User Guide

HP BladeSystem PC Blade Enclosure Integrated Administrator for CCI v1.5

User Guide

Business PCs

First Edition (May 2007)

Document Part Number: 449377-001

About This Book

⚠ **WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

△ **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

NOTE: Text set off in this manner provides important supplemental information.

Table of contents

1 About this guide

Audience assumptions

This guide is for the person who installs, administers, and troubleshoots HP CCI solutions. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Important Safety Information

⚠ **WARNING!** Before installing this product, read the Important Safety Information document included with the system.

Symbols on Equipment

The following symbols may be placed on equipment to indicate the presence of potentially hazardous conditions:

	This symbol, in conjunction with any of the following symbols, indicates the presence of a potential hazard. The potential for injury exists if warnings are not observed. Consult your documentation for specific details.
	This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel. **WARNING**: To reduce the risk of injury from electric shock hazards, do not open this enclosure. Refer all maintenance, upgrades, and servicing to qualified personnel.
	This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason. **WARNING**: To reduce the risk of injury from electric shock hazards, do not open this enclosure.
	This symbol on an RJ-45 receptacle indicates a network interface connection. **WARNING**: To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.
	This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists. **WARNING**: To reduce the risk of injury from a hot component, allow the surface to cool before touching.
	These symbols, on power supplies or systems, indicate that the equipment is supplied by multiple sources of power.

	WARNING: To reduce the risk of injury from electric shock, remove all power cords to completely disconnect power from the system.
	This symbol indicates that the component exceeds the recommended weight for one individual to handle safely. **WARNING**: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Related Documents

For additional information on the topics covered in this guide, refer to the following documents:

- *Network Considerations Guide* white paper
- *QuickSpecs*
- *Setup and Installation Guide: HP BladeSystem bc2000 and bc2500 Blade PC and PC Blade Enclosure*
- *HP Rack 9000 and 10000 Series installation and best practices* white paper
- *Installation Guide: HP BladeSystem PC Blade Switch*
- *Command Line Interface Reference Guide: HP BladeSystem PC Blade Switch*
- *Embedded Web System User Guide for the HP BladeSystem PC Blade Switch*

Getting help

If you have a question about the HP PC Blade Enclosure and have exhausted the information in this guide, you can get additional information and other help in the following locations:

Contact HP

The Contact HP Web site provides various ways to contact HP, including online chat, email, and telephone. Access this Web site at: http://welcome.hp.com/country/us/en/contact_us.html

Support and Troubleshooting

HP's Support and Troubleshooting Web site allows you to download software and drivers and search for support and troubleshooting information for specific products. Access this Web site at: http://welcome.hp.com/country/us/en/support.html.

HP Web Site

The HP Web site has information on this product as well as the latest drivers and flash ROM images. You can access the HP Web site at http://www.hp.com.

Reader Comments

HP welcomes your comments on this guide. Go to the following site to send your comments and suggestions: www.hp.com/go/cci.

2 HP PC Blade Enclosure System Software Features

The HP BladeSystem offers an extensive set of features and optional tools to support effective blade PC management and software deployment. This chapter describes the HP PC Blade Enclosure Integrated Administrator and provides a brief overview of software associated with the system.

HP PC Blade Enclosure Integrated Administrator

The HP PC Blade Enclosure Integrated Administrator is a centralized management and monitoring system for the HP PC Blade Enclosure and blade PCs. The Integrated Administrator acts as a combination terminal server and remote power controller, enabling out-of-band, secure, serial console connections to all blade PCs in the enclosure.

The Integrated Administrator provides enclosure health, blade health, and remote blade manageability. Integrated Administrator features are accessed from any network-based client. The Integrated Administrator provides remote access to any authorized network client, sends alerts, and provides many other blade PC management functions.

The Integrated Administrator subsystem is embedded on a module included with each interconnect tray and includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes the Integrated Administrator independent of the host blade PC and its operating system.

Integrated Administrator Features

The following subsections describe Integrated Administrator functions that deliver state-of-the-art management of the enclosure and blade PCs.

Dedicated LAN network connectivity

Each Integrated Administrator provides a dedicated network connection. The NIC can auto-select speeds between 10 Mbps and 100 Mbps. When the PC Blade Switch (optional) is installed, you can configure the Integrated Administrator to route through a Gigabit uplink connector using VLANs, eliminating the need for a separate management network.

NOTE: The default configuration for the HP BladeSystem PC Blade Switch option has the dedicated IA port and both Switch A and Switch B uplinks in the same VLAN.

