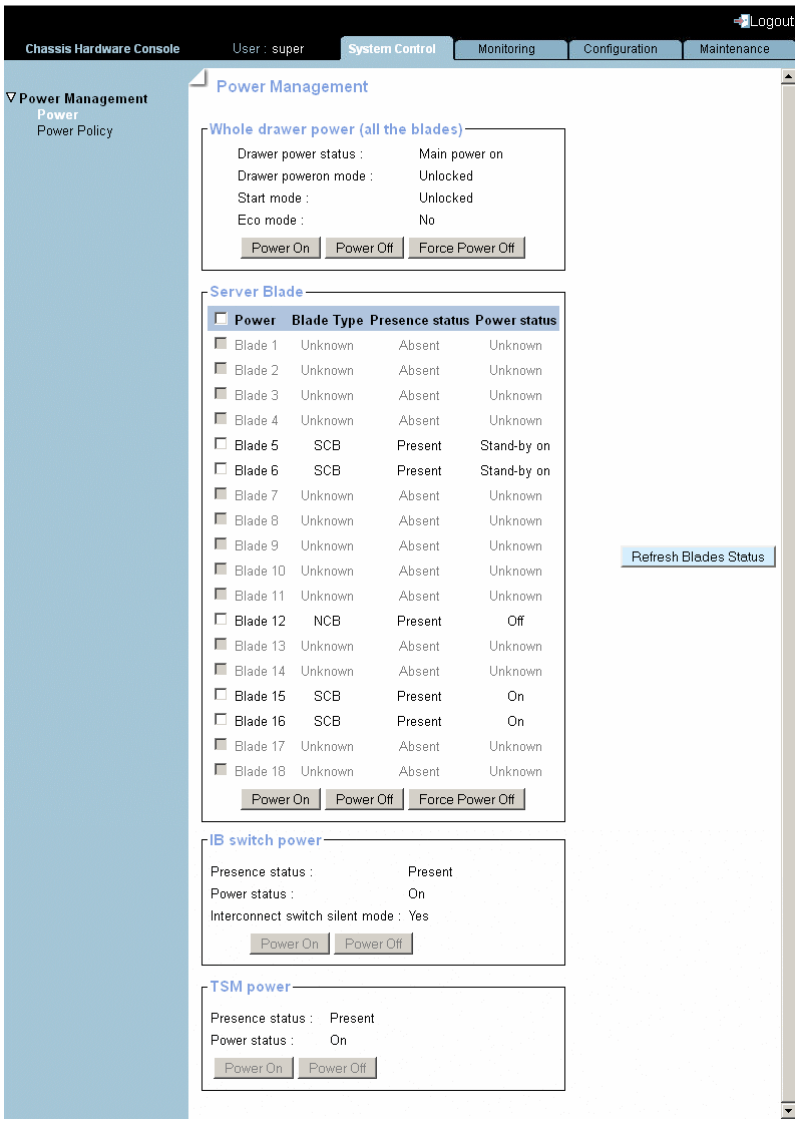
Operations: root users

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 four 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 routine power on/off sequences
- **TSM power** is used to perform routine power on/off sequences



Whole drawer power	
Drawer power status	Provides the status of drawer power. • 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 on: It is the functional state of the drawer
Drawer poweron mode	Provides the status of drawer poweron mode. • Full power on: All the blades and other chassis components are powered on during the drawer powering on • Unlocked (default): All the blades and chassis components are unlocked (12 V hot swap enabled) during the drawer powering on
Start mode	Provides the status of start mode. • Deep Stand-by: The blade stays in stand-by off state (i.e. BMC is not running) • Light Stand-by: The blade state becomes stand-by on (i.e. the BMC will be running) • Unlocked (default): The blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)
Eco mode	Provides the status of Eco mode. • Yes: This forces drawer to silent mode. (The drawer can be configured to save the energy when the 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
Blades	
Power	Blade number.
Blade Type	• NCB (compute blade) • GPU (accelerator blade) • SCB (dual-node blade)
Presence status	• Present: The corresponding blade is present • Absent: The corresponding blade is absent
Power status	• Off: The corresponding blade is powered Off • On: The corresponding blade is powered On • Standby-off: The corresponding blade is powered Off. • Standby-on: The corresponding blade is powered On in stand-by mode. • Unknown: The corresponding blade is absent

IB switch power	
Presence status	Indicates the status of the Quad Switch Module (QSM). • Absent: The Quad Switch Module is absent • Present: The Quad Switch Module is present
Power status	Indicates the power status of the Quad Switch Module. • Unknown: The Quad Switch Module is absent • Stand-by off: The Quad Switch Module is powered Off • On: The Quad Switch Module is powered On
Interconnect switch silent mode	Indicates the status of the silent mode. • Yes (default): The QSM and TSM are set to silent • No: The QSM and TSM can be powered off
TSM power	
Presence status	Indicates the status of the 10 Gigabit Ethernet Switch Module (TSM). • Absent: The 10 Gigabit Ethernet Switch Module is absent • Present: The 10 Gigabit Ethernet Switch Module is present
Power status	Indicates the power status of the 10 Gigabit Ethernet Switch Module. • Unknown: The 10 Gigabit Ethernet Switch Module is absent • Stand-by off: The 10 Gigabit Ethernet Switch Module is powered Off • On: The 10 Gigabit Ethernet Switch Module is powered On

Table 3-1. Blade chassis Power Management page features

3.1.1. Viewing the Blade Chassis Whole Drawer Power

The blade chassis power status can be checked at all times from the Hardware Console.

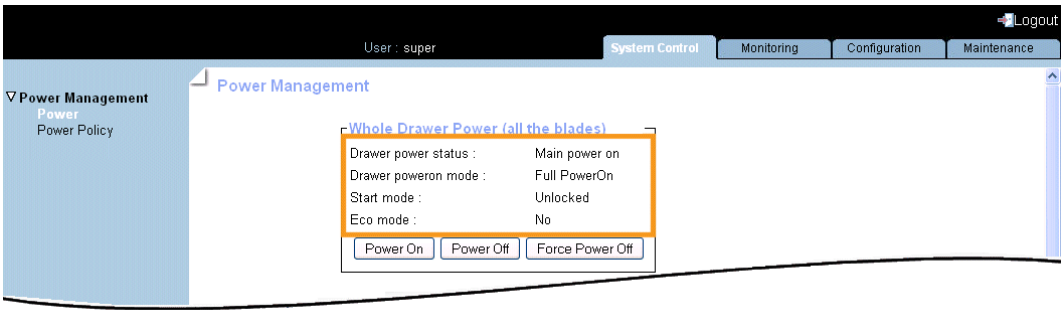
Prerequisites

Viewing: All users

Operations: Admin group users

Procedure

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



Whole drawer power	
Drawer power status	Provides the status of drawer power. • **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 poweron mode	Provides the status of drawer poweron mode. • **Full power on**: All the blades and other chassis components are powered on during the drawer powering on • **Unlocked**: All the blades and chassis components are unlocked (12 V hot swap enabled) during the drawer powering on
Start mode	Provides the status of start mode. • **Deep Stand-by**: The blade stays in stand-by off state (i.e. BMC is not running) • **Light Stand-by**: The blade state becomes stand-by on (i.e. the BMC will be running) • **Unlocked**: The blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)

Whole drawer power	
Eco mode	Provides the status of Eco mode. • **Yes**: This forces drawer to silent mode. (The drawer can be configured to save the energy when the 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

Figure 3-1. Whole drawer power page

3.1.2. Powering on the Blade Chassis

The blade system can be powered on from the Hardware Console.

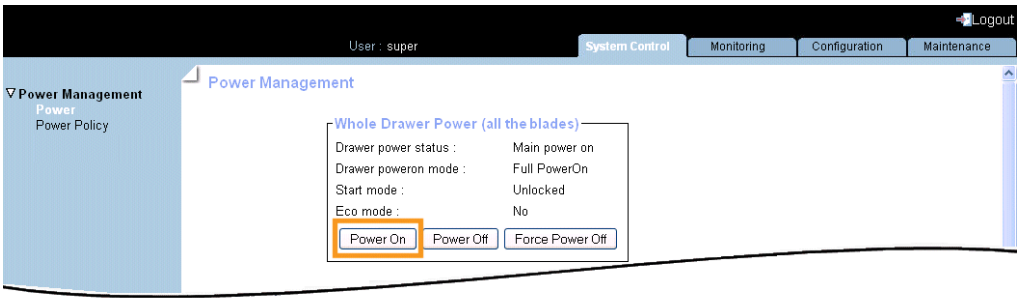
Prerequisites

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.



Power on Information	
Power on	Launches the power up sequence. The final state of blades depends on the setting **Drawer Poweron mode**. If the **Drawer Poweron mode** is **Full Power On**, the blade is powered up. If the **Drawer Poweron mode** is **Unlocked**, the blade reaches the Off (unlocked) power state.

Figure 3-2. Powering on the blade chassis

2. 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.

3. Connect to the **Remote System Console** to follow the power on sequence.

3.1.3. Powering off the Blade Chassis

The blade system can be powered off from the Hardware Console.

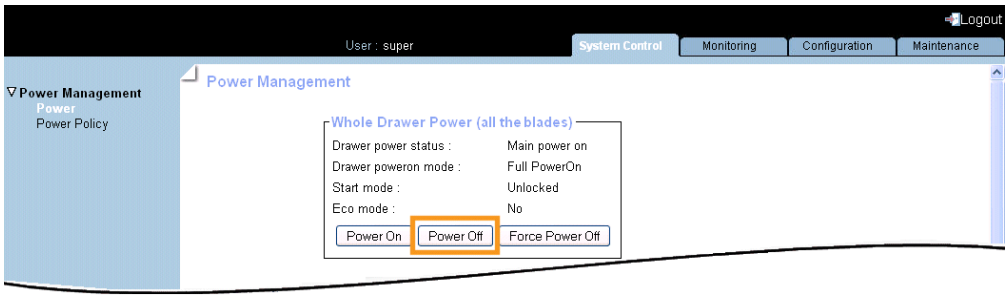
Prerequisites

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.



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

Figure 3-3. Powering off the blade chassis

2. 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 blade

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

3. Connect to the **Remote System Console** to follow the power on sequence.

What to do if an incident occurs?

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 Blade Chassis

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

Prerequisites

Viewing: All users

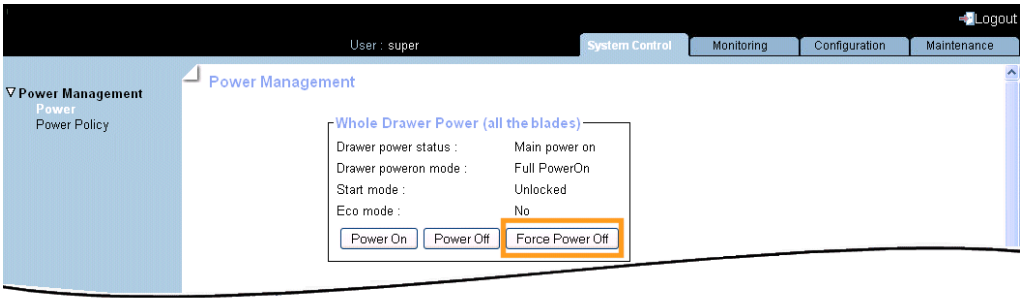
Operations: root users

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.



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.

Figure 3-4. Forcibly powering off the 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. Powering on/off Individual Blades and Checking Status

The 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 blades.

Prerequisites

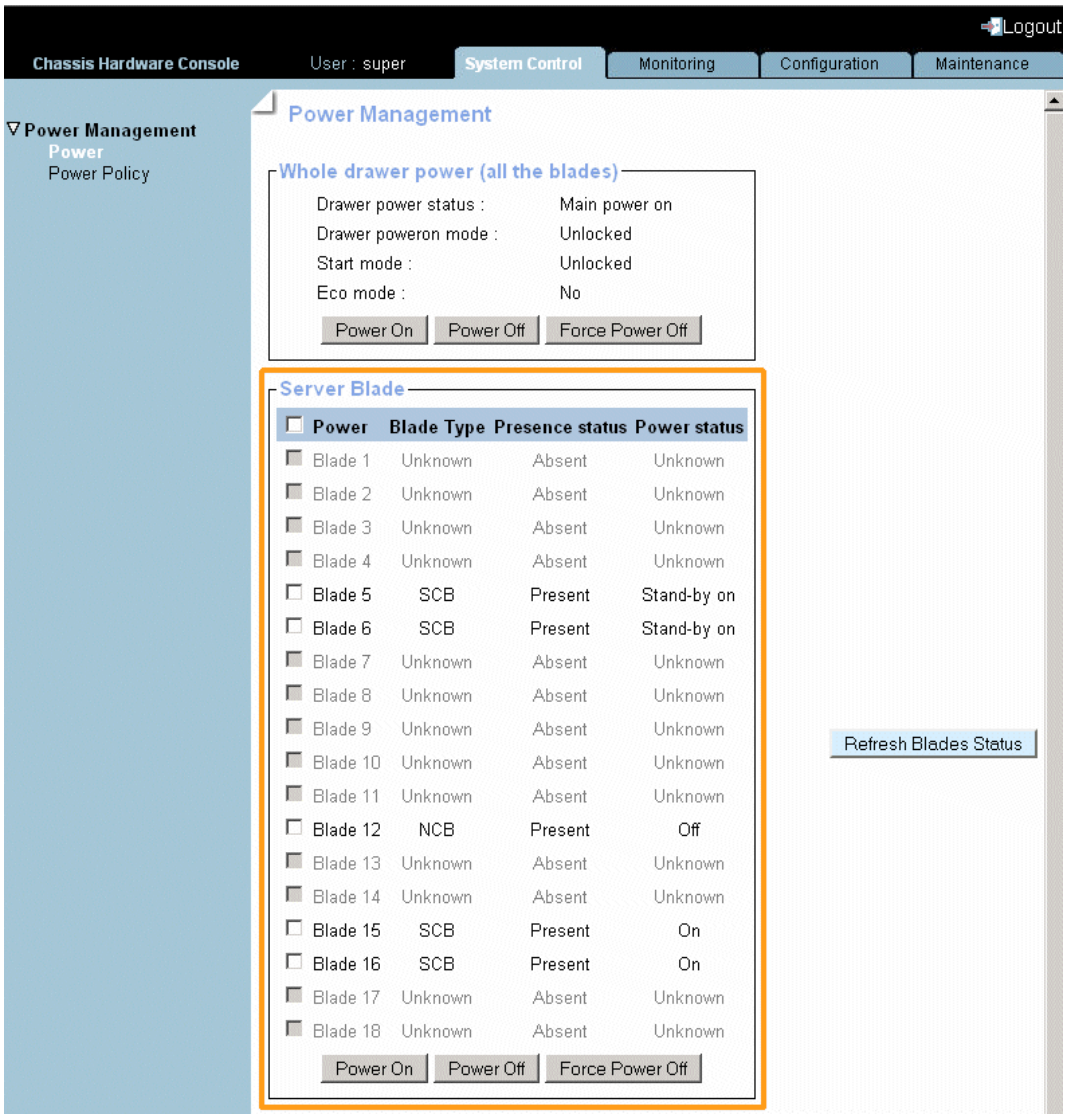
Viewing: All users

Operations: root users

Pocedure

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 **Server Blade**.



Server Blade	
Power On	Accessible only when the system is powered Off. This button powers On the corresponding blade.
Power Off	Accessible only when the system is powered On. This button powers Off the corresponding blade.
Force Power Off	This button performs a power down sequence independently of the Operating System. If the **Power Off** operation fails, you can forcibly power Off by clicking **Force Power Off** button.

Figure 3-5. Blades box description

3.1.6. Viewing Quad Switch Module (QSM) Power Status

IB switch (Quad Switch Module) policies provide the information of Presence status, Power status, and silent mode.

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.

In the **Power Management** page the third box is the **IB Switch Power**.

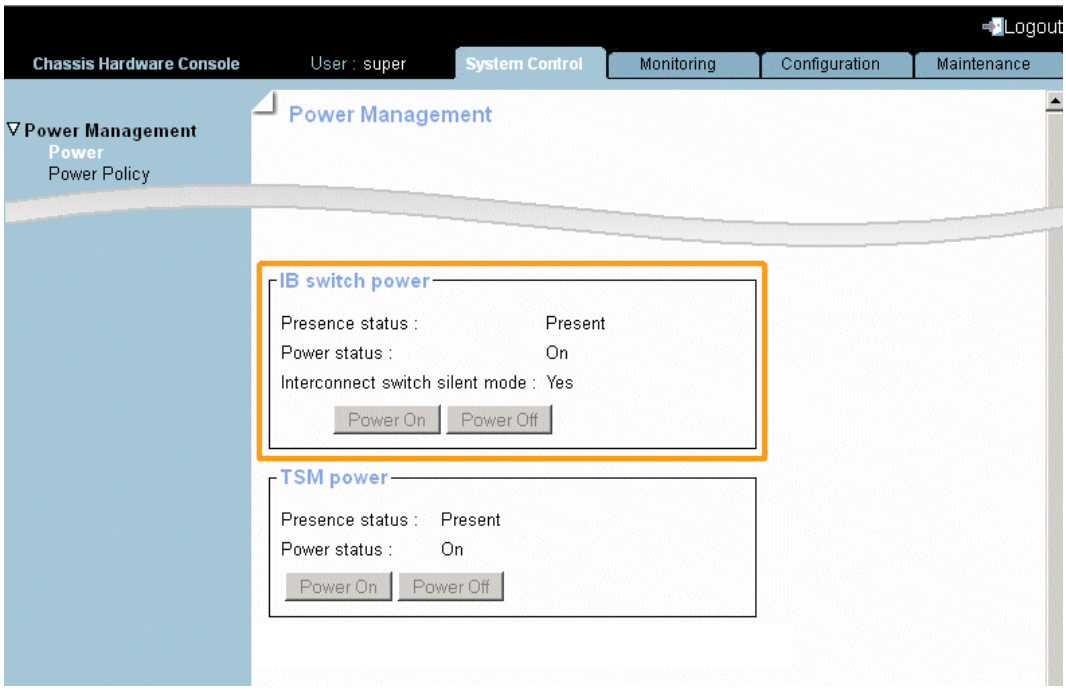


Figure 3-6. IB switch power box

IB Switch Power	
Presence status	Indicates the status of Quad Switch Module. • **Absent**: The Quad Switch Module is absent • **Present**: The Quad Switch Module is present
Power status	Indicates the Power status. • **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
Interconnect switch silent mode	Provides the status of the silent mode. • **Yes**: The IB switch and the TSM silent modes are set to silent • **No**: The IB switch and the TSM can be powered off

Table 3-2. IB Switch Power box description

3.1.7. Viewing 10 Gigabit Ethernet Switch Module (TSM) Power Status

10 Gigabit Ethernet Switch Module policies provide the information of Presence status and Power status.

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.

In the **Power Management** page the fourth box is the **TSM Power**.

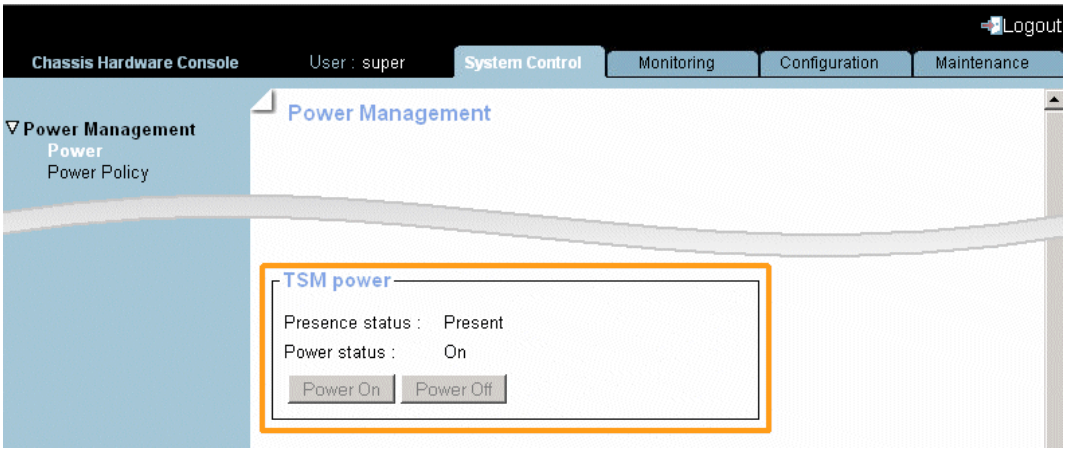


Figure 3-7. TSM power box

10 Gigabit Ethernet Switch Power	
Presence status	Indicates the status of 10 Gigabit Ethernet Switch Module. • **Absent**: The 10 Gigabit Ethernet Switch Module is absent • **Present**: The 10 Gigabit Ethernet Switch Module is present
Power status	Indicates the Power status. • **Unknown**: The 10 Gigabit Ethernet Switch Module is absent • **Stand-by Off**: The 10 Gigabit Ethernet Switch Module is powered Off • **On**: The 10 Gigabit Ethernet Switch Module is powered On

Table 3-3. TSM Power box description

3.2. Applying Power Policies

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

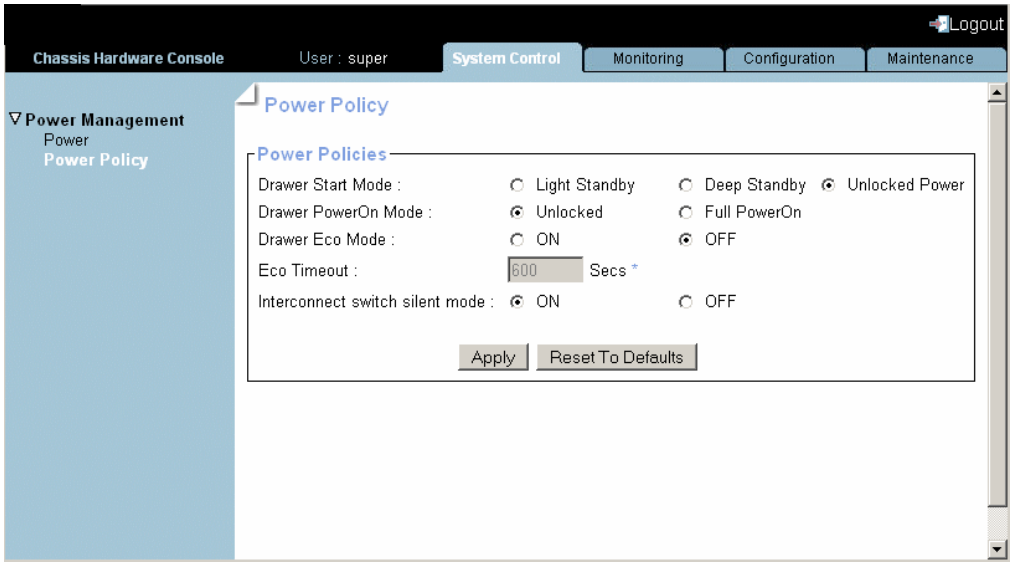
Prerequisites

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.



Power Policies	
Drawer start mode	• **Light Standby**: The **Light stand-by** state is the moderate power consumption waking state for the drawer (the blades are operational) • **Deep Standby**: 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	• **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

Power Policies	
Drawer ECO mode	• ON: This forces drawer to eco mode to be On. (The drawer can be configured to save the energy when the 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 Interconnect 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.
Interconnect Switch Silent Mode	• ON: This forces IB switch (QSM) and TSM silent mode to be silent The IB switch and TSM are implicitly powered on when the blade is powered on, and are implicitly powered off when the last blade is powered off. • OFF: This forces IB switch and TSM silent mode to be not silent. The IB switch and TSM are explicitly powered on/off.

Figure 3-8. Power Policy page

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

Chapter 4. Monitoring the Blade

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

4.1. Initial Messaging and Alert Configuration

When the chassis is first delivered, you will need to perform a few basic configuration tasks to benefit from all the messaging and alert features available. These configuration tasks are explained in detail in Chapter 5, Configuring the Chassis Management Controller, and are listed below:

4.2. Checking Monitoring Sensors

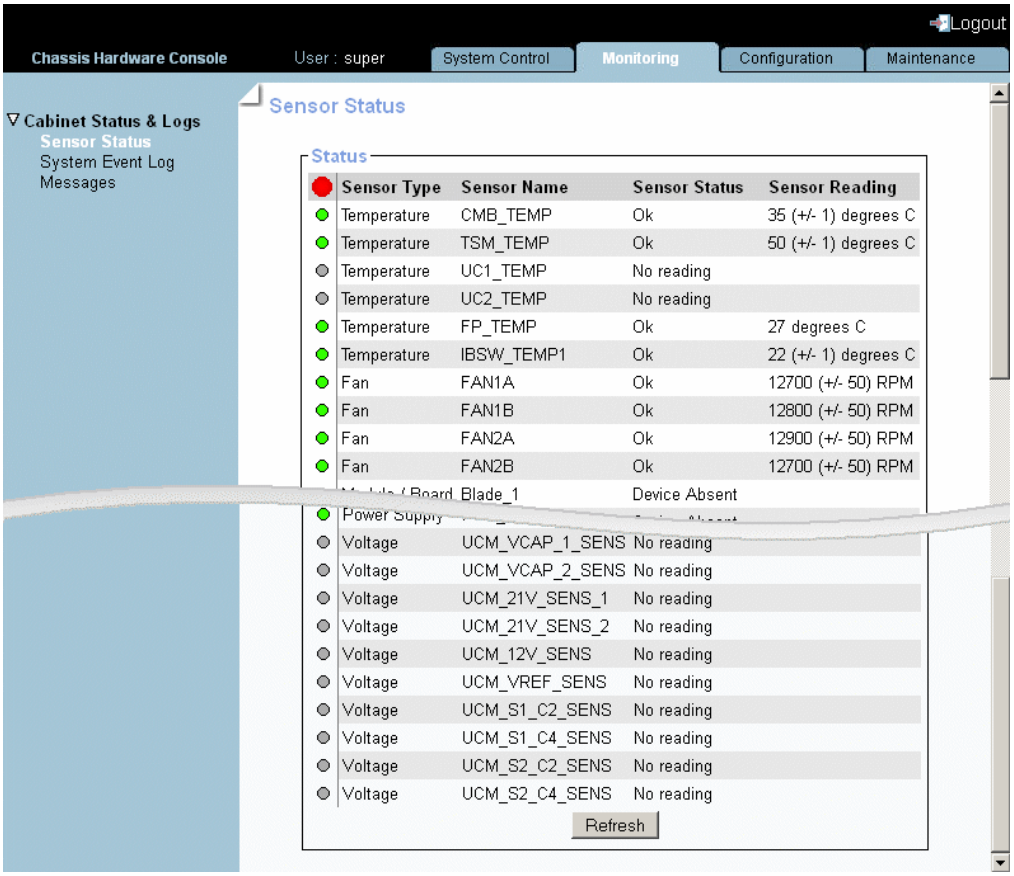
The system is equipped with various sensors that monitor the status of hardware components, such as:

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

Procedure

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

   If a component icon is not green, see Appendix B Troubleshooting the Blade System for more information.



Sensor Status Page	
Refresh button	The Sensor Status page is not automatically updated, therefore the display may not reflect current sensor status. Use this button, located at the top and bottom of the page, to update the display.
Status Icons Description	
The status icons to the left of certain sensors indicate the status of the monitored component with regard to nominal threshold values.	
GREEN	NORMAL Operation correct. No problem has been detected.
YELLOW	NON-CRITICAL A problem has been detected that may need preventive or corrective action.
RED	CRITICAL A problem has been detected. Immediate preventive or corrective action is required.
GRAY	Sensor not available.
GLOBAL	The global status icon at the top of the page reflects overall system status.

Figure 4-1. Sensor Status

For reference, the following table lists sensors reading values without thresholds. Refer to Appendix B Troubleshooting the Blade System for detailed information.

Icon	Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Green Red	Power Supply	PSU_X	Device Present Device Absent	-
Green Red	Power Supply	PSU_X_Fail	OK No reading	-
Green Red Yellow Gray	Power Supply	Drawer Power PSU_X_PWRIn		Value in watts
Green Red Yellow Gray	Temperature	CMB_TEMP ESM_TEMP/TSM_TEMP UC1_TEMP UC2_TEMP FP_TEMP IBSW_TEMP1	OK (normal) Above upper non-critical threshold No reading	Value in °C
Green Red Yellow Gray	Fan	FAN X	OK Below power non-recoverable threshold	Value in RPM
Green Red Yellow Gray	Module/Board	Blade_X IBSW UCM	Device Present Device Absent	
Green Red Yellow Gray	Voltage	PSU_x_12V_PG Blade_x_3V3_PG Blade_x_Sys_PG PSU_x_VIn PSU_x_Out UCM_VCAP_x_SENS UCM_21V_SENS_x UCM_12V_SENS UCM_VREF_SENS UCM_Sx_Cy_SENS		Value in Voltage
Green Red Yellow Gray	Current	PSU_X_In PSU_X_3V3_Iout PSU_X_12V_Iout		Value in Amps

Table 4-1. Sensor status page description

4.3. Checking and Clearing the System Event Log (SEL)

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

- Power supplies
-
- Temperature sensors

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

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

Prerequisites

Viewing: none

Operations: root users

Clearing: you have Alert Settings & Clear SEL permission

Procedure

- From the **Monitoring** tab, click **Cabinet & Status Log > System Event Log** to open the **System Event Log** page.

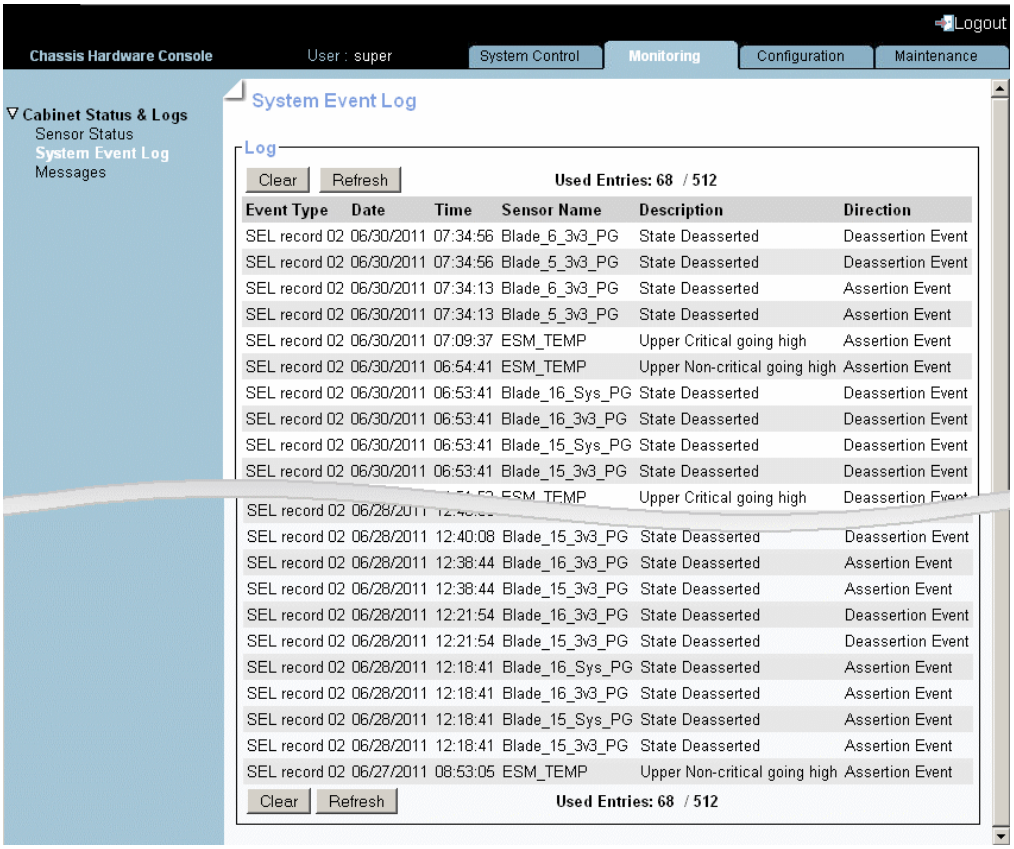


Figure 4-2. System Event Log

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

4.4. Checking the Board and Security Messages Log

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

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

Prerequisites

- Viewing: All users
- Operations: root users

Procedure

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

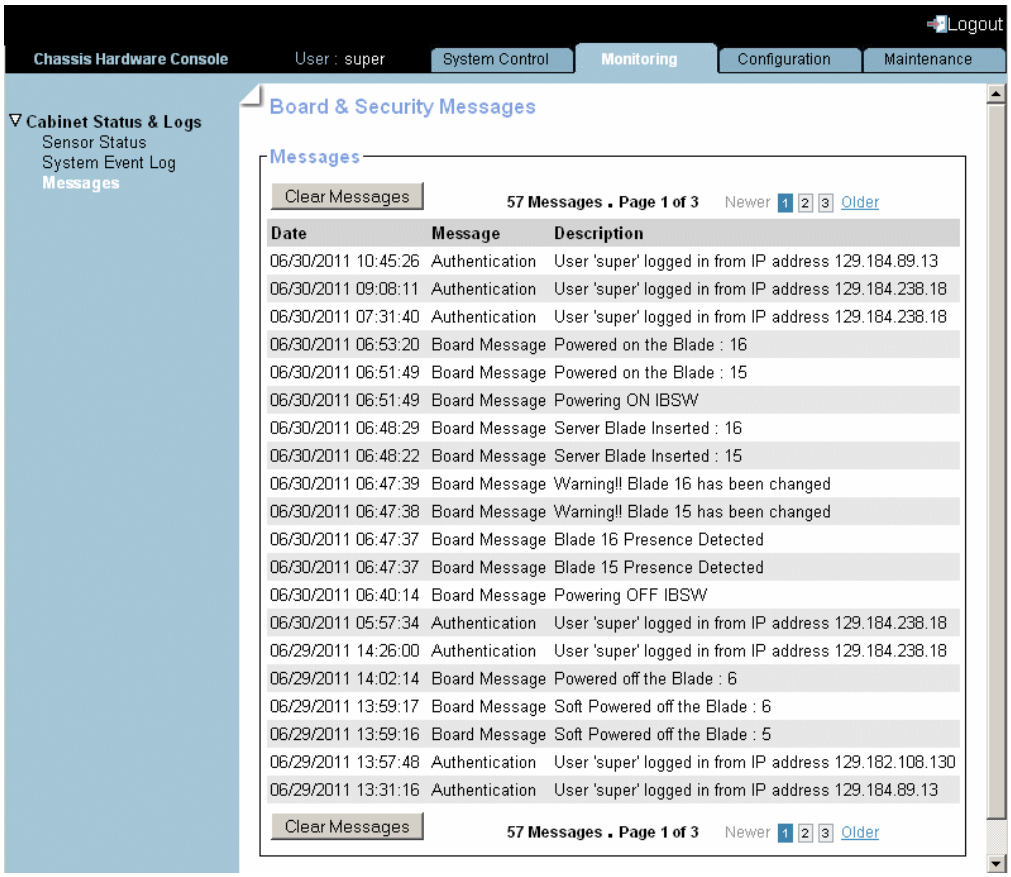


Figure 4-3. Board & Security Messages

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

Chapter 5. Configuring the Chassis Management Controller

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

WARNING

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

5.1. Setting the Chassis Name

This section describes how you can set the chassis name and position so that it can be easily identified by management software or maintenance personnel. You can set this name at any time.

Important **System Management software may be affected when you change the chassis name.**

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

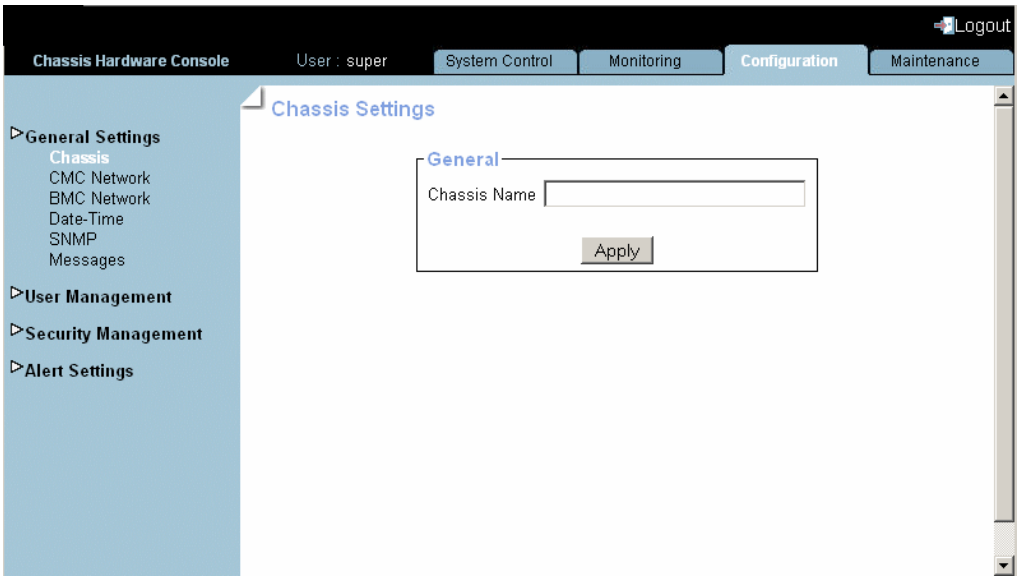
Prerequisites

You have Network Settings permission

You are aware of your organization's naming rules

Procedure

1. From the Configuration tab, click General Settings > Chassis to open the Chassis Settings page.



2. Complete the Chassis Name field.
3. Click Apply.

5.2. Configuring Network Settings for Remote Access

WARNING

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

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

Prerequisites

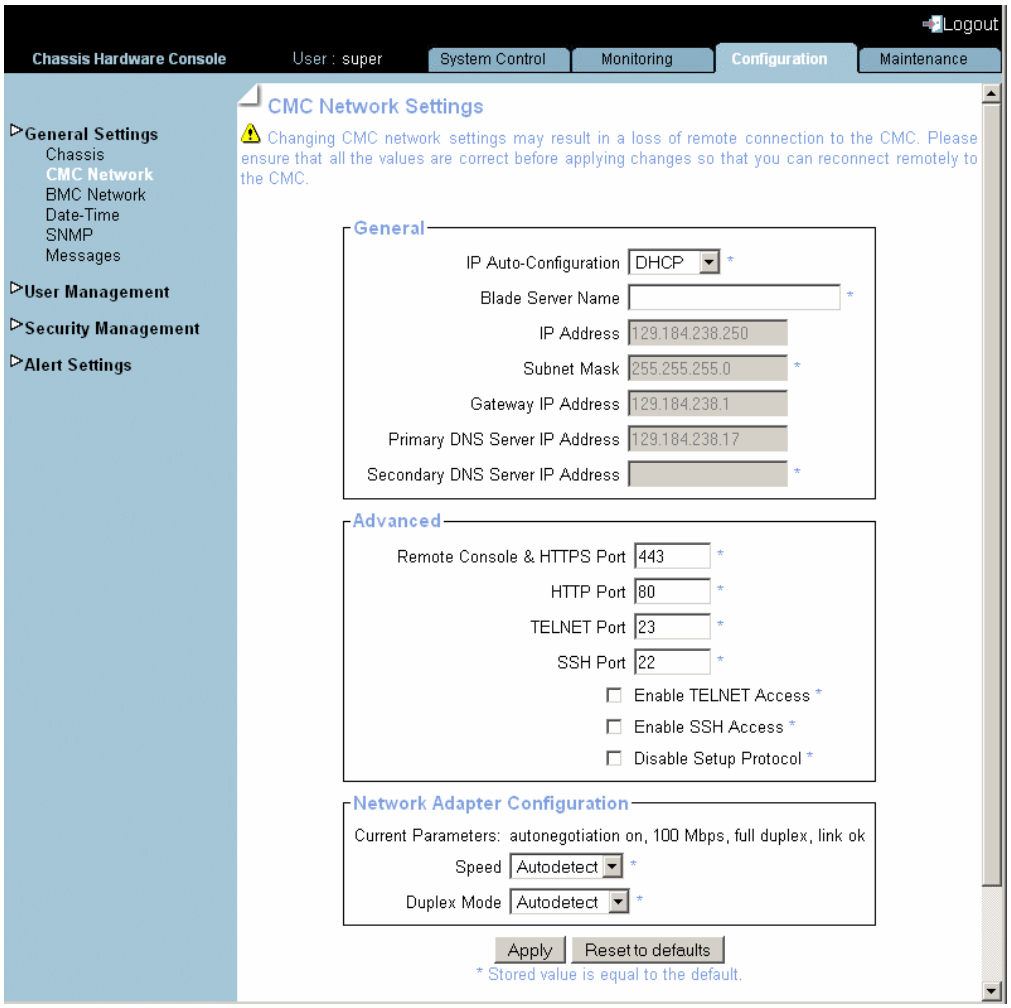
You have Network Settings permission

WARNING

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

Procedure

1. From the **Configuration** tab, click **General Settings** > **CMC Network** to display the 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: • 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.
Blade Server Name (DHCP only)	Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if None is selected. The static IP address you want to use (Factory-default value: 192.x.x.x).
Subnet Mask	Accessible only if None is selected. The subnet mask you want to use (Factory-default value: 255.255.255.0).
Gateway IP Address	Accessible only if None is selected. Your default gateway IP address, if applicable.
Primary DNS Server IP Address	Accessible only if None is selected. Your primary DNS server IP address, if applicable.
Secondary DNS Server IP Address	Accessible only if None is selected. Your secondary DNS server IP address, if applicable.
Advanced Box	
HTTPS Port	The port number used for secure HTTPS connections (Factory-default: 443).
HTTP Port	The port number used for standard HTTP connections (Factory-default: 80).
TELNET Port	The Telnet port number (Factory-default: 23).
SSH Port	The Secure Shell (SSH) port number (Factory-default: 22).
Enable TELNET Access	Select this option to allow connection using a Telnet client. You need SSH/Telnet Access permission.
Enable SSH Access	Select this option to allow connection using an SSH client. You need SSH/Telnet Access permission.
Disable Setup Protocol	Select this option to prevent the *psetup (Windows) tool* and/or *mc-setup (Linux) tool*, used to discover the server on the LAN during initial setup, from re-detecting this server when installing other devices.

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

Note * According to server model and network configuration the **Network Adapter Configuration Box** may not be visible.

Figure 5-1. Network Settings - factory-default values

2. Complete the fields to comply with your network requirements and click **Apply**.
3. Log off the console.
4. Start the console with the new network settings from a remote computer or workstation to test the connection.

What To Do if an Incident Occurs?

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

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

5.3. 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.

WARNING

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

Prerequisites

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.

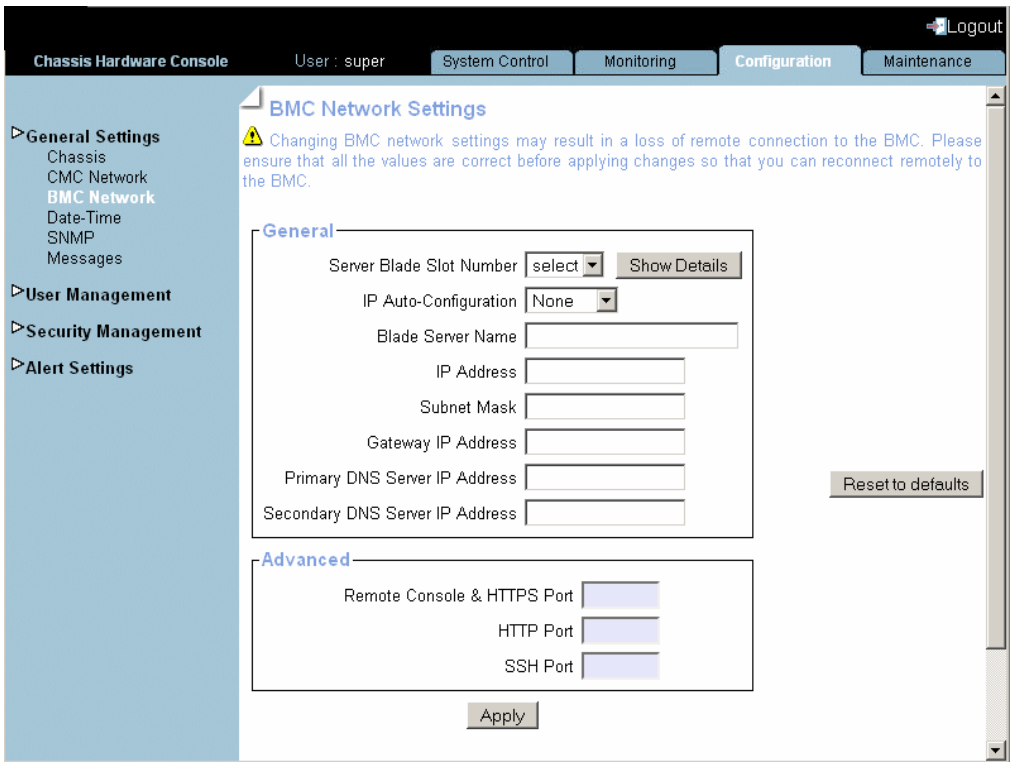


Figure 5-2. BMC Network Settings page

General Box	
Server Blade Slot Number	This drop-down lists all the blades. Show Details: Provides the information of the blades.
IP Auto-Configuration	This drop-down list allows you to enable or disable network auto-configuration via a DHCP or BOOTP server: • None: Auto-configuration is disabled. • DHCP: Network settings are retrieved from a DHCP server (Factory-default value). • BOOTP: Network settings are retrieved from a BOOTP server.
Blade Server Name (DHCP only)	Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server.
IP Address	Accessible only if auto-configuration is disabled. The static IP address you want to use (Factory-default value: 192.168.1.217).
Subnet Mask	Accessible only if auto-configuration is disabled. The subnet mask you want to use (Factory-default value: 255.255.255.0).
Gateway IP Address	Accessible only if auto-configuration is disabled. Your router IP address, if applicable.
Primary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your primary DNS server IP address, if applicable.
Secondary DNS Server IP Address	Accessible only if auto-configuration is disabled. Your secondary DNS server IP address, if applicable.
Advanced Box	
Remote Console and HTTPS Ports	The port number that is used for secure HTTPS connections and for the remote console (Factory-default: 443).
HTTP Port	The port number that is used for standard HTTP connections (Factory-default: 80).
SSH Port	The Secure Shell (SSH) port number (Factory default: 22).

Table 5-1. 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.

5.4. Modifying Internal Clock Settings

WARNING

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

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

WARNING

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

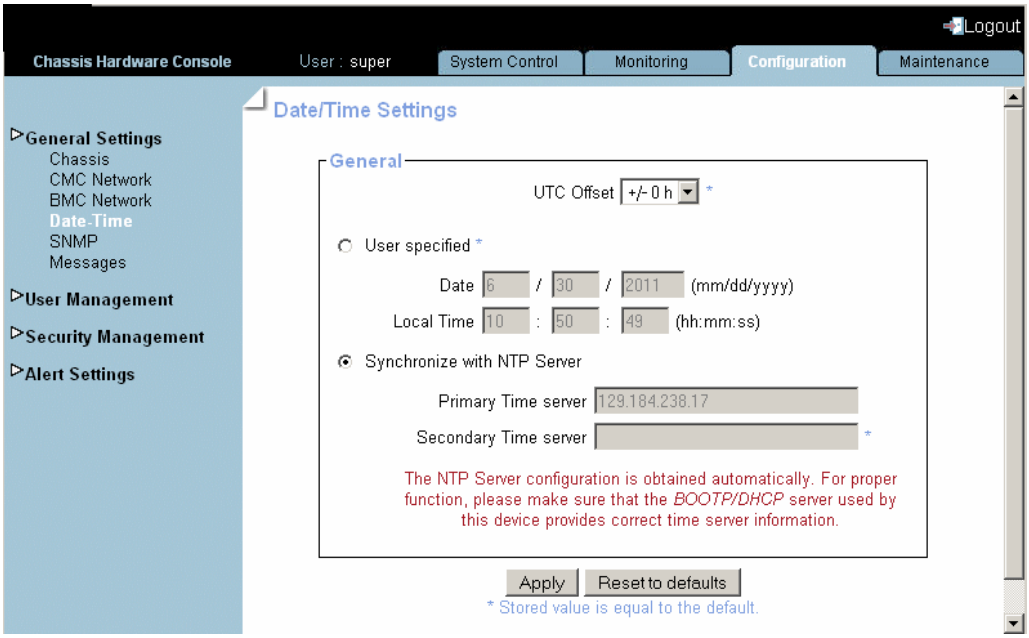
Prerequisites

You have Date/Time Settings permission

If you want to use NTP, you must have the IP addresses of the NTP servers you want to use

Procedure

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



General	
UTC Offset	Use this drop-down list to set the difference between local and universal time.
User Specified Time	This option allows you to manually set the server internal clock. Enter manually both the date and local time and check that the UTC Offset setting is correct.
Synchronize with NTP Server	This option allows you to enter the IP addresses of the NTP servers you want to use. You must use the UTC Offset drop-down list.
Reset to Defaults button	Allows you to display factory-default values.

Figure 5-3. Date/Time Settings - factory-default values

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

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

5.5. Enabling and Configuring the SNMP Agent

When enabled, the SNMP agent allows you to:

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

WARNING

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

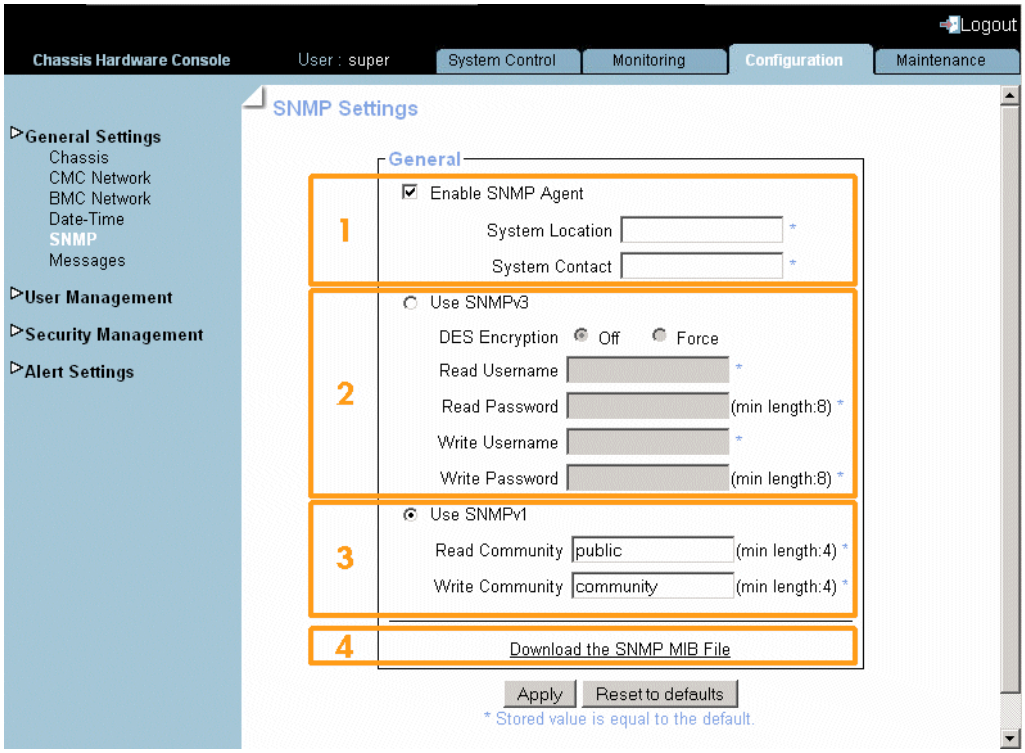
Prerequisites

You have SNMP Settings permission

Your SNMP manager is correctly configured

Procedure

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



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

Figure 5-4. SNMP Settings

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

Note A dedicated **Bull System Manager** Add-on 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 SNMPv1**, complete the corresponding fields accordingly:

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

     . To allow data retrieval and event reporting only, complete the **Read Community** field only.
     . To allow the performance of actions only, complete the **Write Community** field only.
   - If you select **Use SNMPv3**, complete the corresponding fields accordingly:
     . To allow data retrieval and event reporting only, complete the **Read User Name** and **Read Password** fields only.
     . To allow the performance of actions only, complete the **Write User Name** and **Write Password** fields only.
     . To allow data retrieval, event reporting AND the peformance of actions, complete the **Read User Name**, **Read Password**, **Write User Name** and **Write Password** fields
6. Click **Apply**.

5.6. Configuring the Board and Security Message Log

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

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

WARNING

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

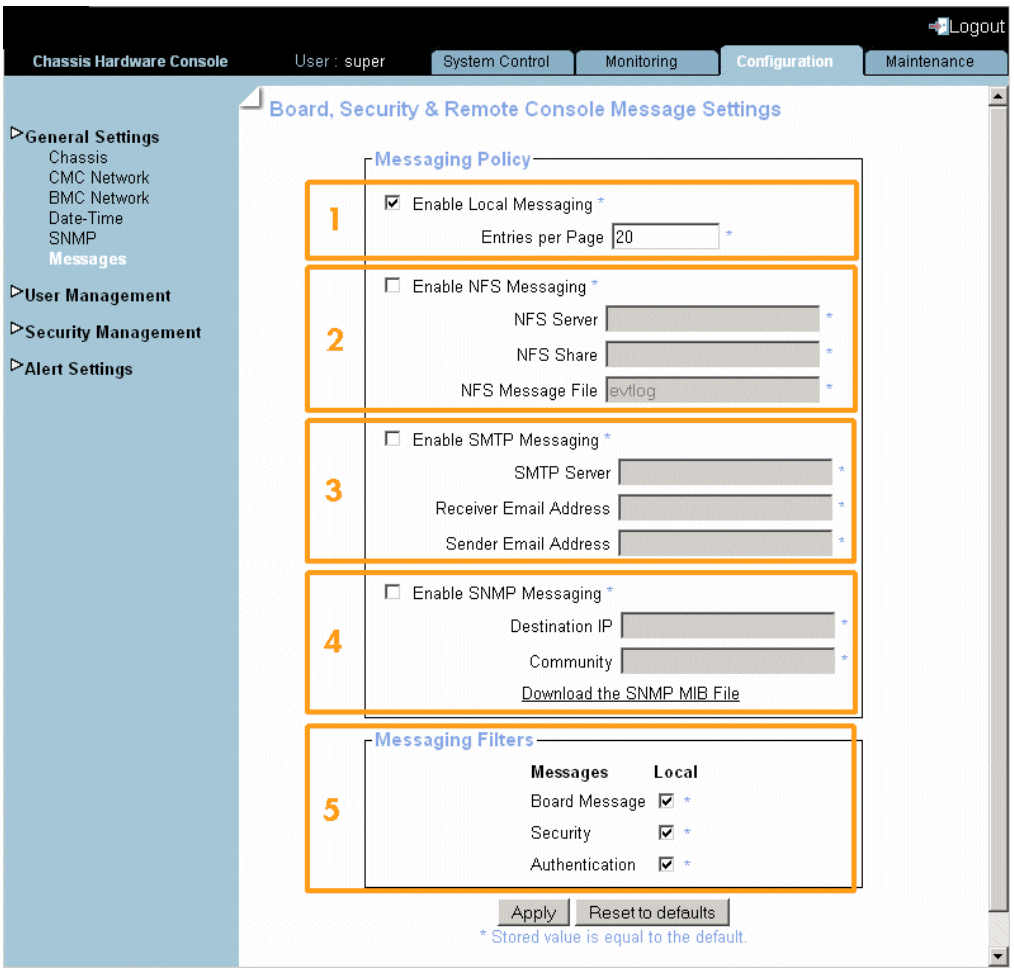
Prerequisites

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

You have configured your NFS / SMTP / SNMP server for messaging

Procedure

1. From the **Configuration** tab, click **General Settings > Messages** to display the **Board, Security & Remote Console Message 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	This option allows board and security messages to be written to a file located on a Network File System (NFS) server. IMPORTANT: • The size of the NFS message file is not limited: each event is appended to the end of the file indefinitely. Depending on your hard disk space, you may have to empty or archive the file at regular intervals. • DO NOT use the same file name to write messages from more than one system using the same NFS shared directory.
	• NFS Server	NFS server hostname or IP address.
	• NFS Share	Full pathname of the NFS shared directory. Note that the NFS shared directory is mounted immediately after you click the Apply button. To avoid error messages, use a valid NFS share value.
	• NFS Message File	Name of the file used to save the board and security messages.
Area 3	Enable SMTP Messaging	This option allows board and security messages to be sent by email to specified recipients. Emails contain the same description strings as the local messages and the mail subject is filled with the corresponding message group (Board Message, Security, 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. Note: The columns displayed in this box depends on the messaging policies enabled.		
Area 5	Board Messages	This group consists of information messages, such as: • Device succesfully started. • Board Reset performed by user… • Firmware upload failed. • No firmware file uploaded. • Uploaded firmware file discarded. • Firmware validation failed. • Firmware file uploaded by user… • Firmware updated by user… • Internal log file cleared by user…….
	Security	This group consists of the following message: • Security Violation.
	Authentication	This group consists of the following messages: • Login failed. • Login succeed.
View Defaults button		Allows you to display factory-default values. Click **Apply** to restore factory-default configuration.