SNMP alerts from Integrated Administrator to a management console

The Integrated Administrator provides notification of enclosure problems. Using a management console, you can access various alerts, such as unauthorized access attempts and network connection failures using SNMP traps.

E-mail alerts from Integrated Administrator to an e-mail account (AlertMail)

AlertMail enables the Integrated Administrator to send system events by email instead of using SNMP traps. AlertMail is completely independent of SNMP, and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with any SMTP capable mail server or SMTP relay agent.

Remote access and control

The Integrated Administrator provides remote functionality to access a limited text-only console of the host blade PC, change the state of the Unit Identification LED on an enclosure or any of its blade PCs, and power up, power down, or reboot a blade PC or groups of blade PCs.

The Integrated Administrator displays alerts regardless of the state of the user's host blade PC and integrates with the HP Systems Insight Manager utility using SNMP to provide alerts and diagnostics of the system.

If a blade PC does not respond, this feature enables an administrator to initiate a cold reboot to bring the blade PC back online. The Integrated Administrator can be used to remotely operate a power button of any blade PC within the enclosure.

Integrated Administrator is fully accessible by common Web browsers. The Integrated Administrator also has a command line interface (CLI) accessible using Secure Shell (encrypted) or Telnet (unencrypted) protocols, providing extensive management capability to remote network users. Local users can access the CLI by attaching a client computer (using a terminal emulator) or terminal to the Integrated Administrator's console (RS-232 serial) port.

NOTE: With a Telnet session, all data - including passwords - are passed as clear text.

User administration and security

The Integrated Administrator supports up to 25 users with customizable access rights and login names. Groups are first assigned bays, and then users are given membership to those groups. This group-centered methodology is designed to facilitate user management across blade PCs.

Integrated Administrator provides strong security for remote management in distributed IT environments by using industry standard Secure Sockets Layer (SSL) encryption of HTTP data transmitted across the network. SSL encryption (up to 128-bit) ensures that the HTTP information is secure as it travels across the network. You can encrypt all remote console data as well.

Integrated Administrator provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. Integrated Administrator also provides the following additional security features:

- User actions logged in the Integrated Administrator System Log
- Login legal warning

IP Security allows an administrator to define a set of IP addresses that are the only ones allowed to connect to the services provided (SSH, HTTP, HTTPS, TELNET, SNMP). This means that an administrator can make sure only a certain set of machines have access to Integrated Administrator.

Automatic network configuration

The Integrated Administrator provides automatic network configuration of the IP address and host name using Dynamic Host Configuration Protocol (DHCP) and Dynamic DNS/WINS. Integrated Administrator comes with a default name and DHCP client that leases an IP address from the DHCP server on the network. For networks that do not use DHCP, the Integrated Administrator can use a static IP configuration.

Automatic time configuration (NTP)

Automatic time configuration allows Integrated Administrator to synchronize its date and time with a blade PC supporting the Network Time Protocol (NTP).

Integration with the HP Systems Insight Manager utility

Integrated Administrator provides full integration with the HP Systems Insight Manager utility under key operating environments. This integration provides:

- Support for SNMP management—Support for SNMP trap delivery to a HP Systems Insight Manager console
- Management processor—The HP Systems Insight Manager utility adds support for a new device type, the management processor. All Integrated Administrators (in HP PC Blade Enclosure) on the network are discovered in the HP Systems Insight Manager utility as management processors. The management processors are associated with the blade PCs they manage.
- Integrated Administrator hyperlinks—The HP Systems Insight Manager utility provides a hyperlink on the blade PC device page to launch and connect to Integrated Administrator.
- Grouping of Integrated Administrator processors—All Integrated Administrator management processors can be grouped together logically and displayed on one page in the HP Systems Insight Manager utility. This capability provides access to all Integrated Administrators on the network from one point in HP Systems Insight Manager.

  For more information on the HP Systems Insight Manager utility, refer to the ProLiant Essentials Foundation Pack documentation that ships with the system or refer to: http://h18013.www1.hp.com/products/servers/management/hpsim/index.html.

Event Notification

The Integrated Administrator provides real-time event notifications for an enclosure. When an event occurs, the Integrated Administrator notifies connected users by generating an icon that the user can click to view more details.

Status Information

The Integrated Administrator enables an enclosure administrator to update the rack name, enclosure name, asset tag, time zone, date, and time, as well as observe the status and general information for every component in the enclosure.

Overview of HP BladeSystem Software Tools

The following subsections described tools and utilities supported by the HP BladeSystem blade PC systems to facilitate monitoring and management of the enclosure.