Figure 5-5. Board, Security & Remote Console Messages Settings - factory-default values

2. Complete the fields as required.
3. Click **Apply**.

5.7. Managing Users

WARNING

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

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

5.7.1. Creating a User Account

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

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

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

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

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

Prerequisites

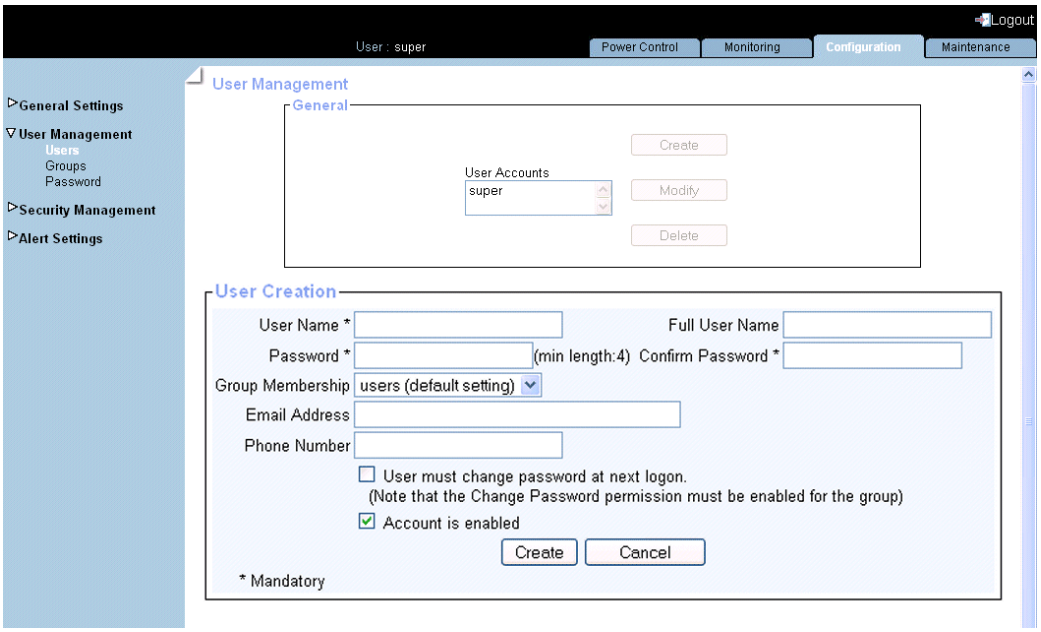
You have User/Group Management permission

You have created the group that the user is to be a member of

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

Procedure

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



User Creation	
User Name	Name the user will use to log on (often a "short name"). • Name limited to 32 characters. • The following characters are not allowed: \"!`&*%|~?/ and space.
Full User Name	The user's full name. • Name limited to 32 characters. • The following characters are not allowed: \"!`&*%|~?/ and space.
Password	The password the user will use to log on. • Minimum password length: 4 characters. • Maximum password length: 32 characters. • The following character is not allowed: space.
Confirm Password	
Group Membership	Use this drop-down list to select the group that this user is to be a member of, according to the permissions you want the user to have. Note: If you do not select a group, the newly created user is automatically attached to the predefined users group. The Change Password permission is NOT enabled for the predefined users group.
Email Address	User's email address. Example: john.smith@acme.com.
Phone Number	User's phone number. Use only arabic numerals and optionally the characters .-+ with NO spaces. Examples: 0625252525, +33.1.25.25.25.25

User Creation	
User must change password at next logon	When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on.
Account is enabled	When cleared, this option makes the user account unavailable: the user's account information is maintained but it is no longer possible to log on using this account.

Figure 5-6. User Management - User Creation

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

5.7.2. Displaying User Account Details

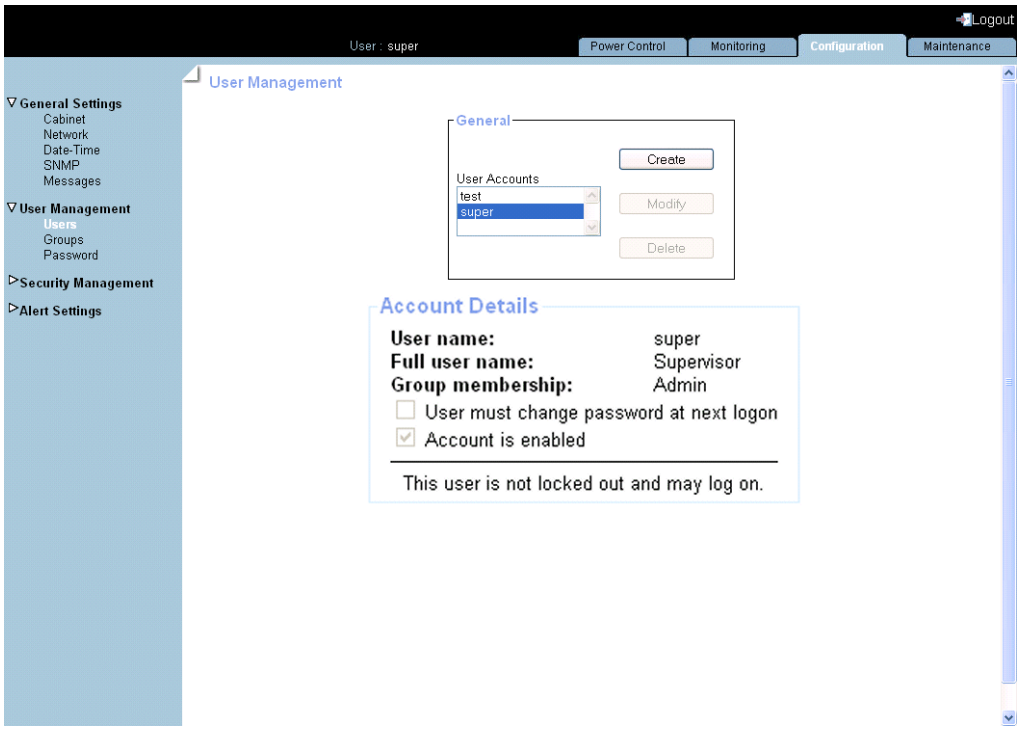
For easy user management, you can display the basic details of any user account at any time. You may want to use this feature, for example, to check user account details after the creation or modification of a user account or to check whether a user is locked out or not.

Prerequisites

You have **User/Group Management** permission

Procedure

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



Account Details	
User name	Name the user uses to log on (often a “short name”).
Full user name	The user's full name.
Group membership	Group that this user is a member of (and consequently the permissions the user has).
Email address	User's email address. This entry does not appear if the field is not completed when the user is created.
Phone number	User's phone number. This entry does not appear if the field is not completed when the user is created.
User must change password at next logon	When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on.
Account is enabled	When selected, the user account is active and the user is able to log on.

Figure 5-7. User Management - Account Details

5.7.3. Modifying a User Account

You can edit user account information at any time.

5.7.3.1. Updating Details

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

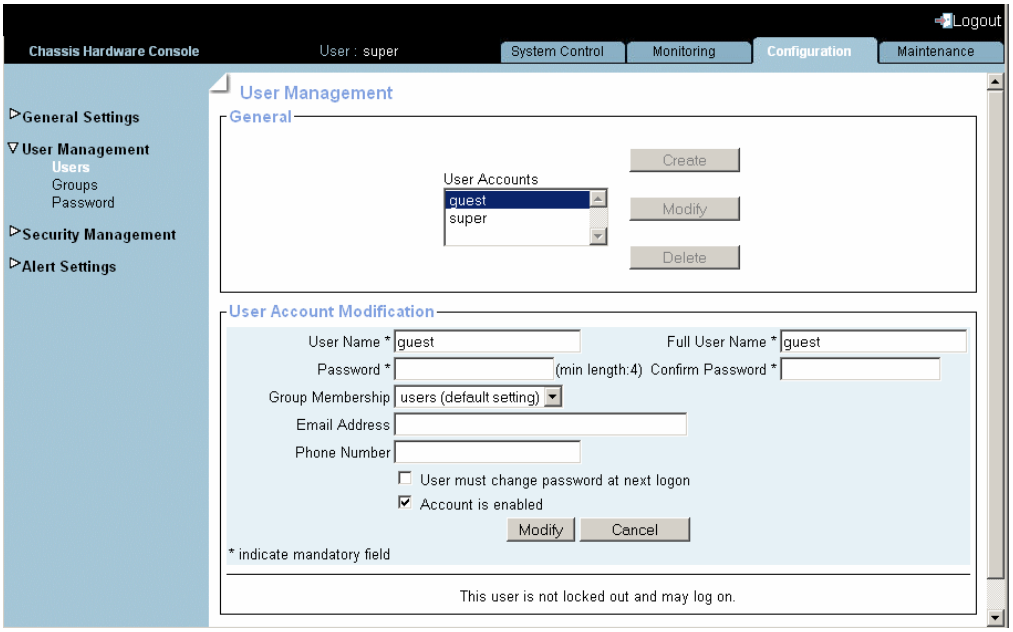
Note You cannot change the account details of the predefined **super** user. However, the default **super** user password can be changed through the **Password Management** page, as detailed in Modifying the Password, on page 5-28.

Prerequisites

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

Procedure

1. From the **Configuration** tab, click **User Management > Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.



3. Modify one (or more) of the following fields depending on your needs:
   - **User Name**,
   - **Full User Name**,
   - **Password** and **Confirm Password**,
   - **Email Address**,
   - **Phone Number**.

   Note For details about these fields, see Figure 5-6, on page 5-21.

4. Click **Modify**. User account details are changed.

5.7.3.2. Changing Group

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

Prerequisites

The group must be created

You have **User/Group Management** permission

Procedure

1. From the **Configuration** tab, click **User Management > Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. Select in the **Group Membership** drop-down list the wanted group, according to the permissions you want the user to have.
4. Click **Modify**. The user's group membership is updated.

5.7.4. Disabling/Enabling User Accounts

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

Prerequisites

You have **User/Group Management** permission

Procedure

1. From the **Configuration** tab, click **User Management > Users** to display the **User Management** page.
2. Select the user account you want to modify in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
3. To disable the account, clear the **Account is enabled** check box; to enable the account, select it.
4. Click **Modify**. The account is updated.

5.7.5. Forcing User Password Changes

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

Prerequisites

You have **User/Group Management** permission

The Group has **Change Password** permission

Procedure

1. Check that **Change Password** permission is enabled for the group to which the user belongs:
   a. From the **Configuration** tab, click **User Management > Groups** to display the **Group Management** page.
   b. Select the group to which the user belongs and click **Permissions** to display the **Group Permissions** page.
   c. Check that **Change Password** permission is enabled for the group. If this is not the case, enable the **Change Password** permission for the group.
2. From the **Configuration** tab, click **User Management > Users** to display the **User Management** page.
3. Select the user account in the **User Accounts** list box and click **Modify** to open the **User Account Modification** box.
4. Select the **User must change password at next logon** check box.
5. Click **Modify**. The user will be requested to change his/her password the next time he/she tries to log on.

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

5.7.6. Deleting a User Account

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

Prerequisites

You have **User/Group Management** permission

Procedure

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

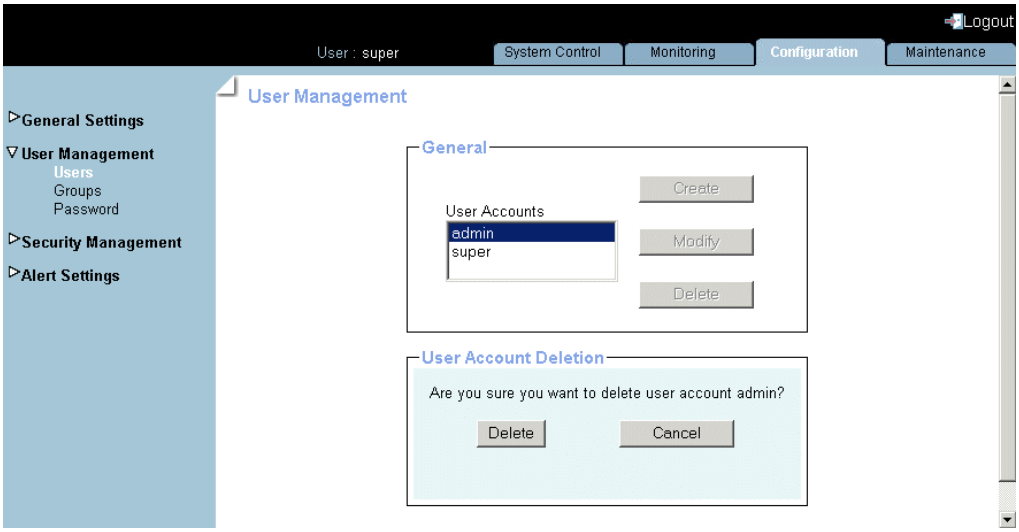


Figure 5-8. User Account Deletion

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

5.7.7. Manually Unlocking a User Account

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

Prerequisites

You have **User/Group Management** permission

Procedure

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

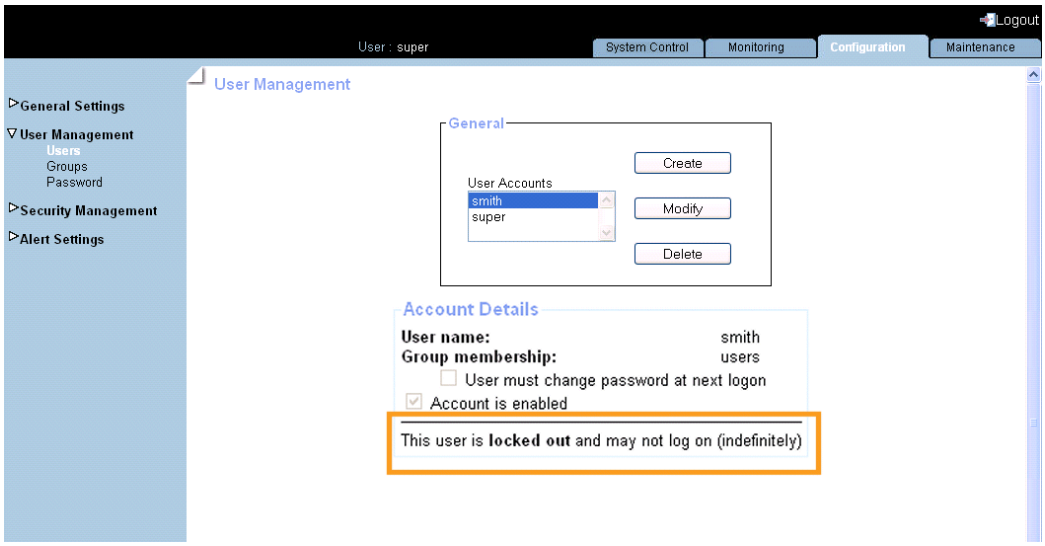


Figure 5-9. User Management - Locked-out user

3. Click **Modify** to display the **User Account Modification** box.
4. Click **Unblock**. The user account is unlocked and the user can now log on again.

5.7.8. Modifying the Password

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

Prerequisites

You have **Change Password** permission

Procedure

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

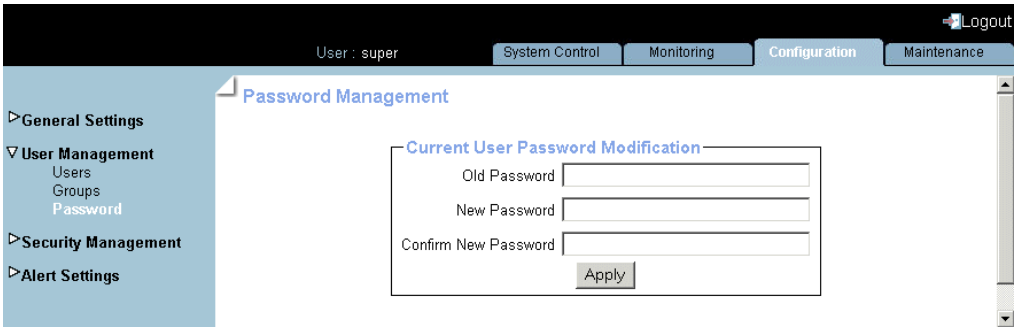


Figure 5-10. Password Management

Important

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

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

5.7.9. Creating a Group

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

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

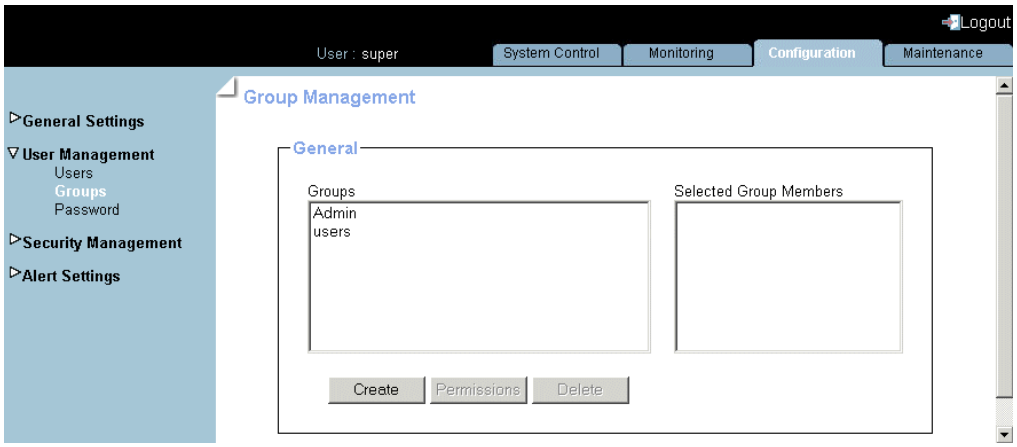
Important **Predefined groups and users cannot be renamed or deleted, but the default super user password can be changed.**
Permissions for the Admin group are not modifiable.
Permissions for the Users group are modifiable.

Prerequisites

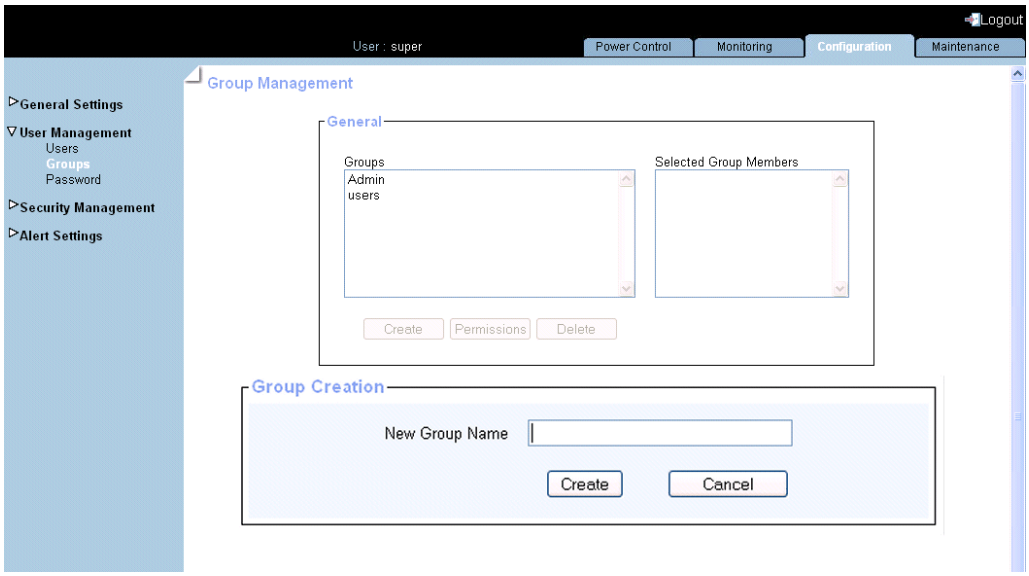
You have User/Group Management permission

Procedure

1. From the Configuration tab, click User Management > Groups to display the Group Management page.



2. Click Create to open the Group Creation box.



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

Figure 5-11. Group Management - Group Creation

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

5.7.10. Configuring Permissions

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

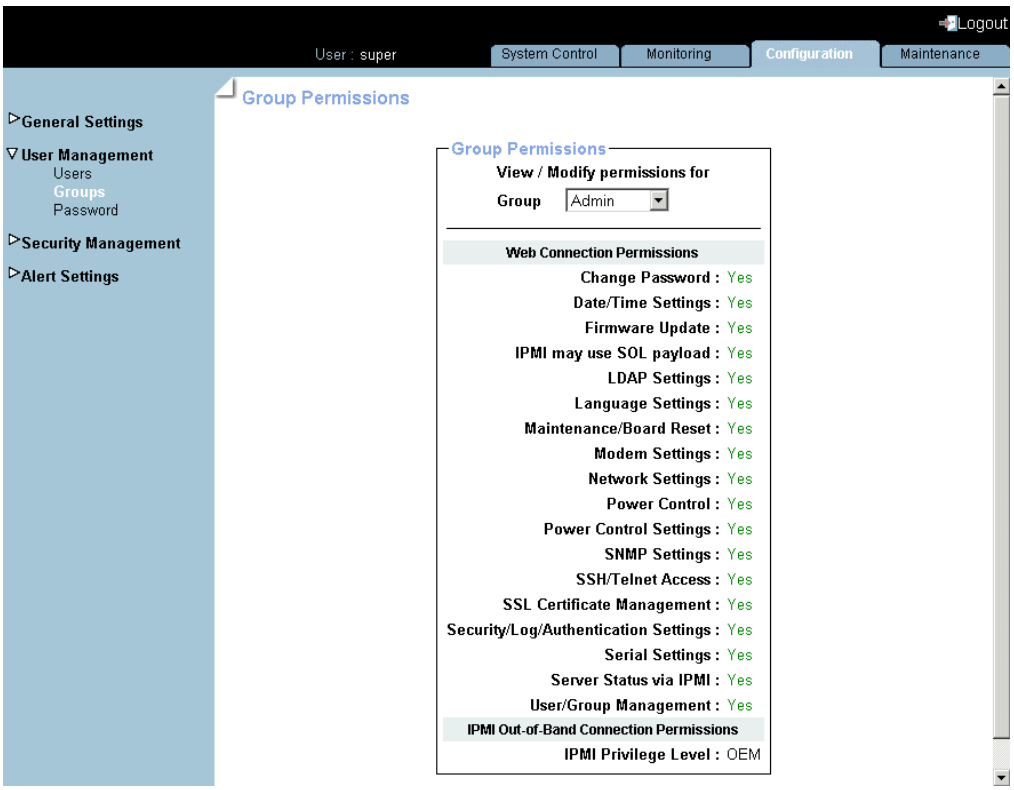
Prerequisites

You have **User/Group Management** permission

You have created the group for which you want to set permissions

Procedure

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



Group Permissions	
View / Modify Permissions for Group	This drop-down list allows you to select a group in order to view and/or modify the permissions set for the selected group.
Web Connection Permissions	This list allows you to enable or disable console features for the selected group. Select either 'Yes' or 'No' to enable or disable the feature(s) associated with each permission and click 'Apply'. Use Tables 5-2 and 5-3 to help you select permissions. Note: Certain features are accessible to all users and the associated non-configurable permissions are not listed in this page.
Out-of-Band Connection Permissions	The 'IPMI Privilege Level' drop-down list allows you to set a role for the selected group. See Table 5-4 and the IPMI specification for more details.

Figure 5-12. Group Permissions

3. Use Tables 5-2 and 5-3 below to help you select the permissions you want to assign to the selected group.
4. Click **Apply** to validate the selected permissions for the group.

The following tables list permissions and associated features.

Console: Non-Configurable Permissions

Feature	Tab
Sensor Status	Monitoring
System Event Log: Viewing & Refreshing	Monitoring
Management Controller	Maintenance
FRU	Maintenance
Connected Users	Maintenance

Table 5-2. Hardware Console: Non-configurable permissions

Console: Configurable Permissions

Configurable Permission	Feature	Tab
Change Password	Password	Configuration
Date/Time Settings	Date-Time	Configuration
Firmware Update	Firmware Upgrade	Maintenance
IPMI may use SOL payload	Serial-Over-Lan connection (User accounts with this permission can launch a SOL session)	-
LDAP Settings	Security management/Authentication	Configuration
Language Settings		
Maintenance/Board Reset	Hardware Exclusion	Maintenance
Modem Settings	Network	Configuration
Network Settings	Network	Configuration
Power Control	Power Management	Power Control
Power Control Settings	Power Management	Power Control
SNMP Settings	SNMP	Configuration
SSH/Telnet Access	SSH/Telnet connection (User accounts with this permission can send SSH/Telnet commands through the LAN)	-
SSL Certificate Management	SSL Certificate	Configuration
Security/Log/Authentication Settings	Encryption	Configuration
	User Logon Policy	Configuration
	Power Button Lockout	Configuration
	User Lockout	Configuration
Serial Settings		Configuration
Server Status via IPMI		Configuration
User/Group Management	Users	Configuration
	Groups: Management	Configuration
	Groups: Permissions	Configuration

Table 5-3. Hardware Console: Configurable permissions

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

Table 5-4. IPMI: Out-of-Band privileges

5.7.11. Viewing Group Membership

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

Prerequisites

You have **User/Group Management** permission

Procedure

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

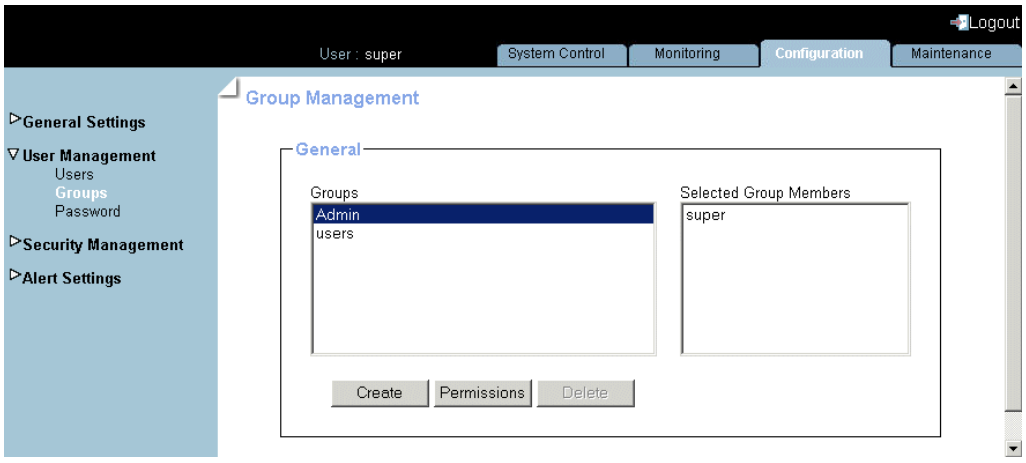


Figure 5-13. Group Management

5.7.12. Deleting a Group

You can delete an empty group when no longer needed.

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

Prerequisites

You have **User/Group Management** permission

No users are members of the group to be deleted, i.e. users have been deleted or moved to another group

Procedure

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

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

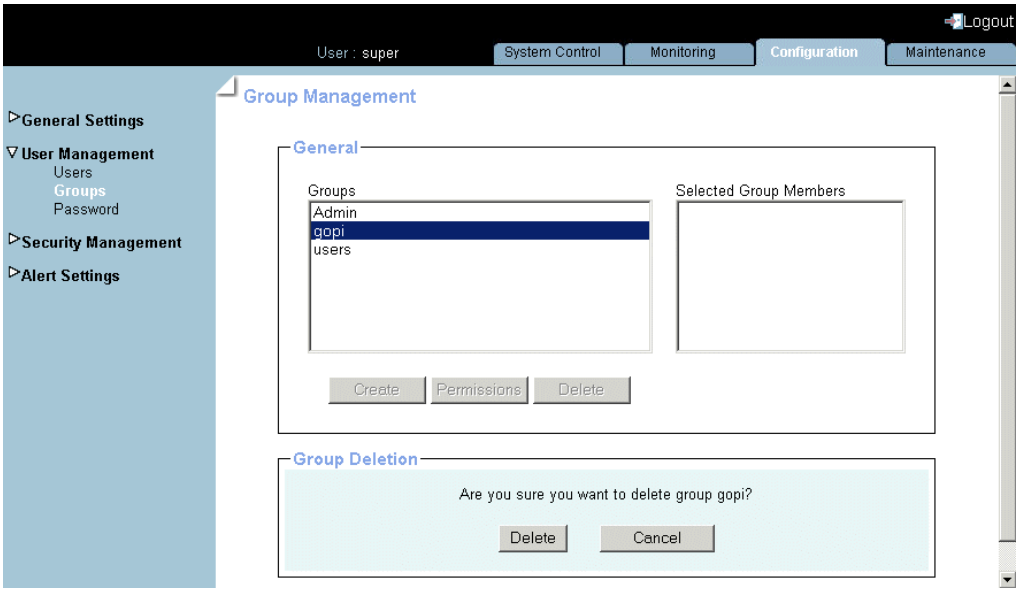


Figure 5-14. Group Management - Group Deletion

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

5.8. Configuring Security Parameters

WARNING

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

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

5.8.1. Forcing HTTPS Connections

This feature allows you to secure Web connections to the console.

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

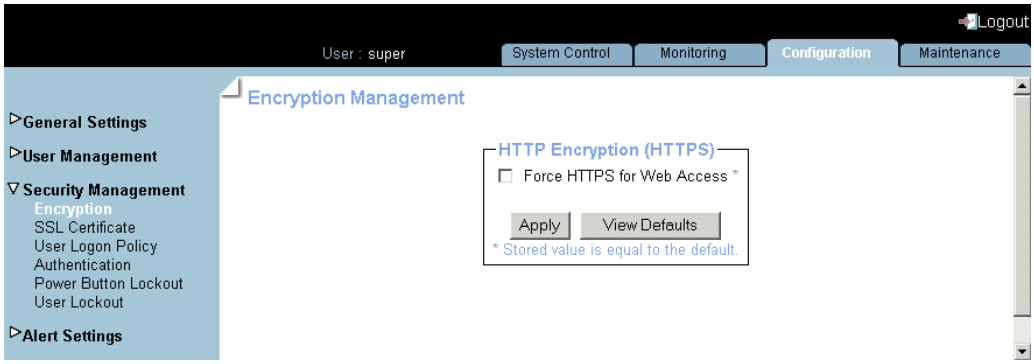
Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 5-3.