ROM-Based Setup Utility (RBSU)

RBSU performs a wide range of configuration activities and provides access to numerous settings, including those for system devices, operating system selection, and boot controller order. RBSU is also fully compatible with remote serial console mode using the Integrated Administrator.

Headless operation

HP bc-series blade PCs include VGA, keyboard, mouse, and USB interfaces; however, these blade PCs are designed primarily for headless operation and management with no keyboard or monitor attached.

ProLiant Essentials Rapid Deployment Pack

The ProLiant Essentials Rapid Deployment Pack features a graphical deployment console, which provides intuitive drag-and-drop events, such as scripts and images, to deploy the operating systems and applications on any combination of blade PCs installed in the enclosures.

With the Rapid Deployment Pack, users can automatically install pre-defined configurations on newly installed blade PCs. For more information about the Rapid Deployment Pack, refer to an authorized reseller, the Rapid Deployment CD that ships with the enclosure, or go to: www.hp.com/servers/rdp.

HP Systems Insight Manager

HP Systems Insight Manager is an easy-to-use, intuitive software utility designed for collecting blade PC information, including fault conditions, performance, security, remote management, and recovery services. The HP BladeSystem is fully compatible with the HP Systems Insight Manager utility.

HP Blade PC Automatic System Recovery (ASR-2)

ASR-2 is a diagnostic/recovery feature that automatically restarts the blade PC in the event of a critical operating system failure.

Enclosure Self Recovery (ESR)

ESR, similar to ASR-2, is a self-monitoring reliability feature of the Integrated Administrator. If the Integrated Administrator does not boot or hangs during operation, ESR automatically resets the Integrated Administrator for an attempted self-recovery. The blade PCs and interconnect tray are not affected by ESR.

HP PC Blade Enclosure Management System and Utilities

The HP PC Blade Enclosure Management System and Utilities provide a full suite of configuration and management interfaces and tools for the HP PC Blade Enclosure (option). Full featured Web-based and menu-driven console interfaces are provided management of the interconnect switch.

You can configure both interfaces to require a valid user name and password for authentication. RMON and SNMP manageability are supported with an SNMP-based scripting utility and sample scripts. You

can also save the interconnect switch configuration to a TFTP server as backups and as templates for preconfiguring other switches.

The interconnect switch is compatible with industry standards and has full for support for IEEE 802.1Q VLANs.

3 Getting Started

The HP PC Blade Enclosure Integrated Administrator enables monitoring and management of all functions within an enclosure, including functions specific to the blade PCs housed within it. Once configured, the Integrated Administrator provides these features through both a Web-based user interface and CLI.

This chapter addresses first-time configuration of the Integrated Administrator after the enclosure is installed and powered up in a rack:

- Reviewing configuration tools and information
- Identifying the Integrated Administrator connectors
- Determining the Integrated Administrator initial IP address
- Setting up the Web-based user interface
- Additional steps
- Help

Reviewing Configuration Tools and Information

The Integrated Administrator is ready for operation immediately after powering up. The following features and information are designed to facilitate the setup and management of the Integrated Administrator:

- Each Integrated Administrator ships with a unique preconfigured Administrator password and host name.
- If the network uses Dynamic DNS or WINS, you can access the Integrated Administrator using the factory-configured host name.

NOTE: The preconfigured Administrator password and host name are displayed on the Integrated Administrator Default Network Settings Tag (settings tag) attached to the interconnect tray.

- If the network uses DHCP, an IP address can be automatically assigned to the Integrated Administrator.
- The blade PC health driver enables the Integrated Administrator to gracefully power down the blade PC and provides the Integrated Administrator with the name as defined within the operating system of the blade PC, thermal condition, status, and operating system for each blade PC.

△ **CAUTION:** Without the blade PC health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shut down a blade PC. This condition may result in the permanent loss of critical data.

Identifying Integrated Administrator Components

Each HP PC Blade Enclosure interconnect tray ships with the Integrated Administrator module already installed and provides external connectivity using two connectors on the rear panel.

△ **CAUTION:** Do not plug anything into the enclosure link connectors. They are reserved for future use and are not designed to accept a 10/100 Ethernet connector.