Prerequisites

You have Security Settings permission

Procedure

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



	HTTP Encryption (HTTPS)
Force HTTPS for Web Access	The HTTPS protocol requires the use of an URL in one of the following formats: • https://<IP Address> • https://<Hostname> IMPORTANT: if this option is selected, the HTTP protocol (http://<IP address or hostname>) can no longer be used to connect to the console.
Reset to defaults button	Allows you to display factory-default values. Click Apply to restore factory-default configuration.

Figure 5-15. Encryption Management - factory-default values

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

5.8.2. Getting and Installing a New SSL Certificate

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

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

Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 5-3 .

Prerequisites

You have **SSL Certificate Management** permission

Procedure

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

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

Figure 5-16. SSL Certificate Management

2. Complete the fields and click **Create** to generate your CSR.
3. Click **Download** to save the CSR to your chassis and send it to the Certification Authority, which will check your information, generate a signed Certificate and send it back to you.
4. When you receive your signed certificate, use the **Certificate Upload** box to install the certificate.

5.8.3. Configuring the Logon Policy

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

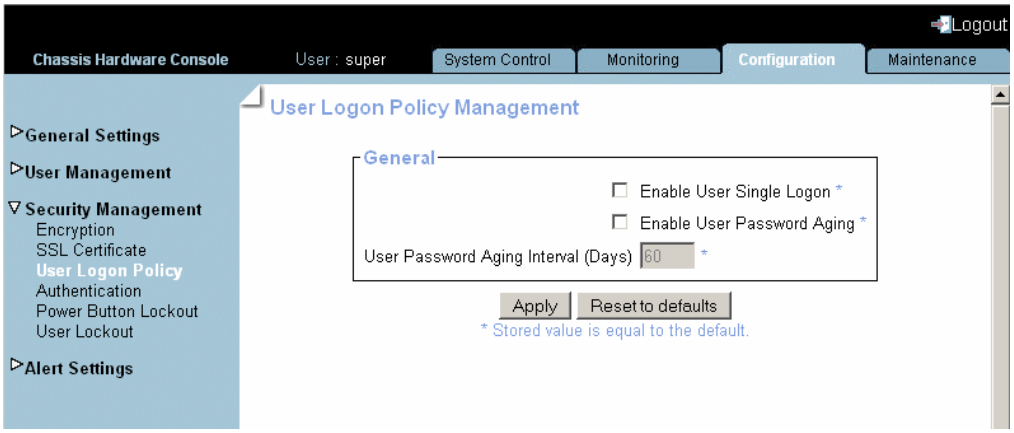
Prerequisites

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

You log on with the user account you want to configure

Procedure

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



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

Figure 5-17. User Logon Policy Management - factory-default values

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

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

Prerequisites

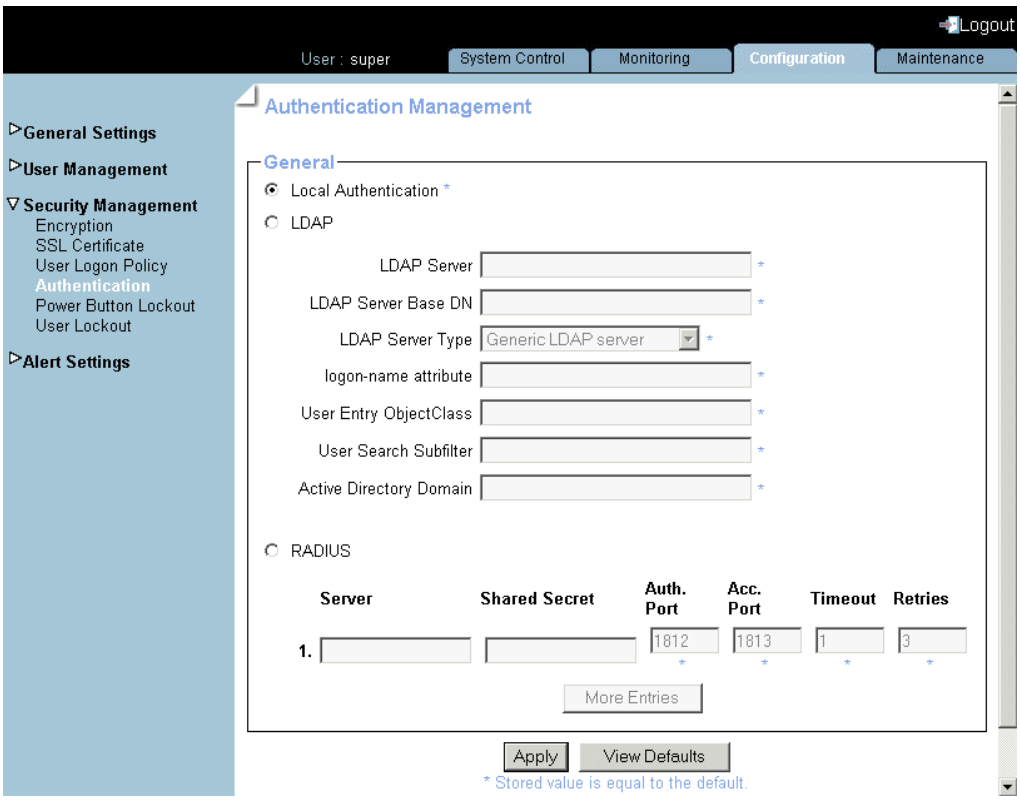
You have **Security/Log/Authentication Settings** permission

For LDAP or RADIUS authentication management, you have configured the DNS server from the **Enterprise Network Settings** page

For RADIUS authentication management, you have declared the console as a RADIUS client (name and IP address) and have defined the shared secret

Procedure

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



General	
Local Authentication	Select to enable local console authentication.
LDAP	Select to enable LDAP server authentication.
• LDAP Server Base DN	Enter the starting node to search for user accounts. Example: dc=users,dc=domain,dc=com
• LDAP Server Type	Enter LDAP server type: • Novell Directory Service if you are using Novell eDirectory. • Microsoft Active Directory. • Generic LDAP Server if you are using any other LDAP directory.
• Logon Name Attribute	If you have selected Novell Directory Service or Microsoft Active Directory, leave these fields blank to use the directory's default value. • Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory Example: cn. • User Entry Object Class: object class that identifies a user in the directory Example: organizationalPerson.
• User-entry ObjectClass	If you have selected Novell Directory Service or Microsoft Active Directory, leave these fields blank to use the directory's default value. • Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory Example: cn. • User Entry Object Class: object class that identifies a user in the directory Example: organizationalPerson.
• User Search Subfilter	Restricts the search to certain user accounts. (example: (&(objectClass=person)(ou=System Validation)))
RADIUS	Select to enable RADIUS authentication
• Server	Enter the RADIUS server 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	Enter the RADIUS server port number used to listen to authentication requests (#1812 by default).
• Acc. Port	Enter the RADIUS server port number used to listen to accounting requests (#1813 by default).
• Timeout (sec.)	Enter the maximum time in seconds to wait for the completion of the request. If the requested job is not completed within this interval of time it is cancelled.

General	
• Retries	Enter the maximum number of retries if a request cannot be completed.
• More Entries	If you use more than one RADIUS server, click this button to add authentication configurations.
View Defaults button	Allows you to display factory-default values. Click **Apply** to restore factory-default configuration.

Figure 5-18. Authentication Settings - factory-default values

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

5.8.5. Configuring Power Button Lockout

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

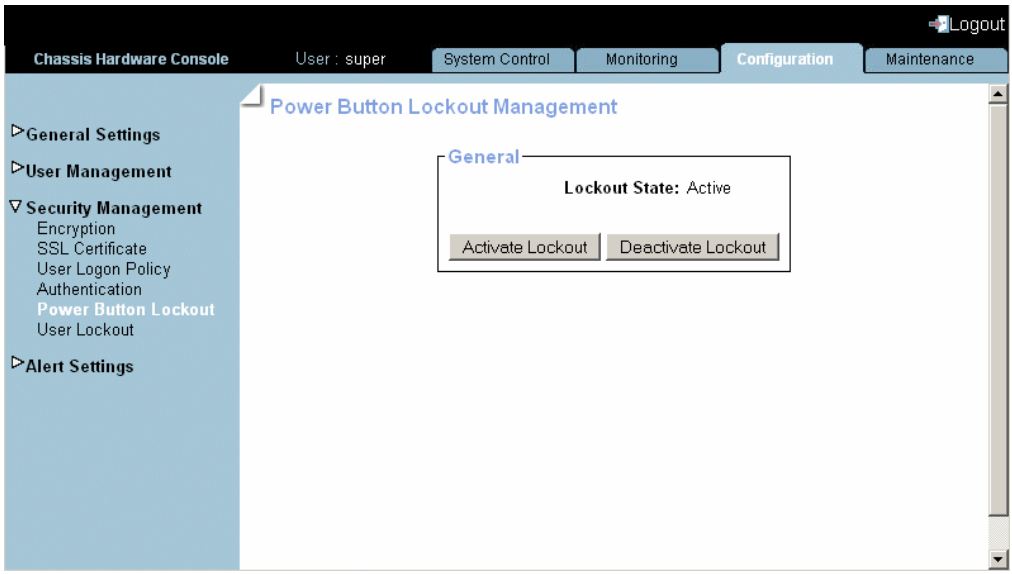
Prerequisites

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

You have logged on with the user account to configure

Procedure

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



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

Figure 5-19. Power Button Lockout Management

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

5.8.6. Configuring User Account Lockout

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

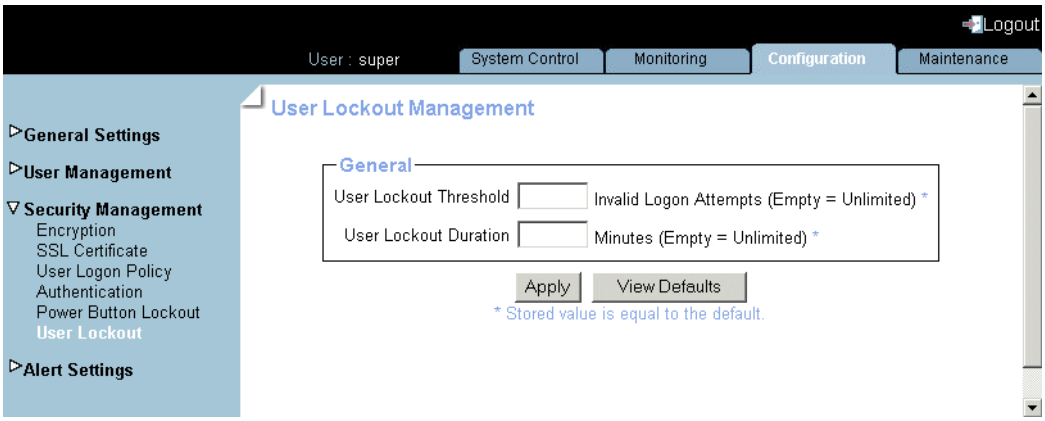
Prerequisites

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

You have logged on with the user account to configure

Procedure

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



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

Figure 5-20. User Lockout Management - factory-default values

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

5.9. Configuring Alerts

WARNING

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

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

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

- Configure the event trap server community string and email server IP and sender addresses. For details, see Configuring SNMP and SMTP Servers, on page 5-44.
- Configure the event trap server IP address(es) and/or email recipient address(es). For details, see Configuring LAN Destinations, on page 5-45.
- Configure the alert transmission policy(ies). For details, see Configuring Alert Policies, on page 5-47.
- Select the events you want to report. For details, see Managing Predefined Event Filters, on page 5-50 and Customizing an Event Filter, on page 5-52.

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

5.9.1. Configuring SNMP and SMTP Servers

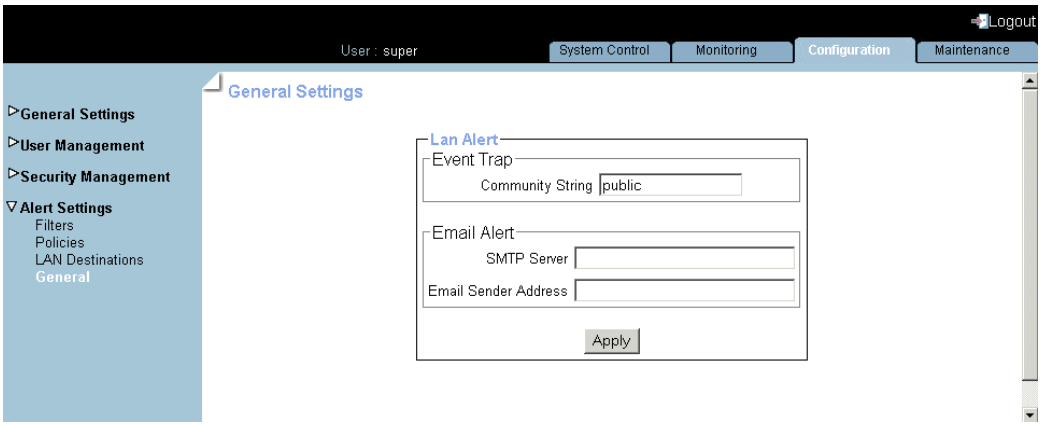
To be able to send events as alerts to SNMP managers and/or email recipients, you need to supply event trap server and email server details.

Prerequisites

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

Procedure

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



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

Figure 5-21. Alert General Settings

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

5.9.2. 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

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

Procedure

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

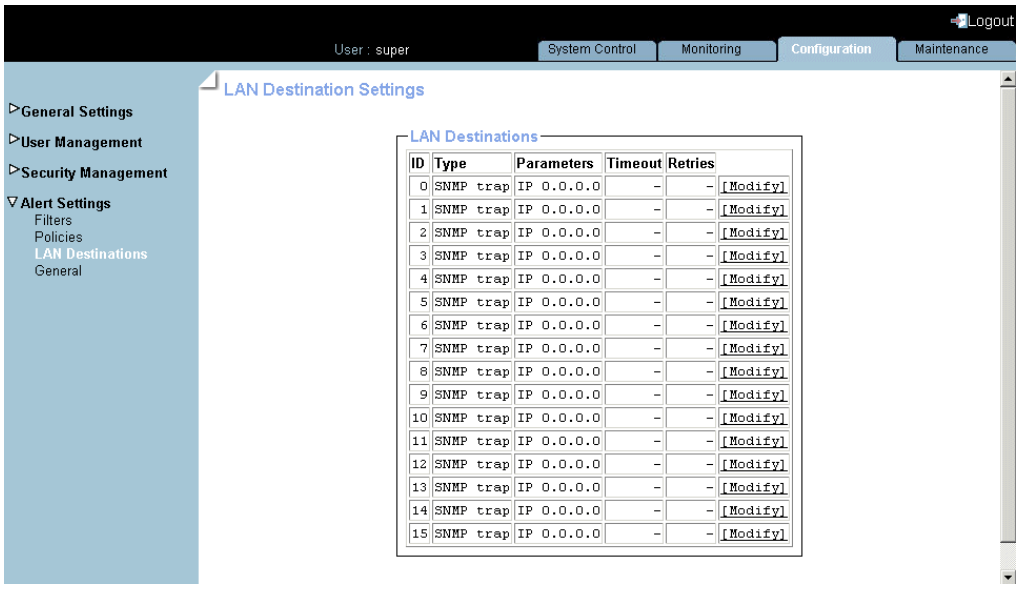
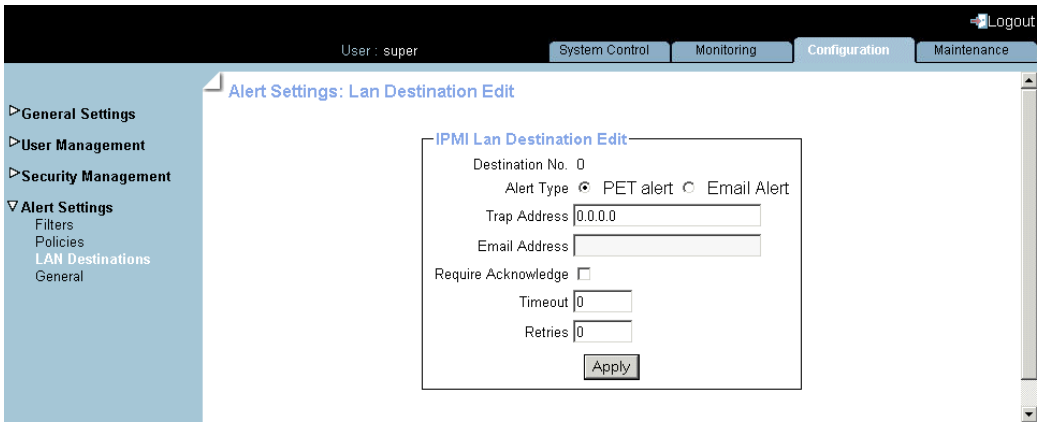


Figure 5-22. LAN Destination Settings

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



IPMI LAN Destination Edit	
Destination Number	Read-only. Predefined number used to identify the destination to which alert messages are to be sent.
Alert Type	Alert messaging format and method: • PET alert (Platform Event Trap): sends a PET alert to the specified trap address. • Email alert: generates an email alert to the specified email address.
Trap Address	PET alerts only. SNMP manager IP address. Example: 192.x.x.x.
Email Address	Email alerts only. Recipient's email address. Example: john.smith@bull.net
Require Acknowledge	PET alerts only. Select if you require alert message acknowledgement.
Timeout	PET alerts only. Time in seconds to wait for acknowledgement before retrying.
Retries	PET alerts only. Number of retries to make before aborting.

Figure 5-23. Alert Settings: LAN Destination Edit

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

5.9.3. Configuring Alert Policies

Alert policies allow you to define alert messaging strategies.

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

Prerequisites

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

Procedure

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

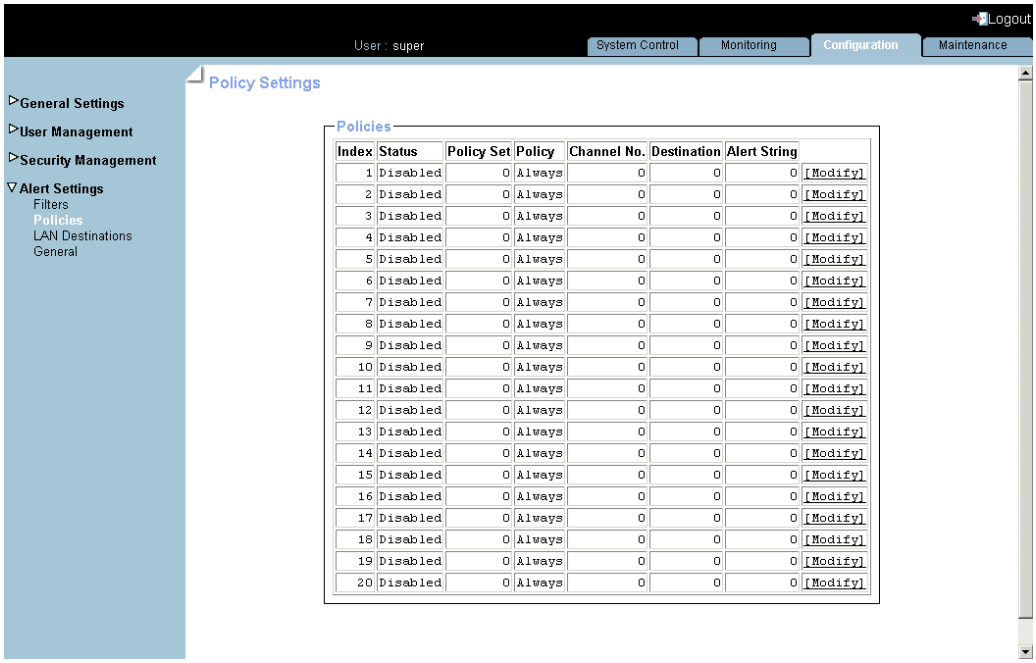
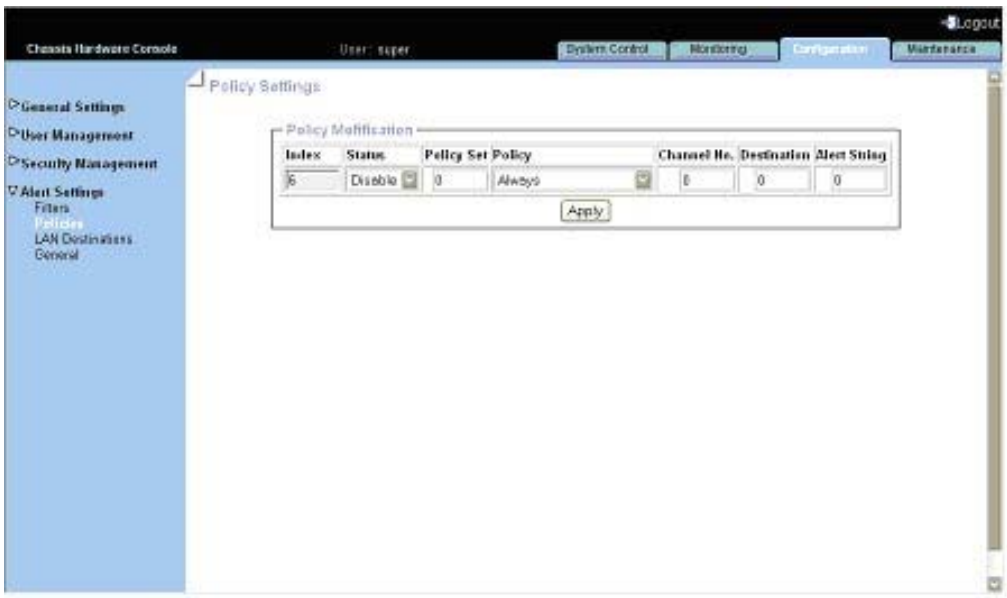


Figure 5-24. Alert policy settings

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



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

Policy Modification	
Policy	This drop-down list allows you to define an event messaging strategy for the current policy. This strategy is dependent on the strategies defined for preceding policies belonging to the same policy set. According to the strategy you want to apply, select one of the following values: • Always: always send the alert to this destination. • Skip this destination: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination in the table. • Stop alerting: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and all subsequent destinations in the table. • Skip to next different destination type: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination using a different transmission method (PET alert vs Email alert).
Channel No.	Read-only
Destination	Enter the predefined number used to identify the destination to which alert messages are to be sent. Note: This number corresponds to the number in the ID column on the LAN Destination Settings page.
Alert String	0 Read-only.

Figure 5-25. Alert policy settings - Modification

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

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

5.9.4. Managing Predefined Event Filters

Several event filters are factory-predefined and enabled by default. These predefined filters, listed in the Filter Table, cover all potential events. They cannot be modified, but can be enabled/disabled according to your needs. **The last filter in the list of predefined filters covers ALL events.**

For details, refer to .

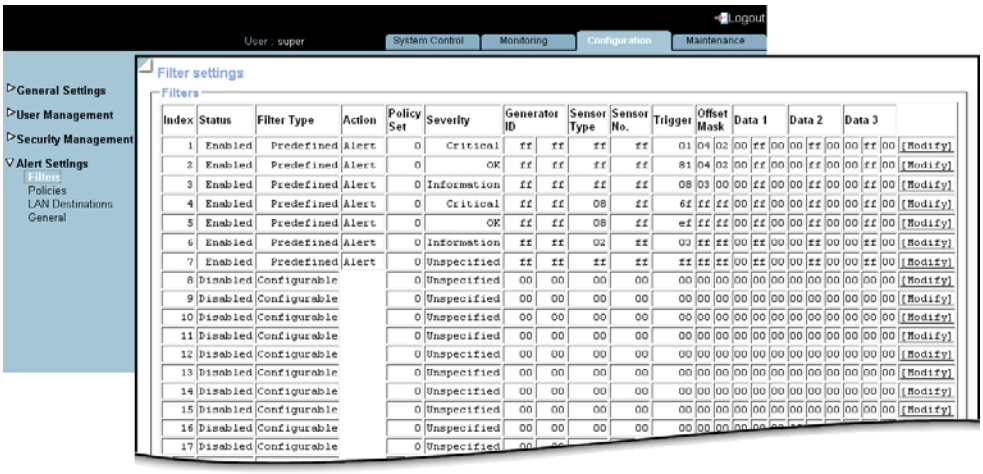
Note You can also define custom or "configurable" event filters. This is an advanced option. For details about advanced alert transmission options, you may consult the official *IPMI Specification* and Customizing an Event Filter, on page 4-5.

Prerequisite

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

Procedure

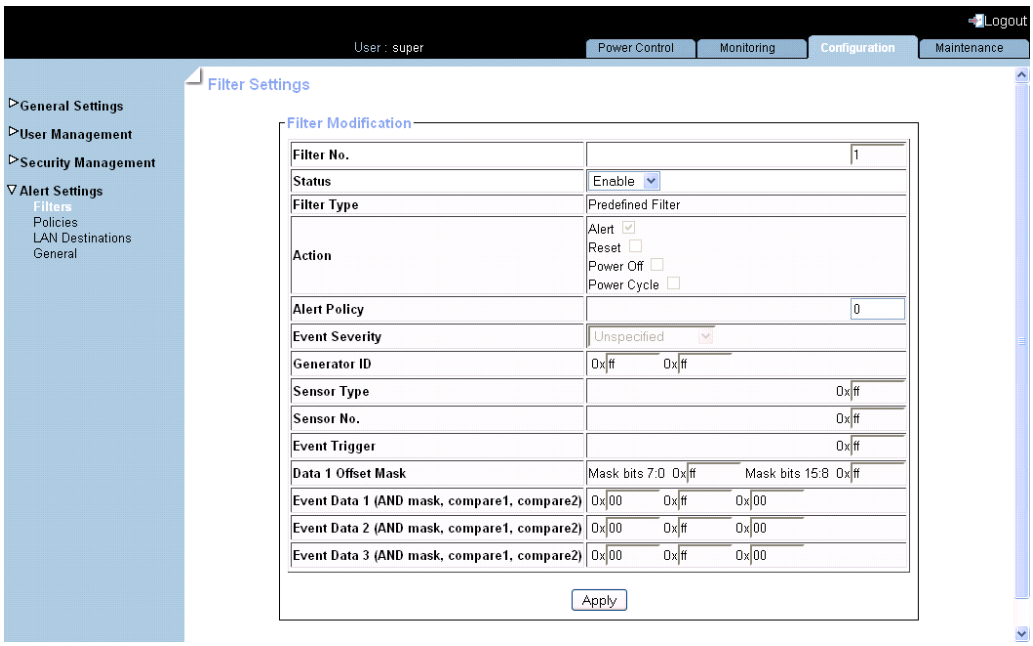
1. From the **Configuration** tab, click **Alert Settings > Filters** to display the **Filter Settings** page.



Index	Status	Filter Type	Action	Policy Set	Severity	Generator ID		Sensor Type	Sensor No.	Trigger	Offset Mask		Data 1		Data 2		Data 3		
1	Enabled	Predefined	Alert	0	Critical	ff	ff	ff	ff	01	04	02	00	ff	00	00	ff	00	[Modify]
2	Enabled	Predefined	Alert	0	OK	ff	ff	ff	ff	81	04	02	00	ff	00	00	ff	00	[Modify]
3	Enabled	Predefined	Alert	0	Information	ff	ff	ff	ff	08	03	00	ff	00	00	ff	00	00	[Modify]
4	Enabled	Predefined	Alert	0	Critical	ff	ff	08	ff	6f	ff	ff	00	ff	00	00	ff	00	[Modify]
5	Enabled	Predefined	Alert	0	OK	ff	ff	08	ff	ef	ff	ff	00	ff	00	00	ff	00	[Modify]
6	Enabled	Predefined	Alert	0	Information	ff	ff	02	ff	03	ff	ff	00	ff	00	00	ff	00	[Modify]
7	Enabled	Predefined	Alert	0	Unspecified	ff	ff	ff	ff	ff	ff	ff	00	ff	00	00	ff	00	[Modify]
8	Disabled	Configurable		0	Unspecified	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	[Modify]
10	Disabled	Configurable		0	Unspecified	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	[Modify]
12	Disabled	Configurable		0	Unspecified	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	[Modify]
14	Disabled	Configurable		0	Unspecified	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	[Modify]
16	Disabled	Configurable		0	Unspecified	00	00	00	00	00	00	00	00	00	00	00	00	00	[Modify]
17	Disabled	Configurable		0	Unspecified	00	00												

Figure 5-26. Managing predefined filters

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



Filter Modification	
Filter No.	Read-only, according to order in the Filter List.
Status	Two possible values: • Disable (default value): the filter is not taken into account when an event occurs. • Enable: the action specified in the Action field is executed if an event matches filter parameters.
Filter Type	Read-only: Predefined Filter
Action	Read-only: Alert. • Alert: the event is sent to the specified destination(s) (for details, see Configuring LAN Destinations, on page 5-45) • Reset: the chassis is reset. • Power Off: the chassis is powered down. • Power Cycle: the chassis is restarted.
Alert Policy	Read-only: 0.
Event Severity	Read-only, according to predefined severity.
Generator ID	Read-only. For further details, you may consult the official *IPMI Specification.*
Sensor Type	
Sensor No.	
Event Trigger	
Data 1 Offset Mask	
Event Data 1 (AND mask, compare1, compare2)	
Event Data 2 (AND mask, compare1, compare2)	

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

Figure 5-27. Modifying predefined filters

3. In the **Status** drop-down list, select either **Enable** or **Disable** depending on your needs and click **Apply**.