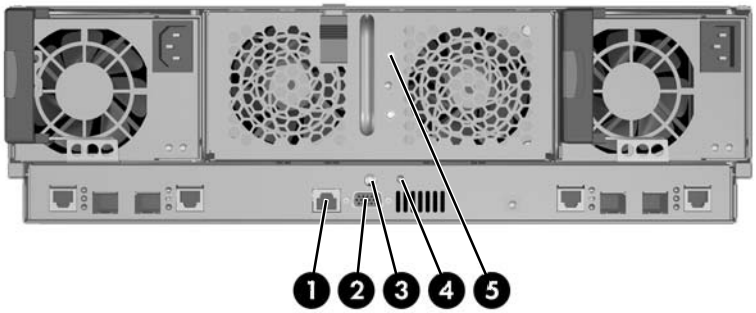


Table 3-1 Integrated Administrator Rear Panel Components

Item	Description
1	Management (10/100 Ethernet) connector for remote access through a Web-based user interface, Telnet, or Secure Shell.
2	Console (serial) connector for local access to the command line interface using a laptop computer.
3	Integrated Administrator reset button.
4	Integrated Administrator health LED
5	Enclosure Unit Identification button/LED

Determining the Integrated Administrator's Initial IP Address

HP recommends that you connect a local client device, such as a laptop computer, to the console (serial) connector in order to determine the initial IP address used by the network to recognize the Integrated Administrator. After using that IP address to access the Integrated Administrator locally using the console (serial) connector, you can use the Integrated Administrator default values to complete the initial configuration.

The organization of this section reflects this process:

- Requirements for local client devices
- Default values for the Integrated Administrator
- Determining the IP address using the local console

Requirements for Local Client Devices

You can access the Integrated Administrator locally using the serial connector on the rear panel of the enclosure using a local client device, such as a laptop computer. The local client device must run a terminal emulator, such as HyperTerminal for Windows systems or Kermit for Linux systems.

The terminal emulator must operate at the following settings:

- Bits per second: 9600
- Bits: 8
- Parity: None
- Stop bits: 1
- Flow control: none
- Emulation: VT100
- Backspace key sends Ctrl-H

Default Values for the Integrated Administrator

The Integrated Administrator is configured with a default user name, password, and DNS name. A settings tag with the preconfigured values is attached to the interconnect tray containing the Integrated Administrator module.

NOTE: For security reasons, HP recommends changing the Administrator password when accessing Integrated Administrator for the first time.

Determining the IP Address using the Local Console

To determine the Integrated Administrator IP address using the local console perform the following steps:

1. Access the Integrated Administrator console:
   a. Connect a local client device (such as a laptop computer) with VT100 terminal emulation software to the Integrated Administrator (serial) console connector using a null modem serial cable.
   b. Open a terminal emulation session with the following settings: 9600 bps, 8 data bits, no parity, and 1 stop bit.
   c. Log into the Integrated Administrator using the password on the settings tag attached to the interconnect tray.
2. Establish the Integrated Administrator IP address.

For a detailed explanation of the command line conventions used in this document, see Command Line Conventions on page 118.

If a DHCP server is attached to the network, determine the Integrated Administrator IP address. Type the following command at the command line interface:

```
SHOW NETWORK
```

If a DHCP server is not attached to the network, type the following commands sequentially to assign a static IP address to the Integrated Administrator:

```
SET IPCONFIG STATIC <IP address><subnet mask>

SET GATEWAY <IP address>

SET DNS <primary address> {<secondary address>}
```

You can now access the Integrated Administrator using a Web browser, Secure Shell, Telnet, or SNMP.

Setting Up the Web-Based User Interface

To set up the Web-based user interface, proceed as follows:

1. Type the Integrated Administrator IP address or DNS name in the address bar of the Web browser. A security alert displays as shown below.

   If you click **Yes**, the browser continues to the Login window of Integrated Administrator. The alert message appears each time you access the Integrated Administrator management processor in a browser.

   If you click **No**, you are returned to what was previously displayed on your browser.

   If you click **View Certificate**, a popup window displays the certificate information. Installing the certificate to your browser prevents the security alert message from displaying in the future.

   NOTE: To install your own certificate onto the Integrated Administrator rather than the automatically generated certificate, see the information on certificate-related commands in Administering Security Certificates on page 109.

   If the certificate is removed from your browser, the security alert message is displayed again.

2. Install the certificate to your browser:

   a. Click **Install Certificate**. The Certificate Manager Import Wizard starts.