5.9.5. Customizing an Event Filter

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

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

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

Prerequisites

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

Procedure

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

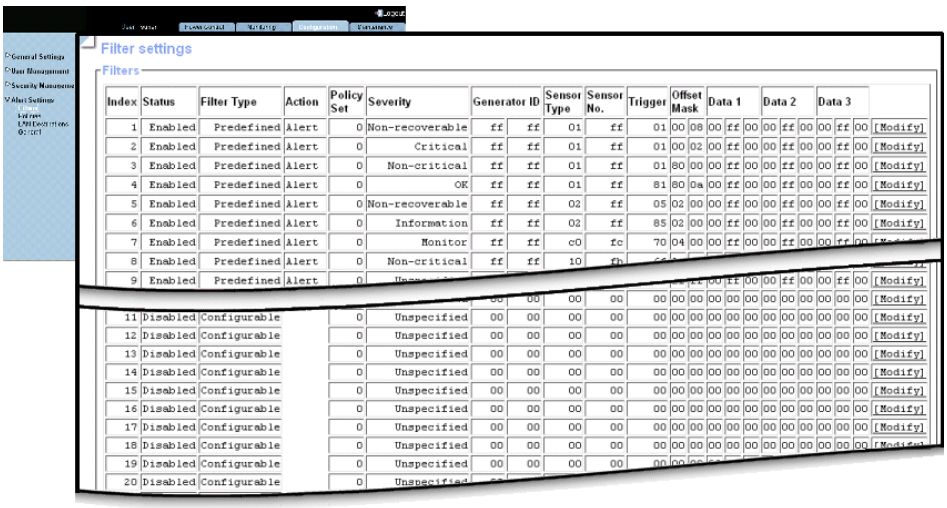
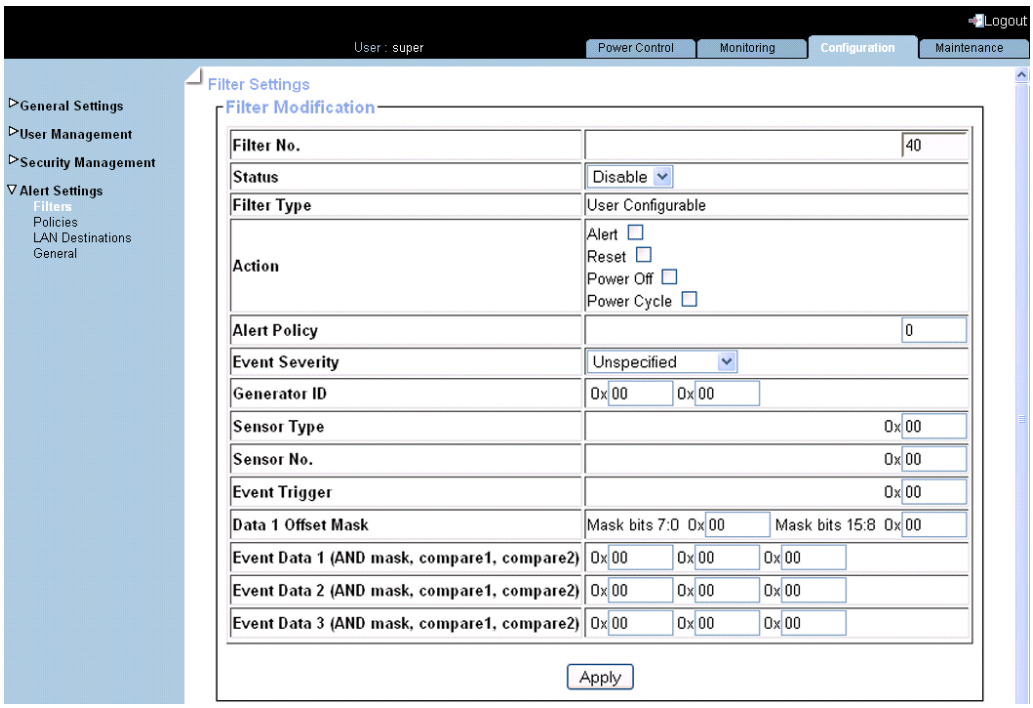


Figure 5-28. Customizing an event filter

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



Filter Modification	
Filter No.	Filter number (read-only field).
Status	Two possible values: • Disable (default value): the filter is not taken into account when an event occurs. • Enable: the action specified in the Action field is executed if an event matches filter parameters.
Filter Type	This read-only field displays User Configurable to specify that you are editing a configurable event filter.
Action	Possible values: • Alert: the event is sent to the specified destination(s) (for details, see Configuring LAN Destinations, on page 5-45) • Reset: the chassis is reset. • Power Off: the chassis is powered off. • Power Cycle: the chassis is powered off then powered on.
Alert Policy	Default value: 0. Policies can be grouped into different policy sets, if required. This is a feature for advanced users. Only one policy set, Policy Set 0, is implemented for the predefined event filters. For details about advanced alert transmission options, you may consult the official *IPMI Specification*.
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. For further details, you may consult the official *IPMI Specification* or your Customer Representative.
Sensor Type	
Sensor No.	
Event Trigger	
Data 1 Offset Mask	
Event Data 1 (AND mask, compare1, compare2)	
Event Data 2 (AND mask, compare1, compare2)	
Event Data 3 (AND mask, compare1, compare2)	

Figure 5-29. Configurable Filters - Modification

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

Chapter 6. Using Maintenance Features

This chapter explains the maintenance operations you can perform from the console and using the utilities provided on the *Resource and Documentation CD*. It includes the following topics:

6.1. Getting Management Controller Information

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

Procedure

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

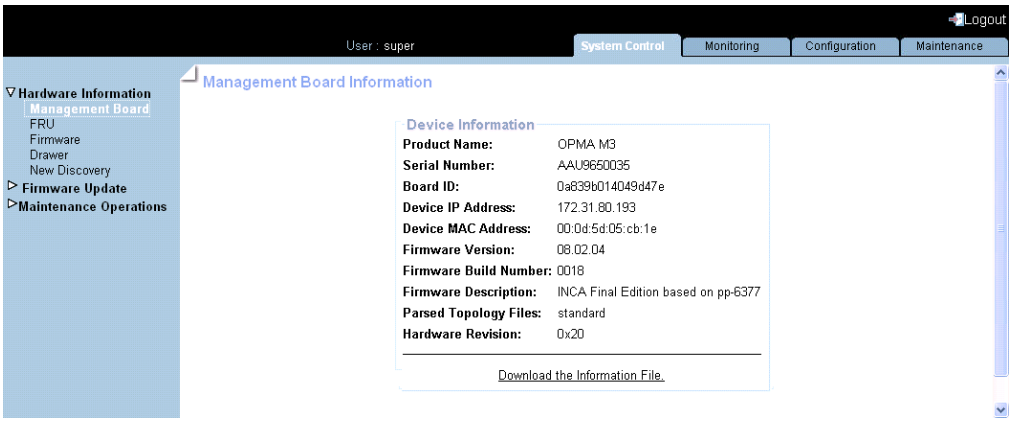


Figure 6-1. Management Controller Information

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

6.2. Getting FRU Information

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

Procedure

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

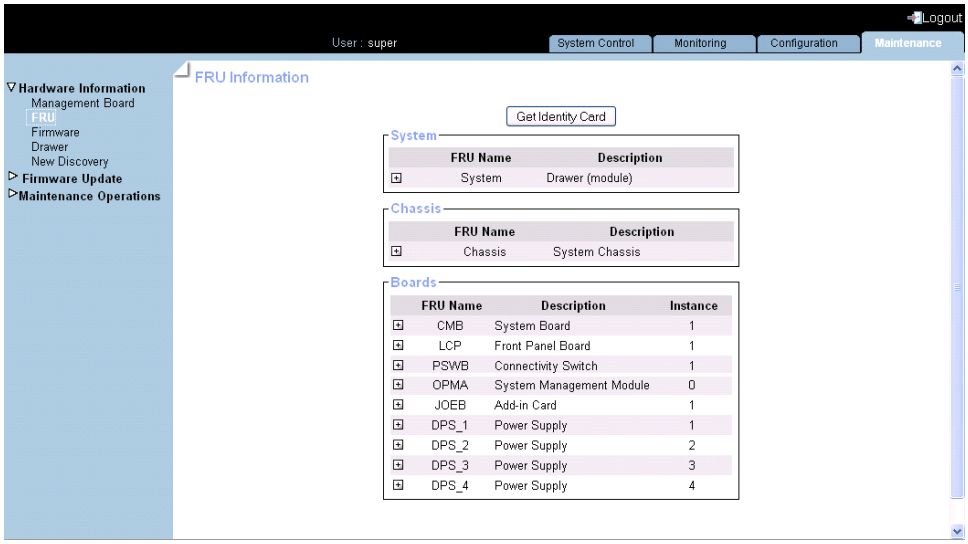


Figure 6-2. FRU Information

Note The plus button next to a FRU name indicates that the line can be expanded to show more information on the FRU.

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

6.3. Displaying Firmware Versions

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

Procedure

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

Figure 6-3. Viewing Firmware Information - Server Example

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

6.4. Getting Drawer Information

This section provides information for the following components:

- Blades
- LCP
- IBSwitch (QSM)
- UCM
- ESM

Procedure

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

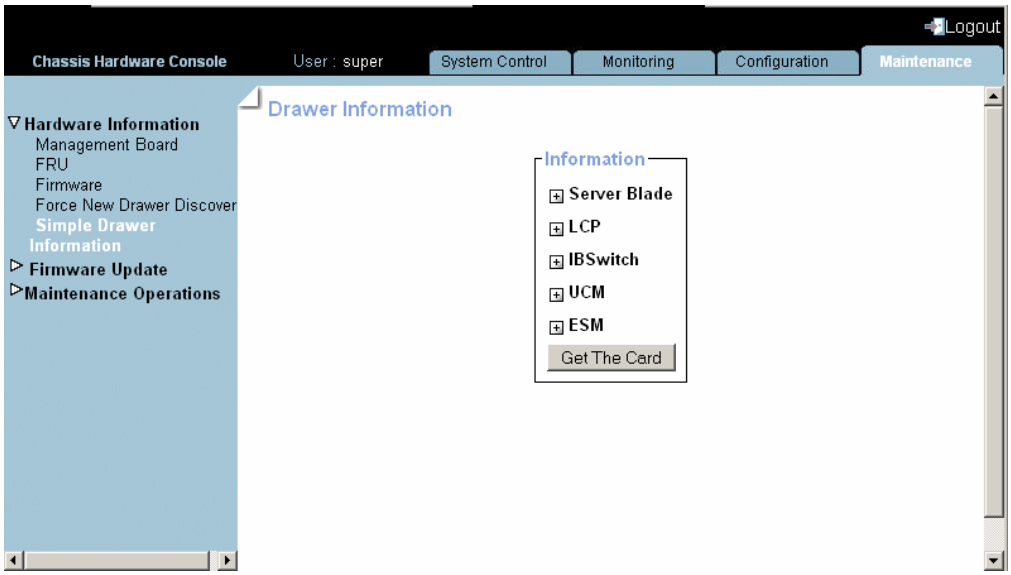


Figure 6-4. Drawer Information page

2. To save blade information to an HTML file, click **Download the Blade information file**.

6.5. Updating Firmware

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

- Local Control Panel (LCP)
- Chassis Management Controller (CMC)

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

6.6. Resetting the Management Board

Prerequisites

Viewing: All users

Operations: root users

Procedure

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

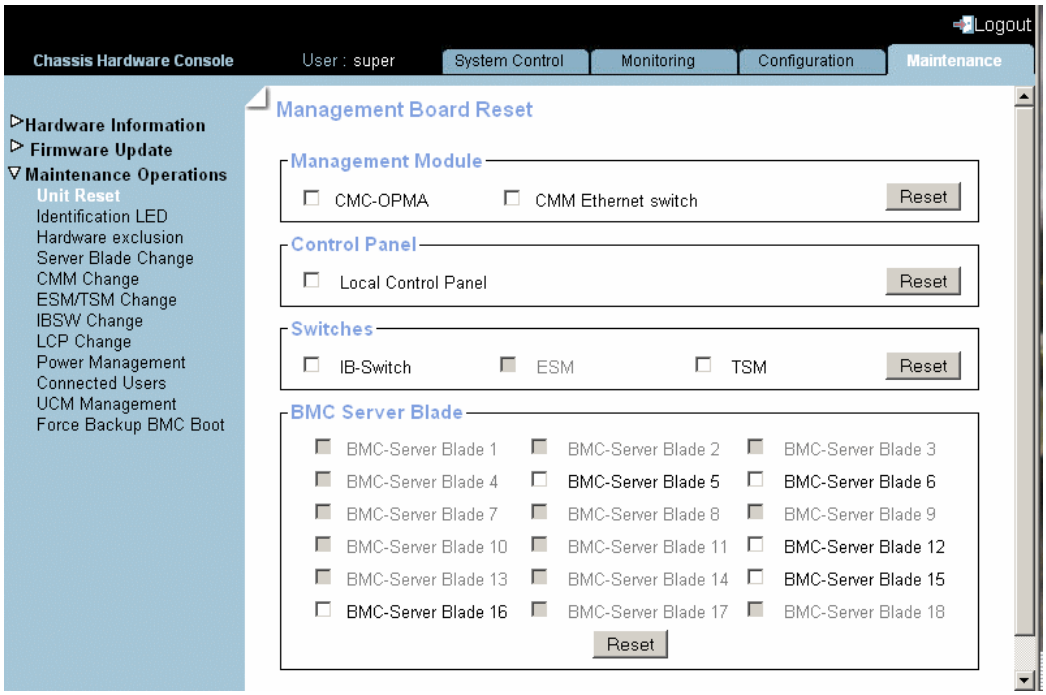


Figure 6-5. Management Board Reset page

Management Board Reset page description	
Management Module	CMC-OPMA
Control Panel	Local Control Panel
Switches	IB-Switch (QSM)
	ESM/TSM
BMC-Server Blade	Blade numbers

Table 6-1. Management Board Reset page description

2. Select/Clear the box(es) as required and click **Reset**.

6.7. Enabling/Disabling LEDs

Prerequisites

Viewing: All users

Operations: Admin group users

Procedure

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

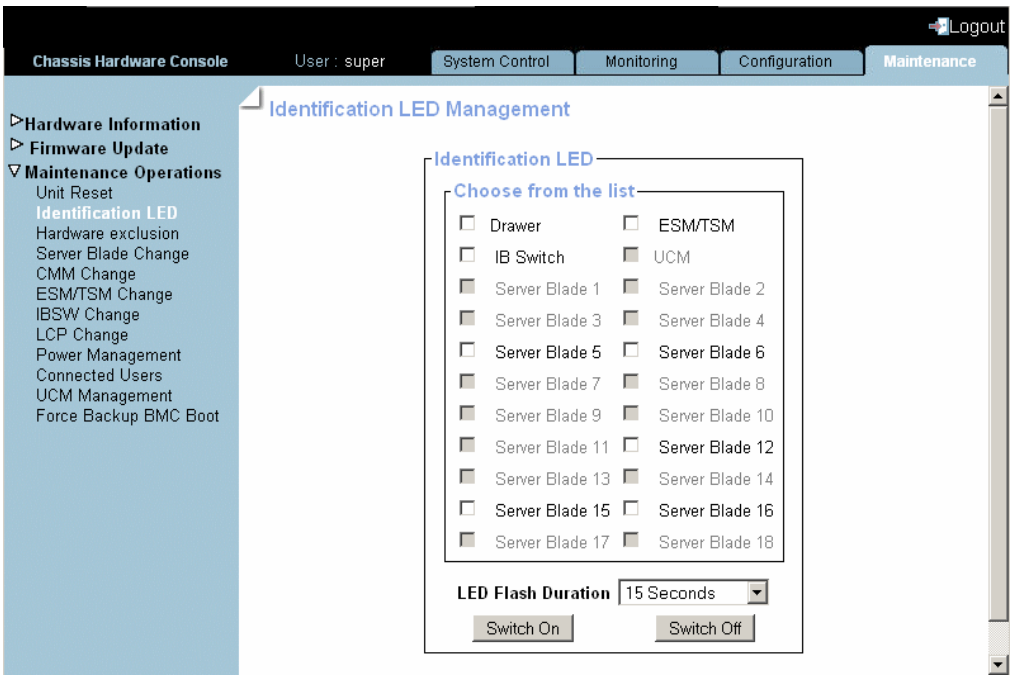


Figure 6-6. Identification LED Management page

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/Including Computing Elements

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

Prerequisites

You have Maintenance/Board Reset permission

Procedure

1. From the Maintenance tab, click Maintenance Operations > Hardware Exclusion to display the Hardware Exclusion Management page.

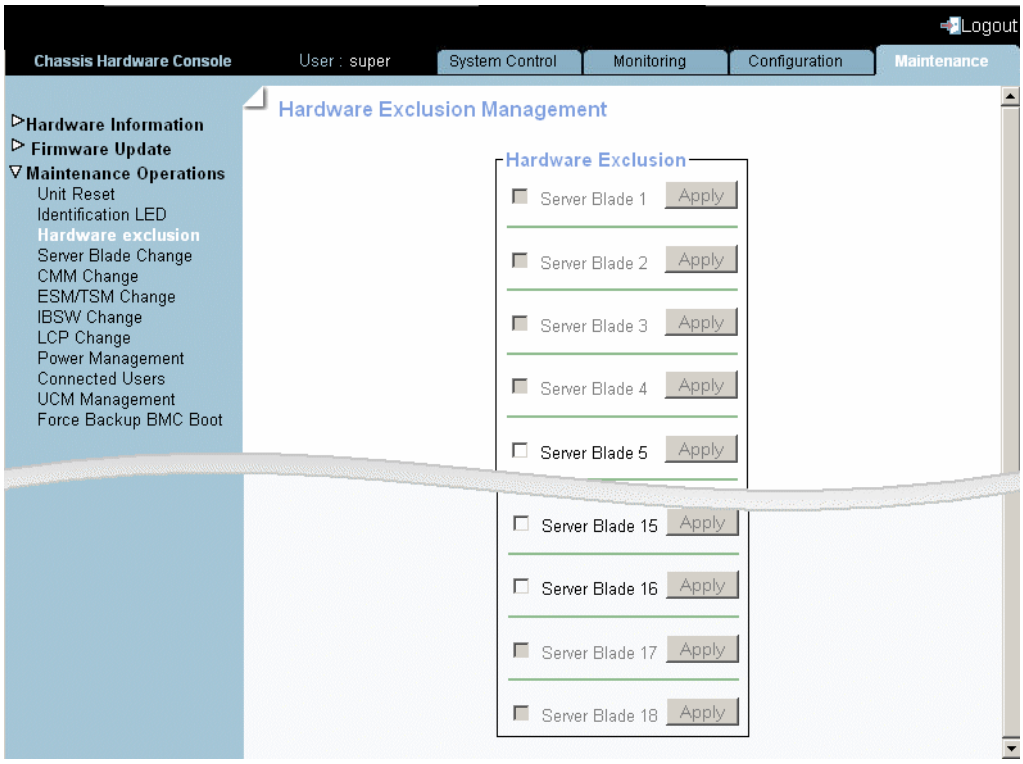


Figure 6-7. Hardware Exclusions

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

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

6.9. Managing Blades

You can manage the removal/insertion of blades for servicing operations.

Note For information on servicing the blades, see the related *Service 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.

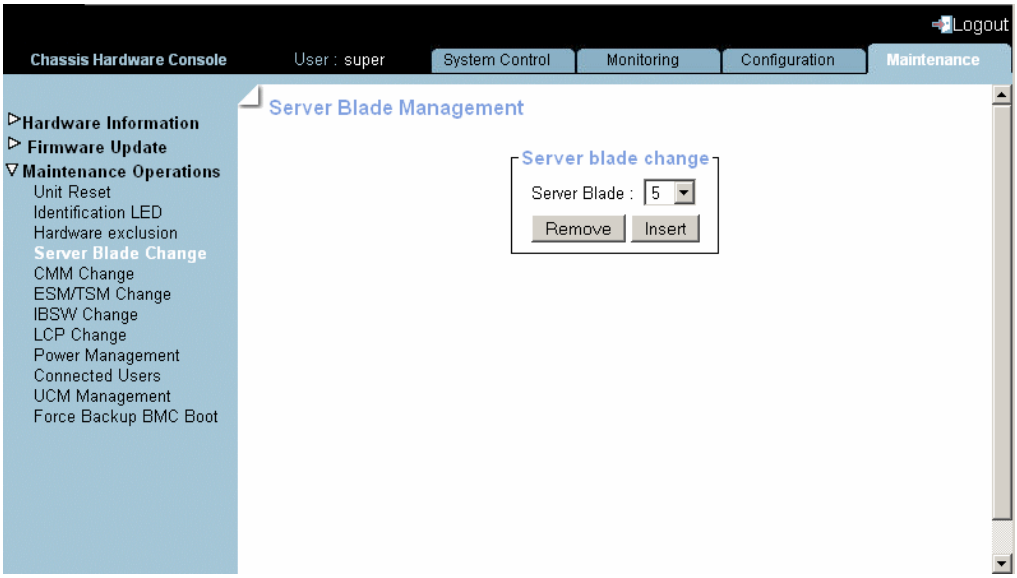


Figure 6-8. Blade Management page

2. Select the **Blade** number from the drop-down.
3. Click **Remove/Insert** as required.
4. If the operation is to remove, blade should be in power off state, otherwise warning will be displayed. If the blade is in off state then ID LED will start blinking.

6.10. Managing the CMM

You can manage the removal/insertion of the CMM for servicing operations.

Note For information on servicing the CMM, see the related *Service 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.

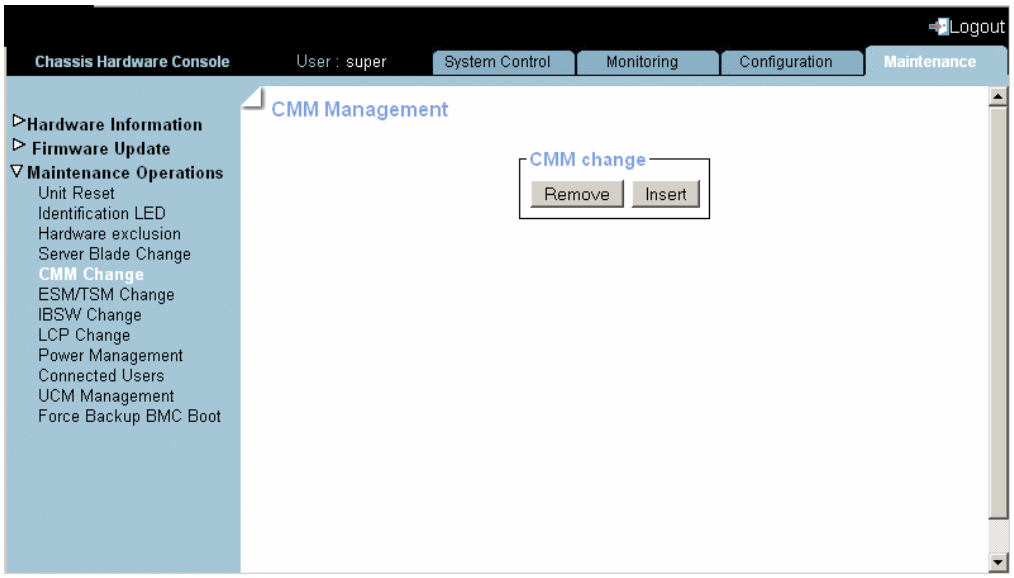


Figure 6-9. CMM Management page

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

6.11. Managing the LCP

You can manage the removal/insertion of the LCP for servicing operations.

Note For information on servicing the LCP, see the related *Service Guide*.

Prerequisites

Viewing: All users

Operations: root users

Procedure

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

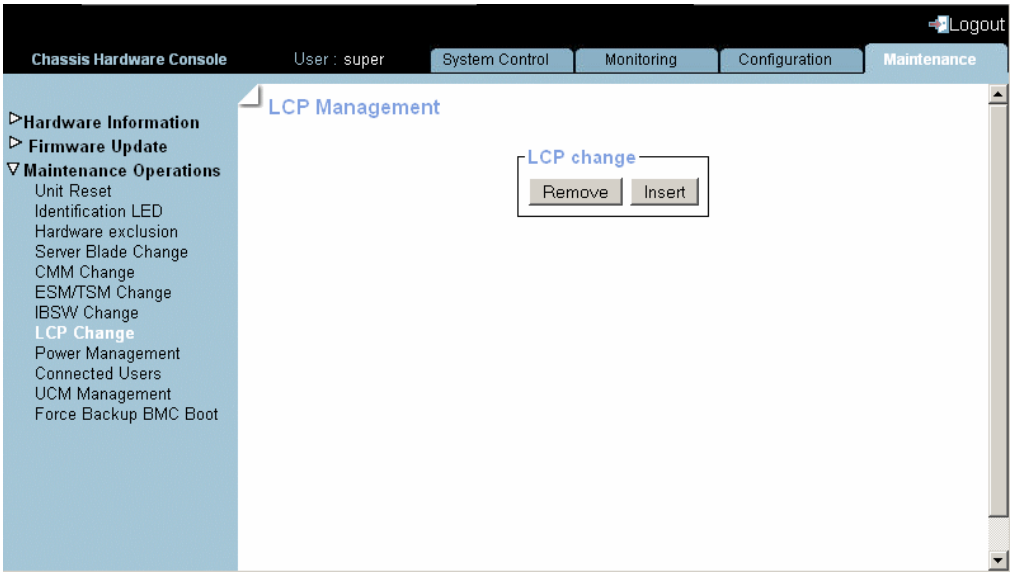


Figure 6-10. LCP Management page

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

6.12. Managing the QSM

You can manage the removal/insertion of the QSM (IBSW Switch) for servicing operations.

Note For information on servicing the QSM, see the related *Service 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.

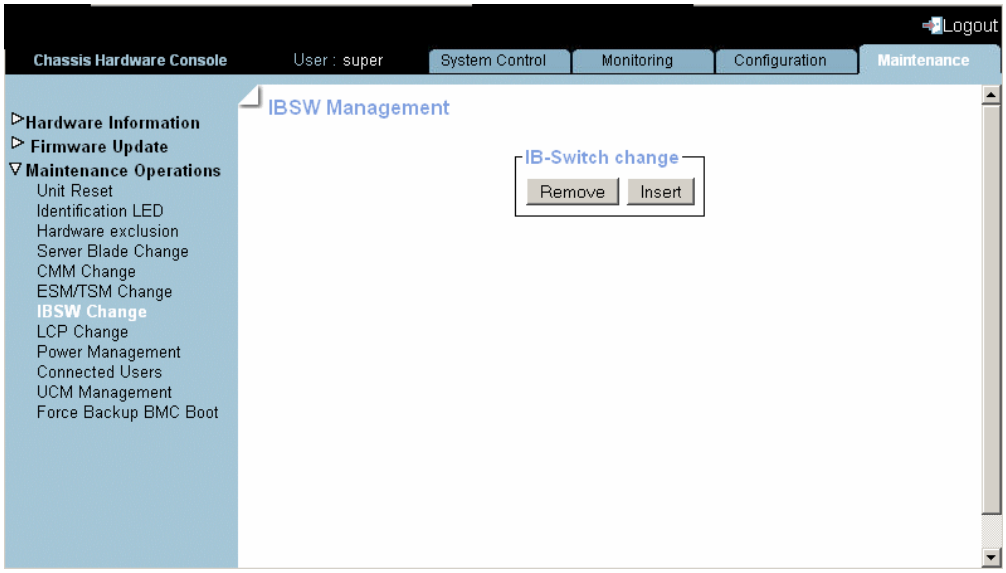


Figure 6-11. IBSW Management page

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

6.13. Managing the ESM/TSM

You can manage the removal/insertion of the ESM / TSM for servicing operations.

Note For information on servicing the ESM / TSM, see the related *Service Guide*.

Prerequisites

Viewing: All users

Operations: root users

Procedure

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

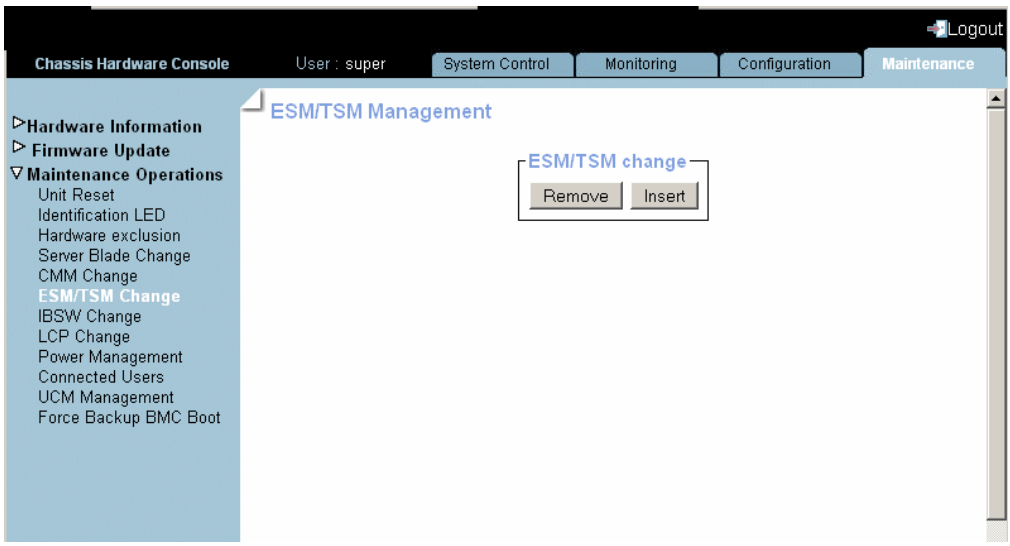


Figure 6-12. ESM / TSM Management page

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 (QSM) power used to perform routine power on/off sequences
- TSM power used to perform routine power on/off sequences

Prerequisites

Viewing: All users

Operations: Admin group users

Procedure

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

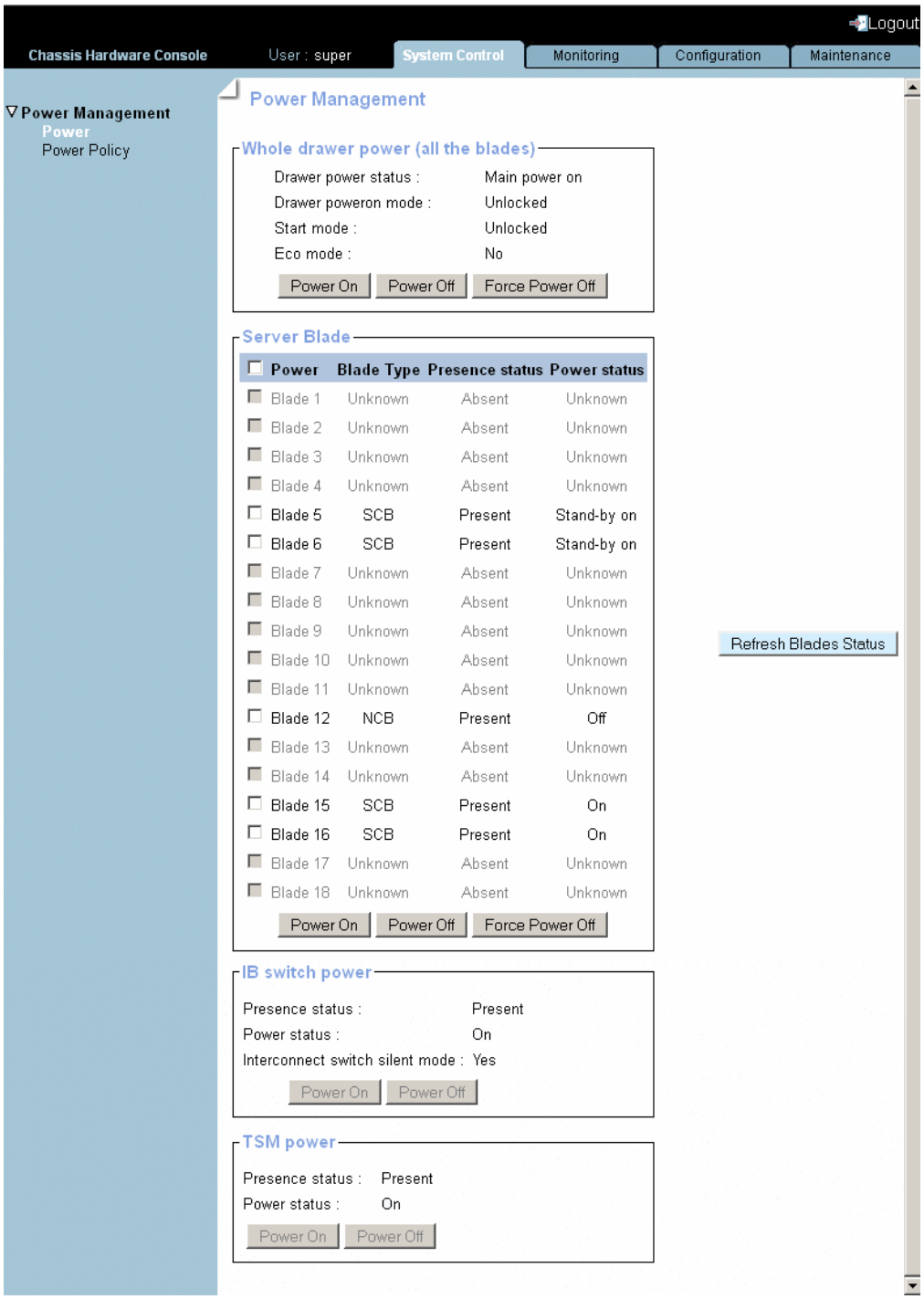


Figure 6-13. Power Management page

Whole drawer power	
Drawer power status	Provides the status of drawer power. • **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 poweron mode	Provides the status of drawer poweron mode. • **Full power on**: This means all the blades and other boards are powered on when the drawer powering on is launched • **Unlocked**: This means all the blades and other boards are unlocked (12 V hot swap enabled) when the drawer powering on is launched
Start mode	Provides the status of start mode. • **Deep Stand-by**: In this mode, the blade stays in stand-by off state (i.e. BMC not running) • **Light Stand-by**: In this mode, the blade state becomes stand-by on (i.e. the BMC will be running) • **Unlocked Power**: In this mode, the blade state becomes Off (i.e. the BMC will be running and the 12V power enabled)
Eco mode	Provides the status of Eco mode. • **Yes**: This forces drawer to silent mode. (The drawer can be configured to save the energy when the 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	Blade number.
Presence status	• **Present**: The corresponding blade is present • **Absent**: Server corresponding blade is absent
Power status	• **Off**: The corresponding blade is powered Off • **On**: The corresponding blade is powered On • **Unknown**: The corresponding blade is absent

IB switch (QSM) power	
Presence status	Provides the presence status of the Quad Switch Module. • **Absent**: the Quad Switch Module is absent • **Present**: the Quad Switch Module is present
Power status	Provides the power status of the Quad Switch Module. • **Unknown**: the Quad Switch Module is absent • **Stand-by off**: the Quad Switch Module is powered Off • **On**: the Quad Switch Module is powered On
Interconnect switch silent mode	Provides the status of the Interconnect Switch silent mode. • **Yes**: the IB switch & TSM silent mode is set to silent • **No**: the IB switch & TSM can be explicitly powered on/off
TSM power	
Presence status	Provides the presence status of the 10 Gigabit Ethernet Switch Module. • **Absent**: the TSM is absent • **Present**: the TSM is present
Power status	Provides the power status of the 10 Gigabit Ethernet Switch Module. • **Unknown**: the TSM is absent • **Stand-by off**: the TSM is powered Off • **On**: the TSM is powered On

Figure 6-14. Power Management page

2. Click the buttons as required.

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

6.15. Displaying Connected Users

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

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

Procedure

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

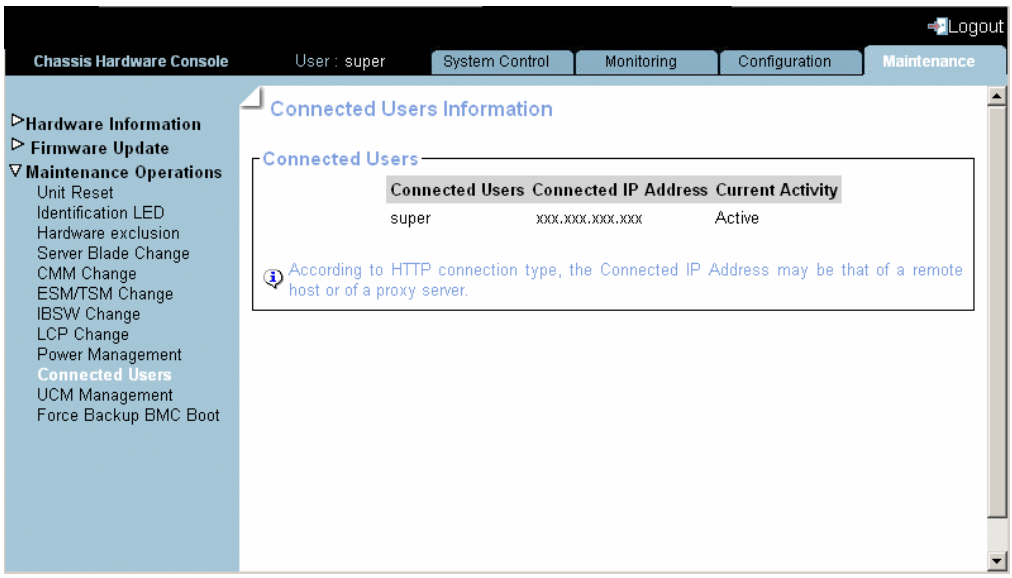


Figure 6-15. Connected Users Information

6.16. Managing the UCM

DANGER

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

UCM Status policies provide the information of Capacitor state, Charger state, Current mode, failure status and Last test result.

Prerequisites

Viewing: All users

Operations: root users

Procedure

From the **Maintenance** tab, expand **Maintenance Operations**, and click **UCM Management** to open the **Ultra Capacitor Module Management** page.

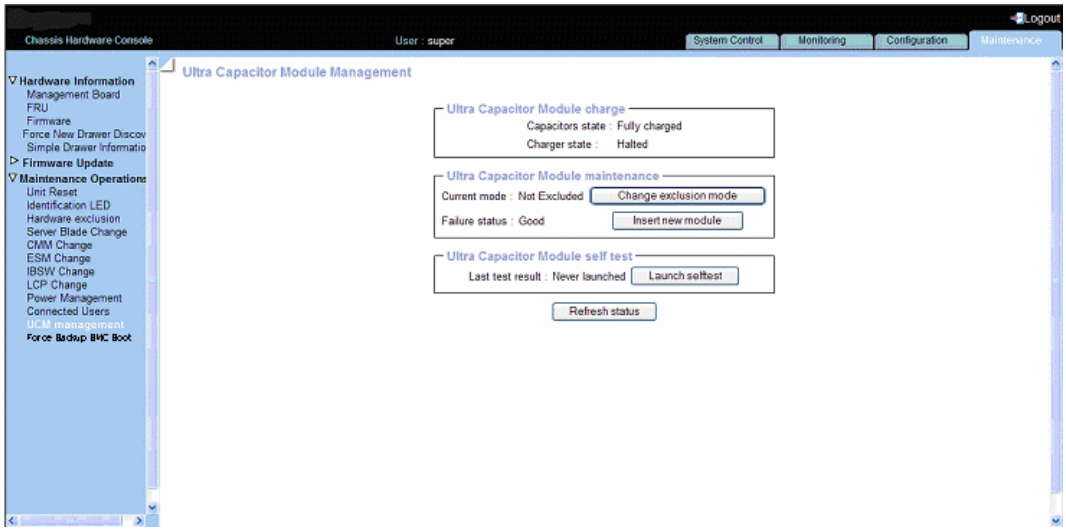


Figure 6-16. Ultra Capacitor Module management

Ultra Capacitor Module Status	
Capacitor state	Provides the status of the capacitor. Depends upon the charge level in the UCM capacitor stack.
Charger state	Provides the status of the the charger. Current UCM charging status.
Current mode	Provides the status of the current mode. UCM exclusion / inclusion status.
Failure status	Provides the status of the failure. • **Fail**: a failure has been detected in the UCM. • **Good**: The UCM is operating correctly.
Last test result	Provides the status of the last test. Last UCM self test result.

Table 6-2. UCM management box description

6.17. Force Backup BMC Boot

You can force a blade BMC to boot from the backup image in case of error on the current boot image.

Prerequisites

Viewing: All users

Operations: root users

Procedure

1. From the **Maintenance** tab, expand **Maintenance Operations**, and click **Force Backup BMC Boot** to open the **Force Backup BMC Boot Management** page.

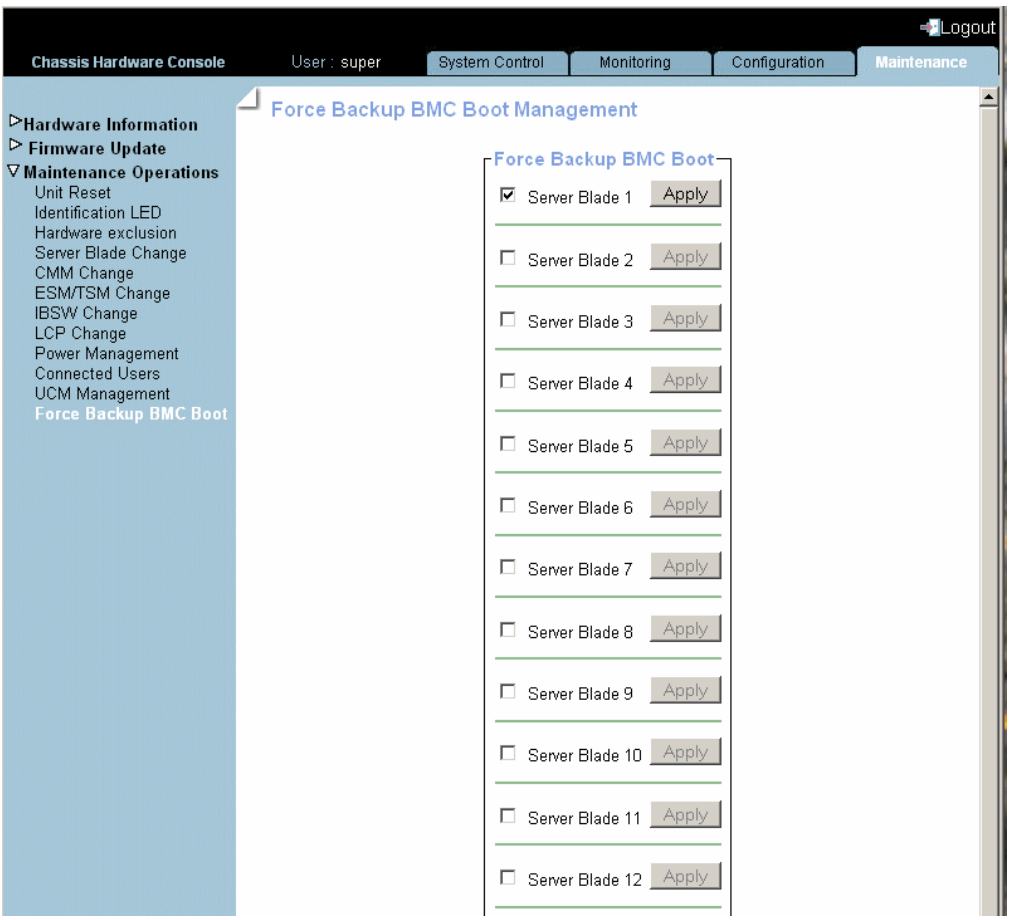
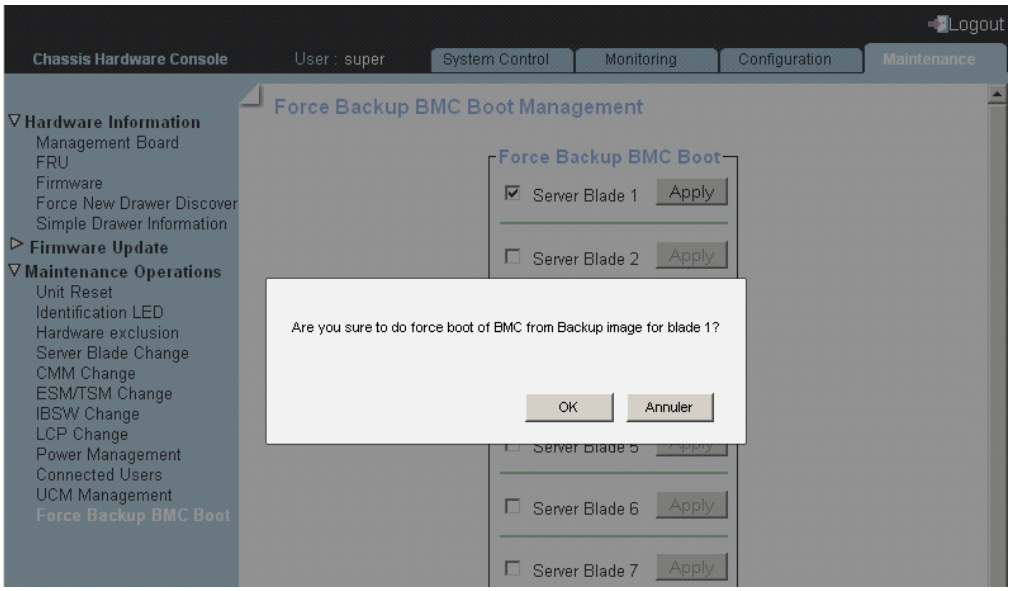
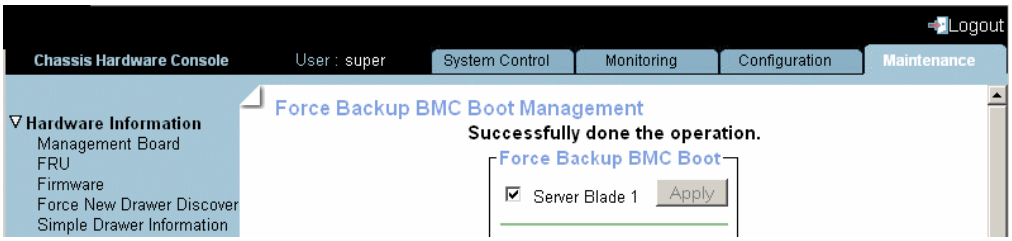


Figure 6-17. Force Backup BMC Boot Management

2. Select the blade you want BMC to boot from the backup image and click **Apply**. You are asked to confirm. Click **OK**.



3. The operation is confirmed by the following message: “Successfully done the operation”.



Appendix A. Specifications

The values indicated in the following table are provided for informational purposes only. These values are not contractual and are subject to change without prior notice.

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

Table A-1. Specifications

Appendix B. Troubleshooting the Blade System

This appendix decribes how to troubleshoot the blade drawer. It includes the following topics:

B.1. Chassis Predefined Alert Filters Description

This section lists chassis predefined event filters. A set of predefined filters, covering all the hardware events likely to occur during system operation, are available for the transmission of alerts to an SNMP Trap Manager or to an email recipient.

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

Component Type	Filter Index
Chassis Management Module (CMM)	1
Ethernet Switch Modules (ESM/TSM)	2
Local Control panel (LCP)	5
Quad Switch Module (QSM)	6, 29
Fan device	7 to 10
Blades	11 to 28, 35 to 70
Ultra Capacitor Module (UCM)	30, 208 to 217
Power Supply Unit (PSU)	31 to 34, 71 to 73, 76 to 92
Drawer Power	75

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.

N°	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.
1	CMM	CMM Temperature (0x01)	At or above upper critical threshold (going high).	Critical	The CMM temperature is upper than the maximum.
1	CMM	CMM Temperature (0x01)	At or below lower critical threshold (going low).	Return to OK	The CMM temperature is now OK.
1	CMM	CMM Temperature (0x01)	At or above upper critical threshold (going high).	Return to OK	The CMM temperature is now OK.
2	ESM / TSM	ESM / TSM Temperature (0x02)	At or below lower critical threshold (going low).	Critical	The ESM / TSM temperature is lower than the minimum.
2	ESM / TSM	ESM / TSM Temperature (0x02)	At or above upper critical threshold (going high).	Critical	The ESM / TSM temperature is upper than the maximum.
2	ESM / TSM	ESM / TSM Temperature (0x02)	At or below lower critical threshold (going low).	Return to OK	The ESM / TSM temperature is now OK.
2	ESM / TSM	ESM / TSM Temperature (0x02)	At or above upper critical threshold (going high).	Return to OK	The ESM / TSM temperature is now OK.
5	LCP	LCP Temperature (0x05)	At or below lower critical threshold (going low).	Critical	The LCP temperature is lower than the minimum.
5	LCP	LCP Temperature (0x05)	At or above upper critical threshold (going high).	Critical	The LCP temperature is upper than the maximum.
5	LCP	LCP Temperature (0x05)	At or below lower critical threshold (going low).	Return to OK	The LCP temperature is now OK.
5	LCP	LCP Temperature (0x05)	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.
6	IBSW	IBSW Temperature (0x06)	At or above upper critical threshold (going high).	Critical	The IBSW temperature is upper than the maximum.
6	IBSW	IBSW Temperature (0x06)	At or below lower critical threshold (going low).	Return to OK	The IBSW temperature is now OK.
6	IBSW	IBSW Temperature (0x06)	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.
7	FAN 1A	FAN 1A Speed (0x07)	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
7	FAN 1A	FAN 1A Speed (0x07)	At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
7	FAN 1A	FAN 1A Speed (0x07)	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
8	FAN 1B	FAN 1B Speed(0x08)	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
8	FAN 1B	FAN 1B Speed(0x08)	At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
8	FAN 1B	FAN 1B Speed(0x08)	At or below lower critical threshold (going low).	Return to OK	Fan speed is returning to normal.
9	FAN 2A	FAN 2A Speed (0x09)	At or below lower non-critical threshold (going low).	Critical	Fan speed is lesser than expected.
9	FAN 2A	FAN 2A Speed (0x09)	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
9	FAN 2A	FAN 2A Speed (0x09)	At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.

N°	Component	Source	Event/Description	Severity	Meaning
9	FAN 2A	FAN 2A Speed (0x09)	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.
10	FAN 2B	FAN 2B Speed (0x0A)	At or below lower critical threshold (going low).	Critical	Fan speed is lesser than expected.
10	FAN 2B	FAN 2B Speed (0x0A)	At or below lower non-critical threshold (going low).	Return to OK	Fan speed is returning to normal.
10	FAN 2B	FAN 2B Speed (0x0A)	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.
11	Blade 1	Blade1 Presence(0x0B)	Device inserted/Device present.	Information	Blade is present.
12	Blade 2	Blade2 Presence(0x0C)	Device removed/Device absent.	Information	Blade is not present.
12	Blade 2	Blade2 Presence(0x0C)	Device inserted/Device present.	Information	Blade is present.
13	Blade 3	Blade3 Presence(0x0D)	Device removed/Device absent.	Information	Blade is not present.
13	Blade 3	Blade3 Presence(0x0D)	Device inserted/Device present.	Information	Blade is present.
14	Blade 4	Blade4 Presence(0x0E)	Device removed/Device absent.	Information	Blade is not present.
14	Blade 4	Blade4 Presence(0x0E)	Device inserted/Device present.	Information	Blade is present.
15	Blade 5	Blade5 Presence(0x0F)	Device removed/Device absent.	Information	Blade is not present.
15	Blade 5	Blade5 Presence(0x0F)	Device inserted/Device present.	Information	Blade is present.
16	Blade 6	Blade6 Presence(0x10)	Device removed/Device absent.	Information	Blade is not present.
16	Blade 6	Blade6 Presence(0x10)	Device inserted/Device present.	Information	Blade is present.
17	Blade 7	Blade7 Presence(0x11)	Device removed/Device absent.	Information	Blade is not present.
17	Blade 7	Blade7 Presence(0x11)	Device inserted/Device present.	Information	Blade is present.
18	Blade 8	Blade8 Presence(0x12)	Device removed/Device absent.	Information	Blade is not present.
18	Blade 8	Blade8 Presence(0x12)	Device inserted/Device present.	Information	Blade is present.
19	Blade 9	Blade9 Presence(0x13)	Device removed/Device absent.	Information	Blade is not present.
19	Blade 9	Blade9 Presence(0x13)	Device inserted/Device present.	Information	Blade is present.
20	Blade 10	Blade10 Presence(0x14)	Device removed/Device absent.	Information	Blade is not present.
20	Blade 10	Blade10 Presence(0x14)	Device inserted/Device present.	Information	Blade is present.
21	Blade 11	Blade11 Presence(0x15)	Device removed/Device absent.	Information	Blade is not present.
21	Blade 11	Blade11 Presence(0x15)	Device inserted/Device present.	Information	Blade is present.
22	Blade 12	Blade12 Presence(0x16)	Device removed/Device absent.	Information	Blade is not present.
22	Blade 12	Blade12 Presence(0x16)	Device inserted/Device present.	Information	Blade is present.
23	Blade 13	Blade13 Presence(0x17)	Device removed/Device absent.	Information	Blade is not present.
23	Blade 13	Blade13 Presence(0x17)	Device inserted/Device present.	Information	Blade is present.

N°	Component	Source	Event/Description	Severity	Meaning
24	Blade 14	Blade14 Presence(0x18)	Device removed/Device absent.	Information	Blade is not present.
24	Blade 14	Blade14 Presence(0x18)	Device inserted/Device present.	Information	Blade is present.
25	Blade 15	Blade15 Presence(0x19)	Device removed/Device absent.	Information	Blade is not present.
25	Blade 15	Blade15 Presence(0x19)	Device inserted/Device present.	Information	Blade is present.
26	Blade 16	Blade16 Presence(0x1A)	Device removed/Device absent.	Information	Blade is not present.
26	Blade 16	Blade16 Presence(0x1A)	Device inserted/Device present.	Information	Blade is present.
27	Blade 17	Blade17 Presence(0x1B)	Device removed/Device absent.	Information	Blade is not present.
27	Blade 17	Blade17 Presence(0x1B)	Device inserted/Device present.	Information	Blade is present.
28	Blade 18	Blade18 Presence(0x1C)	Device removed/Device absent.	Information	Blade is not present.
28	Blade 18	Blade18 Presence(0x1C)	Device inserted/Device present.	Information	Blade is present.
29	IBSW	IBSW Presence (0x1D)	Device removed/Device absent.	Information	IBSW is not present.
29	IBSW	IBSW Presence (0x1D)	Device inserted/Device present.	Information	IBSW is present.
30	UCM	UCM Presence (0x1E)	Device removed/Device absent.	Information	UCM is not present.
30	UCM	UCM Presence (0x1E)	Device inserted/Device present.	Information	UCM is present.
31	PSU-1	PSU-1 Presence(0x1F)	Device removed/Device absent.	Information	PSU-1 is not present.
31	PSU-1	PSU-1 Presence(0x1F)	Device inserted/Device present.	Information	PSU-1 is present.
32	PSU-2	PSU-2 Presence(0x20)	Device removed/Device absent.	Information	PSU-2 is not present.
32	PSU-2	PSU-2 Presence(0x20)	Device inserted/Device present.	Information	PSU-2 is present.
33	PSU-3	PSU-3 Presence(0x21)	Device removed/Device absent.	Information	PSU-3 is not present.
33	PSU-3	PSU-3 Presence(0x21)	Device inserted/Device present.	Information	PSU-3 is present.
34	PSU-4	PSU-4 Presence(0x22)	Device removed/Device absent.	Information	PSU-4 is not present.
34	PSU-4	PSU-4 Presence(0x22)	Device inserted/Device present.	Information	PSU-4 is present.
35	Blade 1	Blade 1 3v3 PG(0x23)	State Deassertion.	Information	The 3.3V power is not present.
35	Blade 1	Blade 1 3v3 PG(0x23)	State Assertion.	Information	The 3.3V power is present.
36	Blade 2	Blade 2 3v3 PG(0x24)	State Deassertion.	Information	The 3.3V power is not present.
36	Blade 2	Blade 2 3v3 PG(0x24)	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.
37	Blade 3	Blade 3 3v3 PG(0x25)	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.
38	Blade 4	Blade 4 3v3 PG(0x26)	State Assertion.	Information	The 3.3V power is present.

N°	Component	Source	Event/Description	Severity	Meaning
39	Blade 5	Blade 5 3v3 PG(0x27)	State Deassertion.	Information	The 3.3V power is not present.
39	Blade 5	Blade 5 3v3 PG(0x27)	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.
40	Blade 6	Blade 6 3v3 PG(0x28)	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.
41	Blade 7	Blade 7 3v3 PG(0x29)	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.
42	Blade 8	Blade 8 3v3 PG(0x2A)	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.
43	Blade 9	Blade 9 3v3 PG(0x2B)	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.
44	Blade 10	Blade 10 3v3 PG(0x2C)	State Assertion.	Information	The 3.3V power is present.
45	Blade 11	Blade 11 3v3 PG(0x2D)	State Deassertion.	Information	The 3.3V power is not present.
45	Blade 11	Blade 11 3v3 PG(0x2D)	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.
46	Blade 12	Blade 12 3v3 PG(0x2E)	State Assertion.	Information	The 3.3V power is present.
47	Blade 13	Blade 13 3v3 PG(0x2F)	State Deassertion.	Information	The 3.3V power is not present.
47	Blade 13	Blade 13 3v3 PG(0x2F)	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.
48	Blade 14	Blade 14 3v3 PG(0x30)	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.
49	Blade 15	Blade 15 3v3 PG(0x31)	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.
50	Blade 16	Blade 16 3v3 PG(0x32)	State Assertion.	Information	The 3.3V power is present.
51	Blade 17	Blade 17 3v3 PG(0x33)	State Deassertion.	Information	The 3.3V power is not present.
51	Blade 17	Blade 17 3v3 PG(0x33)	State Assertion.	Information	The 3.3V power is present.
52	Blade 18	Blade 18 3v3 PG(0x34)	State Deassertion.	Information	The 3.3V power is not present.
52	Blade 18	Blade 18 3v3 PG(0x34)	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.
53	Blade 1	Blade 1 SYSPG (0x35)	State Assertion.	Information	The 12V power is present.
54	Blade 2	Blade 2 SYSPG (0x36)	State Deassertion.	Information	The 12V power is not present.

N°	Component	Source	Event/Description	Severity	Meaning
54	Blade 2	Blade 2 SYSPG (0x36)	State Assertion.	Information	The 12V power is present.
55	Blade 3	Blade 3 SYSPG (0x37)	State Deassertion.	Information	The 12V power is not present.
55	Blade 3	Blade 3 SYSPG (0x37)	State Assertion.	Information	The 12V power is present.
56	Blade 4	Blade 4 SYSPG (0x38)	State Deassertion.	Information	The 12V power is not present.
56	Blade 4	Blade 4 SYSPG (0x38)	State Assertion.	Information	The 12V power is present.
57	Blade 5	Blade 5 SYSPG (0x39)	State Deassertion.	Information	The 12V power is not present.
57	Blade 5	Blade 5 SYSPG (0x39)	State Assertion.	Information	The 12V power is present.
58	Blade 6	Blade 6 SYSPG (0x3A)	State Deassertion.	Information	The 12V power is not present.
58	Blade 6	Blade 6 SYSPG (0x3A)	State Assertion.	Information	The 12V power is present.
59	Blade 7	Blade 7 SYSPG (0x3B)	State Deassertion.	Information	The 12V power is not present.
59	Blade 7	Blade 7 SYSPG (0x3B)	State Assertion.	Information	The 12V power is present.
60	Blade 8	Blade 8 SYSPG (0x3C)	State Deassertion.	Information	The 12V power is not present.
60	Blade 8	Blade 8 SYSPG (0x3C)	State Assertion.	Information	The 12V power is present.
61	Blade 9	Blade 9 SYSPG (0x3D)	State Deassertion.	Information	The 12V power is not present.
61	Blade 9	Blade 9 SYSPG (0x3D)	State Assertion.	Information	The 12V power is present.
62	Blade 10	Blade 10 SYSPG (0x3E)	State Deassertion.	Information	The 12V power is not present.
62	Blade 10	Blade 10 SYSPG (0x3E)	State Assertion.	Information	The 12V power is present.
63	Blade 11	Blade 11 SYSPG (0x3F)	State Deassertion.	Information	The 12V power is not present.
63	Blade 11	Blade 11 SYSPG (0x3F)	State Assertion.	Information	The 12V power is present.
64	Blade 12	Blade 12 SYSPG (0x40)	State Deassertion.	Information	The 12V power is not present.
64	Blade 12	Blade 12 SYSPG (0x40)	State Assertion.	Information	The 12V power is present.
65	Blade 13	Blade 13 SYSPG (0x41)	State Deassertion.	Information	The 12V power is not present.
65	Blade 13	Blade 13 SYSPG (0x41)	State Assertion.	Information	The 12V power is present.
66	Blade 14	Blade 14 SYSPG (0x42)	State Deassertion.	Information	The 12V power is not present.
66	Blade 14	Blade 14 SYSPG (0x42)	State Assertion.	Information	The 12V power is present.
67	Blade 15	Blade 15 SYSPG (0x43)	State Deassertion.	Information	The 12V power is not present.
67	Blade 15	Blade 15 SYSPG (0x43)	State Assertion.	Information	The 12V power is present.
68	Blade 16	Blade 16 SYSPG (0x44)	State Deassertion.	Information	The 12V power is not present.
68	Blade 16	Blade 16 SYSPG (0x44)	State Assertion.	Information	The 12V power is present.
69	Blade 17	Blade 17 SYSPG (0x45)	State Deassertion.	Information	The 12V power is not present.
69	Blade 17	Blade 17 SYSPG (0x45)	State Assertion.	Information	The 12V power is present.
70	Blade 18	Blade 18 SYSPG (0x46)	State Deassertion.	Information	The 12V power is not present.

N°	Component	Source	Event/Description	Severity	Meaning
70	Blade 18	Blade 18 SYSPG (0x46)	State Assertion.	Information	The 12V power is present.
71	PSU-1	PSU-1 Input Volt(0x47)	At or below lower non-critical threshold (going low).	Critical	PSU-1 input voltage lesser than expected.
71	PSU-1	PSU-1 Input Volt(0x47)	At or below lower critical threshold (going low).	Critical	PSU-1 input voltage lesser than expected.
71	PSU-1	PSU-1 Input Volt(0x47)	At or above upper critical threshold (going high).	Critical	PSU–1 input voltage greater than expected
71	PSU-1	PSU-1 Input Volt(0x47)	At or above upper non-critical threshold (going high).	Critical	PSU–1 input voltage greater than expected.
71	PSU-1	PSU-1 Input Volt(0x47)	At or below lower non-critical threshold (going low).	Return to OK	PSU–1 input voltage returning to normal.
71	PSU-1	PSU-1 Input Volt(0x47)	At or below lower critical threshold (going low).	Return to OK	PSU–1 input voltage returning to normal.
71	PSU-1	PSU-1 Input Volt(0x47)	At or above upper critical threshold (going high).	Return to OK	PSU–1 input voltage returning to normal.
71	PSU-1	PSU-1 Input Volt(0x47)	At or above upper non-critical threshold (going high).	Return to OK	PSU-1 input voltage returning to normal.
72	PSU-2	PSU-2 Input Volt(0x48)	At or below lower non-critical threshold (going low).	Critical	PSU-2 input voltage lesser than expected.
72	PSU-2	PSU-2 Input Volt(0x48)	At or below lower critical threshold (going low).	Critical	PSU-2 input voltage lesser than expected.
72	PSU-2	PSU-2 Input Volt(0x48)	At or above upper critical threshold (going high).	Critical	PSU–2 input voltage greater than expected
72	PSU-2	PSU-2 Input Volt(0x48)	At or above upper non-critical threshold (going high).	Critical	PSU–2 input voltage greater than expected.
72	PSU-2	PSU-2 Input Volt(0x48)	At or below lower non-critical threshold (going low).	Return to OK	PSU–2 input voltage returning to normal.
72	PSU-2	PSU-2 Input Volt(0x48)	At or below lower critical threshold (going low).	Return to OK	PSU–2 input voltage returning to normal.
72	PSU-2	PSU-2 Input Volt(0x48)	At or above upper critical threshold (going high).	Return to OK	PSU–2 input voltage returning to normal.
72	PSU-2	PSU-2 Input Volt(0x48)	At or above upper non-critical threshold (going high).	Return to OK	PSU-2 input voltage returning to normal.
73	PSU-3	PSU-3 Input Volt(0x49)	At or below lower non-critical threshold (going low).	Critical	PSU-3 input voltage lesser than expected.
73	PSU-3	PSU-3 Input Volt(0x49)	At or below lower critical threshold (going low).	Critical	PSU-3 input voltage lesser than expected.
73	PSU-3	PSU-3 Input Volt(0x49)	At or above upper critical threshold (going high).	Critical	PSU–3 input voltage greater than expected
73	PSU-3	PSU-3 Input Volt(0x49)	At or above upper non-critical threshold (going high).	Critical	PSU–3 input voltage greater than expected.
73	PSU-3	PSU-3 Input Volt(0x49)	At or below lower non-critical threshold (going low).	Return to OK	PSU–3 input voltage returning to normal.
73	PSU-3	PSU-3 Input Volt(0x49)	At or below lower critical threshold (going low).	Return to OK	PSU–3 input voltage returning to normal.
73	PSU-3	PSU-3 Input Volt(0x49)	At or above upper critical threshold (going high).	Return to OK	PSU–3 input voltage returning to normal.
73	PSU-3	PSU-3 Input Volt(0x49)	At or above upper non-critical threshold (going high).	Return to OK	PSU-3 input voltage returning to normal.
75	Drawer Power	Drawer Input Power Consumption (0x4B)	None (info only; no monitoring)	Information	

N°	Component	Source	Event/Description	Severity	Meaning
76	PSU-1	PSU-1 Failure (0x4C)	Failure detected asserted.	Critical	PSU-1 Failure.
76	PSU-1	PSU-1 Failure (0x4C)	Predictive failure asserted.	Critical	Predictive PSU-1 Failure.
76	PSU-1	PSU-1 Failure (0x4C)	AC input lost.	Critical	PSU-1 AC input lost.
76	PSU-1	PSU-1 Failure (0x4C)	Failure detected asserted.	Return to OK	PSU-1 returning to normal.
76	PSU-1	PSU-1 Failure (0x4C)	Predictive failure asserted.	Return to OK	PSU-1 returning to normal.
76	PSU-1	PSU-1 Failure (0x4C)	AC input lost.	Return to OK	PSU-1 returning to normal.
77	PSU-2	PSU-2 Failure (0x4D)	Failure detected asserted.	Critical	PSU-2 Failure.
77	PSU-2	PSU-2 Failure (0x4D)	Predictive failure asserted.	Critical	Predictive PSU-2 Failure.
77	PSU-2	PSU-2 Failure (0x4D)	AC input lost.	Critical	PSU-2 AC input lost.
77	PSU-2	PSU-2 Failure (0x4D)	Failure detected asserted.	Return to OK	PSU-2 returning to normal.
77	PSU-2	PSU-2 Failure (0x4D)	Predictive failure asserted.	Return to OK	PSU-2 returning to normal.
77	PSU-2	PSU-2 Failure (0x4D)	AC input lost.	Return to OK	PSU-2 returning to normal.
78	PSU-3	PSU-3 Failure (0x4E)	Failure detected asserted.	Critical	PSU-3 Failure.
78	PSU-3	PSU-3 Failure (0x4E)	Predictive failure asserted.	Critical	Predictive PSU-3 Failure.
78	PSU-3	PSU-3 Failure (0x4E)	AC input lost.	Critical	PSU-3 AC input lost.
78	PSU-3	PSU-3 Failure (0x4E)	Failure detected asserted.	Return to OK	PSU-3 returning to normal.
78	PSU-3	PSU-3 Failure (0x4E)	Predictive failure asserted.	Return to OK	PSU-3 returning to normal.
78	PSU-3	PSU-3 Failure (0x4E)	AC input lost.	Return to OK	PSU-3 returning to normal.
79	PSU-4	PSU-4 Failure (0x4F)	Failure detected asserted.	Critical	PSU-4 Failure.
79	PSU-4	PSU-4 Failure (0x4F)	Predictive failure asserted.	Critical	Predictive PSU-4 Failure.
79	PSU-4	PSU-4 Failure (0x4F)	AC input lost.	Critical	PSU-4 AC input lost.
79	PSU-4	PSU-4 Failure (0x4F)	Failure detected asserted.	Return to OK	PSU-4 returning to normal.
79	PSU-4	PSU-4 Failure (0x4F)	Predictive failure asserted.	Return to OK	PSU-4 returning to normal.
79	PSU-4	PSU-4 Failure (0x4F)	AC input lost.	Return to OK	PSU-4 returning to normal.

N°	Component	Source	Event/Description	Severity	Meaning
80	PSU-4	PSU-4 Input Volt(0x50)	At or below lower non-critical threshold (going low).	Critical	PSU-4 input voltage lesser than expected.
80	PSU-4	PSU-4 Input Volt(0x50)	At or below lower critical threshold (going low).	Critical	PSU-4 input voltage lesser than expected.
80	PSU-4	PSU-4 Input Volt(0x50)	At or above upper critical threshold (going high).	Critical	PSU–4 input voltage greater than expected
80	PSU-4	PSU-4 Input Volt(0x50)	At or above upper non-critical threshold (going high).	Critical	PSU–4 input voltage greater than expected.
80	PSU-4	PSU-4 Input Volt(0x50)	At or below lower non-critical threshold (going low).	Return to OK	PSU–4 input voltage returning to normal.
80	PSU-4	PSU-4 Input Volt(0x50)	At or below lower critical threshold (going low).	Return to OK	PSU–4 input voltage returning to normal.
80	PSU-4	PSU-4 Input Volt(0x50)	At or above upper critical threshold (going high).	Return to OK	PSU–4 input voltage returning to normal.
80	PSU-4	PSU-4 Input Volt(0x50)	At or above upper non-critical threshold (going high).	Return to OK	PSU-4 input voltage returning to normal.
81	PSU-1	PSU-1 Input Current (0x51)	At or below lower non-critical threshold (going low).	Critical	PSU-1 input current lesser than expected.
81	PSU-1	PSU-1 Input Current (0x51)	At or below lower critical threshold (going low).	Critical	PSU-1 input current lesser than expected.
81	PSU-1	PSU-1 Input Current (0x51)	At or above upper critical threshold (going high).	Critical	PSU–1 input current greater than expected
81	PSU-1	PSU-1 Input Current (0x51)	At or above upper non-critical threshold (going high).	Critical	PSU–1 input current greater than expected.
81	PSU-1	PSU-1 Input Current (0x51)	At or below lower non-critical threshold (going low).	Return to OK	PSU–1 input current returning to normal.
81	PSU-1	PSU-1 Input Current (0x51)	At or below lower critical threshold (going low).	Return to OK	PSU–1 input current returning to normal.
81	PSU-1	PSU-1 Input Current (0x51)	At or above upper critical threshold (going high).	Return to OK	PSU–1 input current returning to normal.
81	PSU-1	PSU-1 Input Current (0x51)	At or above upper non-critical threshold (going high).	Return to OK	PSU-1 input current returning to normal.
82	PSU-2	PSU-2 Input Current (0x52)	At or below lower non-critical threshold (going low).	Critical	PSU-2 input current lesser than expected.
82	PSU-2	PSU-2 Input Current (0x52)	At or below lower critical threshold (going low).	Critical	PSU-2 input current lesser than expected.
82	PSU-2	PSU-2 Input Current (0x52)	At or above upper critical threshold (going high).	Critical	PSU–2 input current greater than expected
82	PSU-2	PSU-2 Input Current (0x52)	At or above upper non-critical threshold (going high).	Critical	PSU–2 input current greater than expected.
82	PSU-2	PSU-2 Input Current (0x52)	At or below lower non-critical threshold (going low).	Return to OK	PSU–2 input current returning to normal.
82	PSU-2	PSU-2 Input Current (0x52)	At or below lower critical threshold (going low).	Return to OK	PSU–2 input current returning to normal.
82	PSU-2	PSU-2 Input Current (0x52)	At or above upper critical threshold (going high).	Return to OK	PSU–2 input current returning to normal.
82	PSU-2	PSU-2 Input Current (0x52)	At or above upper non-critical threshold (going high).	Return to OK	PSU-2 input current returning to normal.
83	PSU-3	PSU-3 Input Current (0x53)	At or below lower non-critical threshold (going low).	Critical	PSU-3 input current lesser than expected.
83	PSU-3	PSU-3 Input Current (0x53)	At or below lower critical threshold (going low).	Critical	PSU-3 input current lesser than expected.

N°	Component	Source	Event/Description	Severity	Meaning
83	PSU-3	PSU-3 Input Current (0x53)	At or above upper critical threshold (going high).	Critical	PSU–3 input current greater than expected
83	PSU-3	PSU-3 Input Current (0x53)	At or above upper non-critical threshold (going high).	Critical	PSU–3 input current greater than expected.
83	PSU-3	PSU-3 Input Current (0x53)	At or below lower non-critical threshold (going low).	Return to OK	PSU–3 input current returning to normal.
83	PSU-3	PSU-3 Input Current (0x53)	At or below lower critical threshold (going low).	Return to OK	PSU–3 input current returning to normal.
83	PSU-3	PSU-3 Input Current (0x53)	At or above upper critical threshold (going high).	Return to OK	PSU–3 input current returning to normal.
83	PSU-3	PSU-3 Input Current (0x53)	At or above upper non-critical threshold (going high).	Return to OK	PSU-3 input current returning to normal.
84	PSU-4	PSU-4 Input Current (0x54)	At or below lower non-critical threshold (going low).	Critical	PSU-4 input current lesser than expected.
84	PSU-4	PSU-4 Input Current (0x54)	At or below lower critical threshold (going low).	Critical	PSU-4 input current lesser than expected.
84	PSU-4	PSU-4 Input Current (0x54)	At or above upper critical threshold (going high).	Critical	PSU–4 input current greater than expected
84	PSU-4	PSU-4 Input Current (0x54)	At or above upper non-critical threshold (going high).	Critical	PSU–4 input current greater than expected.
84	PSU-4	PSU-4 Input Current (0x54)	At or below lower non-critical threshold (going low).	Return to OK	PSU–4 input current returning to normal.
84	PSU-4	PSU-4 Input Current (0x54)	At or below lower critical threshold (going low).	Return to OK	PSU–4 input current returning to normal.
84	PSU-4	PSU-4 Input Current (0x54)	At or above upper critical threshold (going high).	Return to OK	PSU–4 input current returning to normal.
84	PSU-4	PSU-4 Input Current (0x54)	At or above upper non-critical threshold (going high).	Return to OK	PSU-4 input current returning to normal.
85	PSU-1	PSU-1 Output Volt (0x55)	At or below lower non-critical threshold (going low).	Critical	PSU-1 output voltage lesser than expected.
85	PSU-1	PSU-1 Output Volt (0x55)	At or below lower critical threshold (going low).	Critical	PSU-1 output voltage lesser than expected.
85	PSU-1	PSU-1 Output Volt (0x55)	At or above upper critical threshold (going high).	Critical	PSU–1 output voltage greater than expected
85	PSU-1	PSU-1 Output Volt (0x55)	At or above upper non-critical threshold (going high).	Critical	PSU–1 output voltage greater than expected.
85	PSU-1	PSU-1 Output Volt (0x55)	At or below lower non-critical threshold (going low).	Return to OK	PSU–1 output voltage returning to normal.
85	PSU-1	PSU-1 Output Volt (0x55)	At or below lower critical threshold (going low).	Return to OK	PSU–1 output voltage returning to normal.
85	PSU-1	PSU-1 Output Volt (0x55)	At or above upper critical threshold (going high).	Return to OK	PSU–1 output voltage returning to normal.
85	PSU-1	PSU-1 Output Volt (0x55)	At or above upper non-critical threshold (going high).	Return to OK	PSU-1 output voltage returning to normal.
86	PSU-2	PSU-2 Output Volt (0x56)	At or below lower non-critical threshold (going low).	Critical	PSU-2 output voltage lesser than expected.
86	PSU-2	PSU-2 Output Volt (0x56)	At or below lower critical threshold (going low).	Critical	PSU-2 output voltage lesser than expected.
86	PSU-2	PSU-2 Output Volt (0x56)	At or above upper critical threshold (going high).	Critical	PSU–2 output voltage greater than expected
86	PSU-2	PSU-2 Output Volt (0x56)	At or above upper non-critical threshold (going high).	Critical	PSU–2 output voltage greater than expected.

N°	Component	Source	Event/Description	Severity	Meaning
86	PSU-2	PSU-2 Output Volt (0x56)	At or below lower non-critical threshold (going low).	Return to OK	PSU–2 output voltage returning to normal.
86	PSU-2	PSU-2 Output Volt (0x56)	At or below lower critical threshold (going low).	Return to OK	PSU–2 output voltage returning to normal.
86	PSU-2	PSU-2 Output Volt (0x56)	At or above upper critical threshold (going high).	Return to OK	PSU–1 output voltage returning to normal.
86	PSU-2	PSU-2 Output Volt (0x56)	At or above upper non-critical threshold (going high).	Return to OK	PSU-2 output voltage returning to normal.
87	PSU-3	PSU-3 Output Volt (0x57)	At or below lower non-critical threshold (going low).	Critical	PSU-3 output voltage lesser than expected.
87	PSU-3	PSU-3 Output Volt (0x57)	At or below lower critical threshold (going low).	Critical	PSU-3 output voltage lesser than expected.
87	PSU-3	PSU-3 Output Volt (0x57)	At or above upper critical threshold (going high).	Critical	PSU–3 output voltage greater than expected
87	PSU-3	PSU-3 Output Volt (0x57)	At or above upper non-critical threshold (going high).	Critical	PSU–3 output voltage greater than expected.
87	PSU-3	PSU-3 Output Volt (0x57)	At or below lower non-critical threshold (going low).	Return to OK	PSU–3 output voltage returning to normal.
87	PSU-3	PSU-3 Output Volt (0x57)	At or below lower critical threshold (going low).	Return to OK	PSU–3 output voltage returning to normal.
87	PSU-3	PSU-3 Output Volt (0x57)	At or above upper critical threshold (going high).	Return to OK	PSU–3 output voltage returning to normal.
87	PSU-3	PSU-3 Output Volt (0x57)	At or above upper non-critical threshold (going high).	Return to OK	PSU-3 output voltage returning to normal.
88	PSU-4	PSU-4 Output Volt (0x58)	At or below lower non-critical threshold (going low).	Critical	PSU-4 output voltage lesser than expected.
88	PSU-4	PSU-4 Output Volt (0x58)	At or below lower critical threshold (going low).	Critical	PSU-4 output voltage lesser than expected.
88	PSU-4	PSU-4 Output Volt (0x58)	At or above upper critical threshold (going high).	Critical	PSU–4 output voltage greater than expected
88	PSU-4	PSU-4 Output Volt (0x58)	At or above upper non-critical threshold (going high).	Critical	PSU–4 output voltage greater than expected.
88	PSU-4	PSU-4 Output Volt (0x58)	At or below lower non-critical threshold (going low).	Return to OK	PSU–4 output voltage returning to normal.
88	PSU-4	PSU-4 Output Volt (0x58)	At or below lower critical threshold (going low).	Return to OK	PSU–4 output voltage returning to normal.
88	PSU-4	PSU-4 Output Volt (0x58)	At or above upper critical threshold (going high).	Return to OK	PSU–4 output voltage returning to normal.
88	PSU-4	PSU-4 Output Volt (0x58)	At or above upper non-critical threshold (going high).	Return to OK	PSU-4 output voltage returning to normal.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or below lower non-critical threshold (going low).	Critical	PSU-1 output current lesser than expected.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or below lower critical threshold (going low).	Critical	PSU-1 output current lesser than expected.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or above upper critical threshold (going high).	Critical	PSU–1 output current greater than expected
89	PSU-1	PSU-1 Ouput Current (0x59)	At or above upper non-critical threshold (going high).	Critical	PSU–1 output current greater than expected.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or below lower non-critical threshold (going low).	Return to OK	PSU–1 output current returning to normal.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or below lower critical threshold (going low).	Return to OK	PSU–1 output current returning to normal.

N°	Component	Source	Event/Description	Severity	Meaning
89	PSU-1	PSU-1 Ouput Current (0x59)	At or above upper critical threshold (going high).	Return to OK	PSU–1 output current returning to normal.
89	PSU-1	PSU-1 Ouput Current (0x59)	At or above upper non-critical threshold (going high).	Return to OK	PSU-1 output current returning to normal.
90	PSU-2	PSU-2 Output Current (0x5A)	At or below lower non-critical threshold (going low).	Critical	PSU-2 output current lesser than expected.
90	PSU-2	PSU-2 Output Current (0x5A)	At or below lower critical threshold (going low).	Critical	PSU-2 output current lesser than expected.
90	PSU-2	PSU-2 Output Current (0x5A)	At or above upper critical threshold (going high).	Critical	PSU–2 output current greater than expected
90	PSU-2	PSU-2 Output Current (0x5A)	At or above upper non-critical threshold (going high).	Critical	PSU–2 output current greater than expected.
90	PSU-2	PSU-2 Output Current (0x5A)	At or below lower non-critical threshold (going low).	Return to OK	PSU–2 output current returning to normal.
90	PSU-2	PSU-2 Output Current (0x5A)	At or below lower critical threshold (going low).	Return to OK	PSU–2 output current returning to normal.
90	PSU-2	PSU-2 Output Current (0x5A)	At or above upper critical threshold (going high).	Return to OK	PSU–2 output current returning to normal.
90	PSU-2	PSU-2 Output Current (0x5A))	At or above upper non-critical threshold (going high).	Return to OK	PSU-2 output current returning to normal.
91	PSU-3	PSU-3 Output Current (0x5B)	At or below lower non-critical threshold (going low).	Critical	PSU-3 output current lesser than expected.
91	PSU-3	PSU-3 Output Current (0x5B)	At or below lower critical threshold (going low).	Critical	PSU-3 output current lesser than expected.
91	PSU-3	PSU-3 Output Current (0x5B)	At or above upper critical threshold (going high).	Critical	PSU–3 output current greater than expected
91	PSU-3	PSU-3 Output Current (0x5B)	At or above upper non-critical threshold (going high).	Critical	PSU–3 output current greater than expected.
91	PSU-3	PSU-3 Output Current (0x5B)	At or below lower non-critical threshold (going low).	Return to OK	PSU–3 output current returning to normal.
91	PSU-3	PSU-3 Output Current (0x5B)	At or below lower critical threshold (going low).	Return to OK	PSU–3 output current returning to normal.
91	PSU-3	PSU-3 Output Current (0x5B)	At or above upper critical threshold (going high).	Return to OK	PSU–3 output current returning to normal.
91	PSU-3	PSU-3 Output Current (0x5B)	At or above upper non-critical threshold (going high).	Return to OK	PSU-3 output current returning to normal.
92	PSU-4	PSU-4 Output Current (0x5C)	At or below lower non-critical threshold (going low).	Critical	PSU-4 output current lesser than expected.
92	PSU-4	PSU-4 Output Current (0x5C)	At or below lower critical threshold (going low).	Critical	PSU-4 output current lesser than expected.
92	PSU-4	PSU-4 Output Current (0x5C)	At or above upper critical threshold (going high).	Critical	PSU–4 output current greater than expected
92	PSU-4	PSU-4 Output Current (0x5C)	At or above upper non-critical threshold (going high).	Critical	PSU–4 output current greater than expected.
92	PSU-4	PSU-4 Output Current (0x5C)	At or below lower non-critical threshold (going low).	Return to OK	PSU–4 output current returning to normal.
92	PSU-4	PSU-4 Output Current (0x5C)	At or below lower critical threshold (going low).	Return to OK	PSU–4 output current returning to normal.
92	PSU-4	PSU-4 Output Current (0x5C)	At or above upper critical threshold (going high).	Return to OK	PSU–4 output current returning to normal.
92	PSU-4	PSU-4 Output Current (0x5C)	At or above upper non-critical threshold (going high).	Return to OK	PSU-4 output current returning to normal.

N°	Component	Source	Event/Description	Severity	Meaning
208	UCM	UCM Vcap 1 (0xD0)	At or below lower non-critical threshold (going low).	Critical	UCM Vcap 1 voltage lesser than expected.
208	UCM	UCM Vcap 1 (0xD0)	At or below lower critical threshold (going low).	Critical	UCM Vcap 1 voltage lesser than expected.
208	UCM	UCM Vcap 1 (0xD0)	At or above upper critical threshold (going high).	Critical	UCM Vcap 1 voltage greater than expected
208	UCM	UCM Vcap 1 (0xD0)	At or above upper non-critical threshold (going high).	Critical	UCM Vcap 1 voltage greater than expected.
208	UCM	UCM Vcap 1 (0xD0)	At or below lower non-critical threshold (going low).	Return to OK	UCM Vcap 1 voltage returning to normal.
208	UCM	UCM Vcap 1 (0xD0)	At or below lower critical threshold (going low).	Return to OK	UCM Vcap 1 voltage returning to normal.
208	UCM	UCM Vcap 1 (0xD0)	At or above upper critical threshold (going high).	Return to OK	UCM Vcap 1 voltage returning to normal.
208	UCM	UCM Vcap 1 (0xD0)	At or above upper non-critical threshold (going high).	Return to OK	UCM Vcap 1 voltage returning to normal.
209	UCM	UCM Vcap 2 (0xD1)	At or below lower non-critical threshold (going low).	Critical	UCM Vcap 2 voltage lesser than expected.
209	UCM	UCM Vcap 2 (0xD1)	At or below lower critical threshold (going low).	Critical	UCM Vcap 2 voltage lesser than expected.
209	UCM	UCM Vcap 2 (0xD1)	At or above upper critical threshold (going high).	Critical	UCM Vcap 2 voltage greater than expected
209	UCM	UCM Vcap 2 (0xD1)	At or above upper non-critical threshold (going high).	Critical	UCM Vcap 2 voltage greater than expected.
209	UCM	UCM Vcap 2 (0xD1)	At or below lower non-critical threshold (going low).	Return to OK	UCM Vcap 2 voltage returning to normal.
209	UCM	UCM Vcap 2 (0xD1)	At or below lower critical threshold (going low).	Return to OK	UCM Vcap 2 voltage returning to normal.
209	UCM	UCM Vcap 2 (0xD1)	At or above upper critical threshold (going high).	Return to OK	UCM Vcap 2 voltage returning to normal.
209	UCM	UCM Vcap 2 (0xD1)	At or above upper non-critical threshold (going high).	Return to OK	UCM Vcap 2 voltage returning to normal.
210	UCM	UCM 21V 1 (0xD2)	At or below lower non-critical threshold (going low).	Critical	UCM 21V 1 voltage lesser than expected.
210	UCM	UCM 21V 1 (0xD2)	At or below lower critical threshold (going low).	Critical	UCM 21V 1 voltage lesser than expected.
210	UCM	UCM 21V 1 (0xD2)	At or above upper critical threshold (going high).	Critical	UCM 21V 1 voltage greater than expected
210	UCM	UCM 21V 1 (0xD2)	At or above upper non-critical threshold (going high).	Critical	UCM 21V 1 voltage greater than expected.
210	UCM	UCM 21V 1 (0xD2)	At or below lower non-critical threshold (going low).	Return to OK	UCM 21V 1 voltage returning to normal.
210	UCM	UCM 21V 1 (0xD2)	At or below lower critical threshold (going low).	Return to OK	UCM 21V 1 voltage returning to normal.
210	UCM	UCM 21V 1 (0xD2)	At or above upper critical threshold (going high).	Return to OK	UCM 21V 1 voltage returning to normal.
210	UCM	UCM 21V 1 (0xD2)	At or above upper non-critical threshold (going high).	Return to OK	UCM 21V 1 voltage returning to normal.
211	UCM	UCM 21V 2 (0xD3)	At or below lower non-critical threshold (going low).	Critical	UCM 21V 2 voltage lesser than expected.

N°	Component	Source	Event/Description	Severity	Meaning
211	UCM	UCM 21V 2 (0xD3)	At or below lower critical threshold (going low).	Critical	UCM 21V 2 voltage lesser than expected.
211	UCM	UCM 21V 2 (0xD3)	At or above upper critical threshold (going high).	Critical	UCM 21V 2 voltage greater than expected
211	UCM	UCM 21V 2 (0xD3)	At or above upper non-critical threshold (going high).	Critical	UCM 21V 2 voltage greater than expected.
211	UCM	UCM 21V 2 (0xD3)	At or below lower non-critical threshold (going low).	Return to OK	UCM 21V 2 voltage returning to normal.
211	UCM	UCM 21V 2 (0xD3)	At or below lower critical threshold (going low).	Return to OK	UCM 21V 2 voltage returning to normal.
211	UCM	UCM 21V 2 (0xD3)	At or above upper critical threshold (going high).	Return to OK	UCM 21V 2 voltage returning to normal.
211	UCM	UCM 21V 2 (0xD3)	At or above upper non-critical threshold (going high).	Return to OK	UCM 21V 2 voltage returning to normal.
212	UCM	UCM 12V (0xD4)	At or below lower non-critical threshold (going low).	Critical	UCM 12V voltage lesser than expected.
212	UCM	UCM 12V (0xD4)	At or below lower critical threshold (going low).	Critical	UCM 12V voltage lesser than expected.
212	UCM	UCM 12V (0xD4)	At or above upper critical threshold (going high).	Critical	UCM 12V voltage greater than expected
212	UCM	UCM 12V (0xD4)	At or above upper non-critical threshold (going high).	Critical	UCM 12V voltage greater than expected.
212	UCM	UCM 12V (0xD4)	At or below lower non-critical threshold (going low).	Return to OK	UCM 12V voltage returning to normal.
212	UCM	UCM 12V (0xD4)	At or below lower critical threshold (going low).	Return to OK	UCM 12V voltage returning to normal.
212	UCM	UCM 12V (0xD4)	At or above upper critical threshold (going high).	Return to OK	UCM 12V voltage returning to normal.
212	UCM	UCM 12V (0xD4)	At or above upper non-critical threshold (going high).	Return to OK	UCM 12V voltage returning to normal.
213	UCM	UCM Vref (0xD5)	At or below lower non-critical threshold (going low).	Critical	UCM Vref voltage lesser than expected.
213	UCM	UCM Vref (0xD5)	At or below lower critical threshold (going low).	Critical	UCM Vref voltage lesser than expected.
213	UCM	UCM Vref (0xD5)	At or above upper critical threshold (going high).	Critical	UCM Vref voltage greater than expected
213	UCM	UCM Vref (0xD5)	At or above upper non-critical threshold (going high).	Critical	UCM Vref voltage greater than expected.
213	UCM	UCM Vref (0xD5)	At or below lower non-critical threshold (going low).	Return to OK	UCM Vref voltage returning to normal.
213	UCM	UCM Vref (0xD5)	At or below lower critical threshold (going low).	Return to OK	UCM Vref voltage returning to normal.
213	UCM	UCM Vref (0xD5)	At or above upper critical threshold (going high).	Return to OK	UCM Vref voltage returning to normal.
213	UCM	UCM Vref (0xD5)	At or above upper non-critical threshold (going high).	Return to OK	UCM Vref voltage returning to normal.
214	UCM	UCM S1 C2 (0xD6)	At or below lower non-critical threshold (going low).	Critical	UCM Stack 1 Capacitor 2 voltage lesser than expected.
214	UCM	UCM S1 C2 (0xD6)	At or below lower critical threshold (going low).	Critical	UCM Stack 1 Capacitor 2 voltage lesser than expected.

N°	Component	Source	Event/Description	Severity	Meaning
214	UCM	UCM S1 C2 (0xD6)	At or above upper critical threshold (going high).	Critical	UCM Stack 1 Capacitor 2 voltage lesser than expected.
214	UCM	UCM S1 C2 (0xD6)	At or above upper non-critical threshold (going high).	Critical	UCM Stack 1 Capacitor 2 voltage lesser than expected.
214	UCM	UCM S1 C2 (0xD6)	At or below lower non-critical threshold (going low).	Return to OK	UCM Stack 1 Capacitor 2 voltage returning to normal.
214	UCM	UCM S1 C2 (0xD6)	At or below lower critical threshold (going low).	Return to OK	UCM Stack 1 Capacitor 2 voltage returning to normal.
214	UCM	UCM S1 C2 (0xD6)	At or above upper critical threshold (going high).	Return to OK	UCM Stack 1 Capacitor 2 voltage returning to normal.
214	UCM	UCM S1 C2 (0xD6)	At or above upper non-critical threshold (going high).	Return to OK	UCM Stack 1 Capacitor 2 voltage returning to normal.
215	UCM	UCM S1 C4 (0xD7)	At or below lower non-critical threshold (going low).	Critical	UCM Stack 1 Capacitor 4 voltage lesser than expected.
215	UCM	UCM S1 C4 (0xD7)	At or below lower critical threshold (going low).	Critical	UCM Stack 1 Capacitor 4 voltage lesser than expected.
215	UCM	UCM S1 C4 (0xD7)	At or above upper critical threshold (going high).	Critical	UCM Stack 1 Capacitor 4 voltage lesser than expected.
215	UCM	UCM S1 C4 (0xD7)	At or above upper non-critical threshold (going high).	Critical	UCM Stack 1 Capacitor 4 voltage lesser than expected.
215	UCM	UCM S1 C4 (0xD7)	At or below lower non-critical threshold (going low).	Return to OK	UCM Stack 1 Capacitor 4 voltage returning to normal.
215	UCM	UCM S1 C4 (0xD7)	At or below lower critical threshold (going low).	Return to OK	UCM Stack 1 Capacitor 4 voltage returning to normal.
215	UCM	UCM S1 C4 (0xD7)	At or above upper critical threshold (going high).	Return to OK	UCM Stack 1 Capacitor 4 voltage returning to normal.
215	UCM	UCM S1 C4 (0xD7)	At or above upper non-critical threshold (going high).	Return to OK	UCM Stack 1 Capacitor 4 voltage returning to normal.
216	UCM	UCM S2 C2 (0xD8)	At or below lower non-critical threshold (going low).	Critical	UCM Stack 2 Capacitor 2 voltage lesser than expected.
216	UCM	UCM S2 C2 (0xD8)	At or below lower critical threshold (going low).	Critical	UCM Stack 2 Capacitor 2 voltage lesser than expected.
216	UCM	UCM S2 C2 (0xD8)	At or above upper critical threshold (going high).	Critical	UCM Stack 2 Capacitor 2 voltage lesser than expected.
216	UCM	UCM S2 C2 (0xD8)	At or above upper non-critical threshold (going high).	Critical	UCM Stack 2 Capacitor 2 voltage lesser than expected.

N°	Component	Source	Event/Description	Severity	Meaning
216	UCM	UCM S2 C2 (0xD8)	At or below lower non-critical threshold (going low).	Return to OK	UCM Stack 2 Capacitor 2 voltage returning to normal.
216	UCM	UCM S2 C2 (0xD8)	At or below lower critical threshold (going low).	Return to OK	UCM Stack 2 Capacitor 2 voltage returning to normal.
216	UCM	UCM S2 C2 (0xD8)	At or above upper critical threshold (going high).	Return to OK	UCM Stack 2 Capacitor 2 voltage returning to normal.
216	UCM	UCM S2 C2 (0xD8)	At or above upper non-critical threshold (going high).	Return to OK	UCM Stack 2 Capacitor 2 voltage returning to normal.
217	UCM	UCM S2 C4 (0xD9)	At or below lower non-critical threshold (going low).	Critical	UCM Stack 2 Capacitor 4 voltage lesser than expected.
217	UCM	UCM S2 C4 (0xD9)	At or below lower critical threshold (going low).	Critical	UCM Stack 2 Capacitor 4 voltage lesser than expected.
217	UCM	UCM S2 C4 (0xD9)	At or above upper critical threshold (going high).	Critical	UCM Stack 2 Capacitor 4 voltage lesser than expected.
217	UCM	UCM S2 C4 (0xD9)	At or above upper non-critical threshold (going high).	Critical	UCM Stack 2 Capacitor 4 voltage lesser than expected.
217	UCM	UCM S2 C4 (0xD9)	At or below lower non-critical threshold (going low).	Return to OK	UCM Stack 2 Capacitor 4 voltage returning to normal.
217	UCM	UCM S2 C4 (0xD9)	At or below lower critical threshold (going low).	Return to OK	UCM Stack 2 Capacitor 4 voltage returning to normal.
217	UCM	UCM S2 C4 (0xD9)	At or above upper critical threshold (going high).	Return to OK	UCM Stack 2 Capacitor 4 voltage returning to normal.
217	UCM	UCM S2 C4 (0xD9)	At or above upper non-critical threshold (going high).	Return to OK	UCM Stack 2 Capacitor 4 voltage returning to normal.

Notes
- 3v3 PG (Power Good) means the 3.3V power is running in the blade
- SYSPG (SYStem Power Good) means the 12V power is running in the blade

Table B-1. Chassis predefined alert filters

B.2. Chassis System Event Log (SEL) Messages

This section lists the Chassis System Event Log Messages and explains actions to recover, where applicable. It includes the following topics:

B.2.1. LCP SEL Messages

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

Description	The LCP temperature is lower than the minimum.
Severity	Critical.
Direction	Assertion.
Filter Number	5.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The LCP temperature is higher than the maximum.
Severity	Critical.
Direction	Assertion.
Filter Number	5.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The LCP temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	5.
Actions	None.

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

Description	The LCP temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	5.
Actions	None.

B.2.2. CMM SEL Messages

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

Description	The CMM temperature is lower than the minimum.
Severity	Critical.
Direction	Assertion.
Filter Number	1.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The CMM temperature is upper than the maximum.
Severity	Critical.
Direction	Assertion.
Filter Number	1.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The CMM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	1.
Actions	None

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

Description	The CMM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	1.
Actions	None.

B.2.3. ESM / TSM SEL Messages

ESM /TSM Temperature : At or below lower critical threshold (going low)

Description	The ESM /TSM temperature is lower than the minimum.
Severity	Critical.
Direction	Assertion.
Filter Number	2.
Actions	Check environmental conditions (fan, air conditioning).

ESM /TSM Temperature: At or above upper critical threshold (going high)

Description	The ESM /TSM temperature is upper than the maximum.
Severity	Critical.
Direction	Assertion.
Filter Number	2.
Actions	Check environmental conditions (fan, air conditioning).

ESM /TSM Temperature: At or below lower critical threshold (going low)

Description	The ESM /TSM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	2.
Actions	None

ESM /TSM Temperature: At or above upper critical threshold (going high)

Description	The ESM /TSM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	2.
Actions	None.

B.2.4. QSM SEL Messages

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

Description	The QSM temperature is lower than the minimum.
Severity	Critical.
Direction	Assertion.
Filter Number	6.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The QSM temperature is upper than the maximum.
Severity	Critical.
Direction	Assertion.
Filter Number	6.
Actions	Check environmental conditions (fan, air conditioning).

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

Description	The QSM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	6.
Actions	None

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

Description	The QSM temperature is now OK.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	6.
Actions	None.

QSM Presence: Device removed/Device absent

Description	The QSM is not present.
Severity	Information.
Direction	Assertion.
Filter Number	29.
Actions	Insert QSM.

QSM Presence: Device inserted/Device present

Description	The QSM is present.
Severity	Information.
Direction	Assertion.
Filter Number	29.
Actions	None.

B.2.5. UCM SEL Messages

UCM Presence: Device removed/Device absent

Description	The UCM is not present.
Severity	Information.
Direction	Assertion.
Filter Number	30.
Actions	Insert UCM.

UCM Presence: Device inserted/Device present

Description	The UCM is present.
Severity	Information.
Direction	Assertion.
Filter Number	30.
Actions	None.

UCM Vcap X: At or below lower non-critical threshold (going low)

Description	UCM Vcap X Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or above upper non-critical threshold (going high)

Description	UCM Vcap X Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or below lower non-critical threshold (going low)

Description	UCM Vcap X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or above upper non-critical threshold (going high)

Description	UCM Vcap X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or below lower critical threshold (going low)

Description	UCM Vcap X Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or above upper critical threshold (going high)

Description	UCM Vcap X Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or below lower critical threshold (going low)

Description	UCM Vcap X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM Vcap X Voltage: At or above upper critical threshold (going high)

Description	UCM Vcap X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	208 for Vcap 1, 209 for Vcap 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X: At or below lower non-critical threshold (going low)

Description	UCM 21V X Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or above upper non-critical threshold (going high)

Description	UCM 21V X Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or below lower non-critical threshold (going low)

Description	UCM 21V X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or above upper non-critical threshold (going high)

Description	UCM 21V X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or below lower critical threshold (going low)

Description	UCM 21V X Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or above upper critical threshold (going high)

Description	UCM 21V X Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or below lower critical threshold (going low)

Description	UCM 21V X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 21V X Voltage: At or above upper critical threshold (going high)

Description	UCM 21V X Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	210 for 21V 1, 211 for 21V 2.
Actions	None.
Comments	X=1 or 2.

UCM 12V: At or below lower non-critical threshold (going low)

Description	UCM 12V Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	212.
Actions	None.

UCM 12V Voltage: At or above upper non-critical threshold (going high)

Description	UCM 12V Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	212.
Actions	None.

UCM 12V Voltage: At or below lower non-critical threshold (going low)

Description	UCM 12V Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	212.
Actions	None.

UCM 12V Voltage: At or above upper non-critical threshold (going high)

Description	UCM 12V Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	212.
Actions	None.

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

Description	UCM 12V Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	212.
Actions	None.

UCM 12V Voltage: At or above upper critical threshold (going high)

Description	UCM 12V Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	212.
Actions	None.

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

Description	UCM 12V Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	212.
Actions	None.

UCM 12V Voltage: At or above upper critical threshold (going high)

Description	UCM 12V Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	212.
Actions	None.

UCM Vref: At or below lower non-critical threshold (going low)

Description	UCM Vref Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or above upper non-critical threshold (going high)

Description	UCM Vref Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or below lower non-critical threshold (going low)

Description	UCM Vref Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	213.
Actions	None.

UCM Vref: At or above upper non-critical threshold (going high)

Description	UCM Vref Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or below lower critical threshold (going low)

Description	UCM Vref Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or above upper critical threshold (going high)

Description	UCM Vref Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or below lower critical threshold (going low)

Description	UCM Vref Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	213.
Actions	None.

UCM Vref Voltage: At or above upper critical threshold (going high)

Description	UCM Vref Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	213.
Actions	None.

UCM SX CY: At or below lower non-critical threshold (going low)

Description	UCM SX CY Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or above upper non-critical threshold (going high)

Description	UCM SX CY Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or below lower non-critical threshold (going low)

Description	UCM SX CY Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or above upper non-critical threshold (going high)

Description	UCM SX CY Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or below lower critical threshold (going low)

Description	UCM SX CY Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or above upper critical threshold (going high)

Description	UCM SX CY Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or below lower critical threshold (going low)

Description	UCM SX CY Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

UCM SX CY Voltage: At or above upper critical threshold (going high)

Description	UCM SX CY Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	214 for S1 C2, 215 for S1 C4, 216 for S2 C2, 217 for S2 C4.
Actions	None.
Comments	X=1 or 2, Y=2 or 4.

B.2.6. PSU SEL Messages

PSU-X Presence: Device removed / Device absent

Description	PSU-X is not present.
Severity	Information.
Direction	Assertion.
Filter Number	31 for PSU-1 to 34 for PSU-4.
Actions	If the PSU-X is physically present: remove it and re-insert it. If the problem persists, replace the power supply.
Comments	X=1, 2, 3 or 4.

PSU-X Presence: Device inserted/ Device present

Description	PSU-X is present.
Severity	Information.
Direction	Assertion.
Filter Number	31 for PSU-1 to 34 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or below lower non-critical threshold (going low)

Description	PSU Input Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or above upper non-critical threshold (going high)

Description	PSU Input Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or below lower non-critical threshold (going low)

Description	PSU Input Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or above upper non-critical threshold (going high)

Description	PSU Input Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or below lower critical threshold (going low)

Description	PSU Input Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or above upper critical threshold (going high)

Description	PSU Input Voltage Greater than Expected
Severity	Critical.
Direction	Assertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or below lower critical threshold (going low)

Description	PSU Input Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Voltage: At or above upper critical threshold (going high)

Description	PSU Input Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	71 for PSU-1 to 74 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or above upper critical threshold (going high)

Description	PSU Input Current Greater than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or above upper critical threshold (going high)

Description	PSU Input Current Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or above upper non-critical threshold (going high)

Description	PSU Input Current Greater than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or above upper non-critical threshold (going high)

Description	PSU Input Current Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or below lower critical threshold (going low)

Description	PSU Input Current Lower than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or below lower critical threshold (going low)

Description	PSU Input Current Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or below lower non-critical threshold (going low)

Description	PSU Input Current Lower than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Input Current: At or below lower non-critical threshold (going low)

Description	PSU Input Current Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	81 for PSU-1 to 84 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: Failure Detected Asserted

Description	PSU Failure.
Severity	Critical.
Direction	Assertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	Replace PSU.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: Predictive Failure Asserted

Description	Predictive PSU Failure.
Severity	Critical.
Direction	Assertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	Replace PSU.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: AC Input Lost

Description	PSU AC Input Lost.
Severity	Critical.
Direction	Assertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	Connect/Check AC Cable.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: Failure Detected Asserted

Description	PSU failure is no more asserted.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: Predictive Failure Asserted

Description	Predictive PSU Failure is no more asserted.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Failure: AC Input Lost

Description	PSU AC Input Lost is no more asserted.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	76 for PSU-1 to 79 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or below lower critical threshold (going low)

Description	PSU Output Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or below lower non-critical threshold (going low)

Description	PSU Output Voltage Lesser than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or above upper critical threshold (going high)

Description	PSU Output Voltage Greater than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or above upper non-critical threshold (going high)

Description	PSU Output Voltage Greater than Expected.
Severity	Critical.
Direction	Assertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or below lower non-critical threshold (going low)

Description	PSU Output Voltage Returning To Normal.
Severity	Return to OK
Direction	Deassertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or below lower critical threshold (going low)

Description	PSU Output Voltage Returning To Normal.
Severity	Return to OK
Direction	Deassertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or above upper critical threshold (going high)

Description	PSU Output Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Voltage: At or above upper non-critical threshold (going high)

Description	PSU Output Voltage Returning To Normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	85 for PSU-1 to 88 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Current: At or above upper critical threshold (going high)

Description	PSU output current greater than expected.
Severity	Critical.
Direction	Assertion.
Filter Number	89 for PSU-1 to 92 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Current: At or above upper critical threshold (going high)

Description	PSU output current returning to normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	89 for PSU-1 to 92 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Current: At or above upper critical threshold (going high)

Description	PSU output current greater than expected.
Severity	Critical.
Direction	Assertion.
Filter Number	89 for PSU-1 to 92 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

PSU-X Output Current: At or above upper critical threshold (going high)

Description	PSU output current returning to normal.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	89 for PSU-1 to 92 for PSU-4.
Actions	None.
Comments	X=1, 2, 3 or 4.

B.2.7. FAN SEL Messages

FAN 1A/1B/2A/2B Speed : At or below lower critical threshold (going low)

Description	Fan speed is lesser than expected.
Severity	Critical.
Direction	Assertion.
Filter Number	7 for FAN 1A, 8 for FAN 1B, 9 for FAN 2A, 10 for FAN 2B.
Actions	If the problem persists, change fan.

FAN 1A/1B/2A/2B Speed : At or below lower critical threshold (going low)

Description	Fan speed is lesser than expected.
Severity	Return to OK.
Direction	Deassertion.
Filter Number	7 for FAN 1A, 8 for FAN 1B, 9 for FAN 2A, 10 for FAN 2B.
Actions	None.

B.2.8. BLADE SEL Messages

Blade_X Presence: Device removed / Device absent

Description	Blade is not present.
Severity	Information.
Direction	Assertion.
Filter Number	11 for Blade 1 to 28 for Blade 18.
Actions	Insert blade X.
Comments	X=1 to 18.

Blade_X Presence: Device inserted / Device present

Description	Blade is present.
Severity	Information.
Direction	Assertion.
Filter Number	11 for Blade 1 to 28 for Blade 18.
Actions	None.
Comments	X=1 to 18.

Blade_X 3V3 PG: State Deasserted

Description	3v3 PG is not present.
Severity	Information.
Direction	Assertion.
Filter Number	35 for Blade 1 to 52 for Blade 18.
Actions	None.
Comments	X=1 to 18.

Blade_X 3V3 PG: State asserted

Description	3V3 PG is present.
Severity	Information.
Direction	Assertion.
Filter Number	35 for Blade 1 to 52 for Blade 18.
Actions	None.
Comments	X=1 to 18.

Blade_X Sys PG: State Deasserted

Description	SYS PG is not present.
Severity	Information.
Direction	Assertion.
Filter Number	53 for Blade 1 to 70 for Blade 18.
Actions	None.
Comments	X=1 to 18.

Blade_X Sys PG: State asserted

Description	SYS PG is present.
Severity	Information.
Direction	Assertion.
Filter Number	53 for Blade 1 to 70 for Blade 18.
Actions	None.
Comments	X=1 to 18.

Notes
- 3v3 PG (Power Good) means 3.3V power is running in the blade.
- SYSPG (SYStem Power Good) means 12V power is running in the blade.

Glossary

A

ABR
Automatic BIOS Recovery.

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

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

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

ASR
Automatic Server Restart.

ASIC
Application Specific Integrated Circuit.

B

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

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

BHC
See Blade Hardware Console.

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

BIST
Built-In Self-Test. See POST.

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

BMC
Baseboard Management Controller. See Embedded Management Controller.

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

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

C

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

CHC
See Chassis Hardware Console.

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

CMB
Chassis Management Board.

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

CMC
Chassis Management Controller.

CMM
Chassis Management Module.

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

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

CSE
Customer Service Engineer.

D

DES
Data Encryption Standard.

DHCP
Dynamic Host Configuration Protocol.

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

DNS
Domain Name Server.

E

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

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

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

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

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

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

ESB
Ethernet Switch Board.

ESM
Ethernet Switch Module.

F

FC-LGA
Flip-Chip Land Grid Array.

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

FPGA
Field Programmable Gate Array.

FQDN
Fully Qualified Domain Name.

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

G

GPU
Graphical Processing Unit.

GUI
Graphical User Interface.

H

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

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

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

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

HPC
High Performance Computing.

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

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

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

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

HT
HyperThreading. See Multi-Threading.

I

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

IB
InfiniBand.

iBMC
Integrated Baseboard Management Controller. See Embedded Management Controller.

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

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

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

ILB / ILBC
I/O Legacy Board / I/O Legacy Board Controller.

INCA
INtegrated Cluster Architecture.

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

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

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

J

JOEM
JTAG Over Ethernet Module.

JTAG
Joint Test Action Group.

K

No entries.

L

LAN
Local Area Network.

LCD
Liquid Crystal Display.

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

LDAP
Lightweight Directory Access Protocol.

LED
Light Emitting Diode.

Logical Partition
When the Base Operating System is a Virtual Machine Monitor, a logical partition is the software environment used to run a Guest Operating System.

Logical Processor
See Thread.

M

MAC
Media Access Control.

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

MESCA
Multiple Environments on a Scalable Csi-based Architecture.

MIB
Management Interface Base.

MIMD
Multiple Instruction Multiple Data

MMX
MultiMedia eXtensions.

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

MTBF
Mean Time Between Failure.

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

Multi-Threading
The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.
Depending on core design, the instructions issued for execution by the core at a given cycle may be either **Hyper-Threading** (HT) - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or **Simultaneous Multi-Threading** (SMT) - from both threads.

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

N

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

NFS
Network File System.

NIC
Network Interface Controller.

NUMA
Non Uniform Memory Access.

NVRAM
Non-Volatile Random Access Memory.

O

Off-Lining
See On-Lining / Off-Lining.

On-Lining / Off-Lining
On-lining and off-lining are dynamic logical operations. On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected). Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

OOB
Out Of Band. Access to system platform management that does not go through the OS or other software running on the main processors of the managed system.

OPMA
Open Platform Management Architecture.

P

PCI
Peripheral Component Interconnect. Bus architecture supporting high-performance peripherals.

PCIe
PCI Express. Latest standard in PCI expansion cards.

PDB
Power Distribution Board. Sub-assembly of the Power Supply Module.

PDU
Power Distribution Unit. Power bus used for the connection of peripheral system components.

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

PEF
Platform Event Filtering.
A feature in IPMI that enables the BMC to generate a selectable action (e.g. power on/off, reset, send Alert, etc.) when a configurable event occurs on the management system.

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

PIROM
The Processor Information ROM contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S-spec numbers, and a 64-bit processor number.

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

POST
Power On Self Test.

Processor
Each processor contains one or more dies in a single package. Each die contains one or more cores. Each core contains one or more threads (logical processors). Each processor is housed in a processor socket.

PSMI
Power Supply Management Interface.

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

PSWB
PCI SWitch Board.

PSWM
PCI SWitch Module.

PWM
Pulse Width Modulation.

Q

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

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

QSB
Quad Switch Board.

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

QSMB
Quad Switch Module. InfiniBand Switch.

R

RADIUS
Remote Authentication Dial-In User Service.

RAS
Reliability, Availability, Serviceability.

RMII
Reduced Media Independent Interface. A standard that reduceds the number of signals/pins required to connect an Ethernet chip to physical layer transceiver. See MII.

RTC
Real Time Clock.

S

SAS
Serial Attached SCSI. A data transfert technology used to move data to and from computer storage devices such as hard drives and tape drives.

SATA
Serial ATA. A computer bus technology for connecting hard disks and other devices.

SEL
System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.
A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

Server Hardware Console
Graphical user interface used to access the management software embedded in the server module.

SHC
See Server Hardware Console.

Simultaneous Multi-Threading
See Multi-Threading.

SMBIOS
System Management BIOS.

SM-BUS
System Management Bus.

SMI
System Management Interrupt.

SMP
Symmetrical Multi Processor. The processing of programs by multiple processors that share a common operating system and memory.

SMT
Simultaneous Multi-Threading.

SMTP
Simple Mail Transfer Protocol.

SNC
Scalable Node Controller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

SNMP
Simple Network Management Protocol.

SoC
System on Chip.

Socket
Central Processing Unit mutlticore interface.

SOL
Serial Over LAN. Mechanism that enables the input and output of the serial port of a managed system to be redirected via an IPMI session over IP.

SO-DIMM
Small Outline Dual In-line Memory.

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

SSH
Secured Shell.

SSL
Secure Socket Layer.

T

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

Thread
A thread or logical processor is the execution context within a single core and the software visibility of multi-threading. A single multi-threaded processor contains two or more threads (or logical processors).

Thresholding
An Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, this message is selected for routing.

TKW
TUKWILA Intel Itanium Processor (4 cores per socket).

U

UCM
Ultra Capacitor Module.

UVLO
Under Voltage Latch Output.

V

VMM
Virtual Machine Monitor.

W

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

X

XCSI
Extended Common System Interface. High-speed point-to-point Bull interface, used to interconnect servers. XCSI ports are located and managed in the BCS (node controller).

XNC
External Node Controller. See BCS.

Y

No entries.

Z

No entries.

Index

V

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

REFERENCE
86 A1 50FB 07