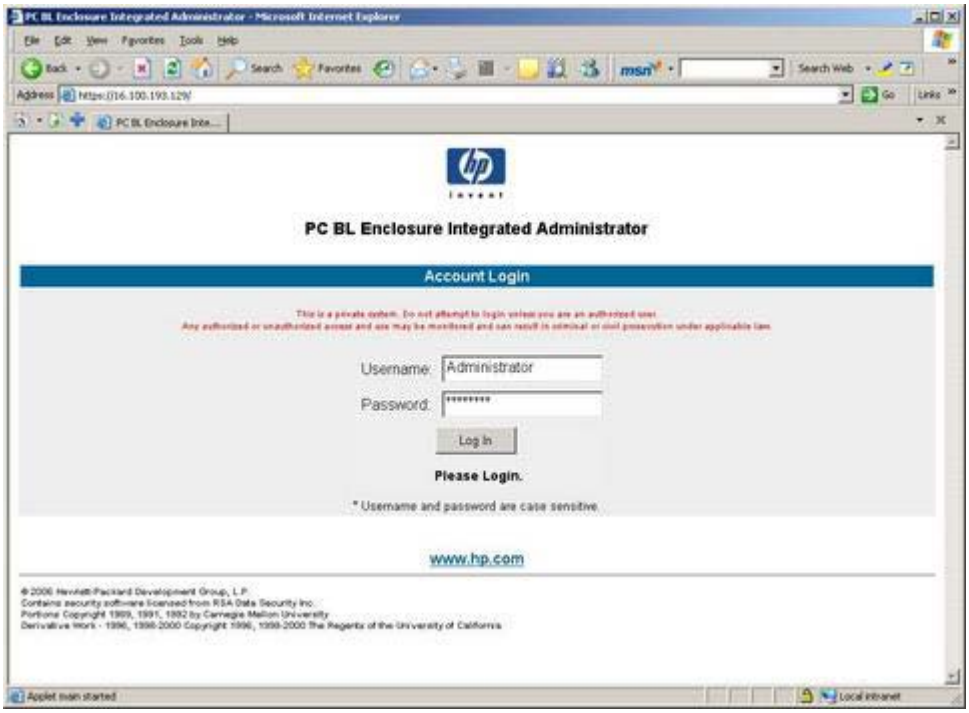
   b. Click **Next**.

   c. Click **Next** for the browser to automatically select the certificate store when the Certificate Store window appears.

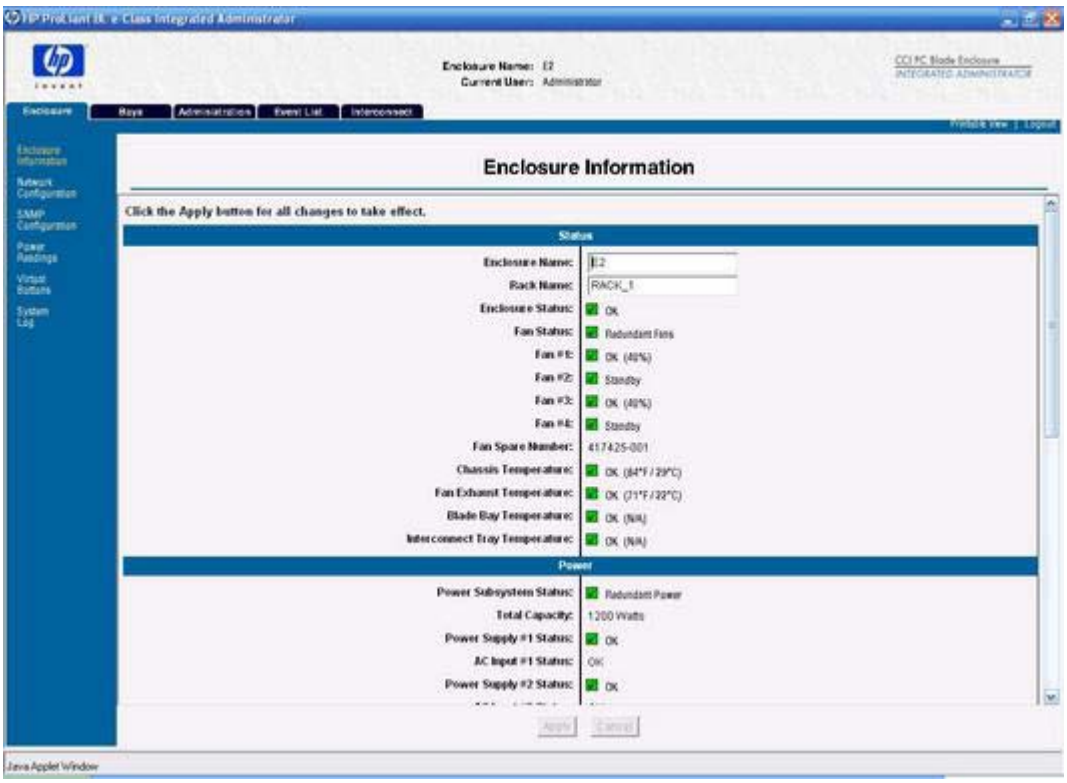
   d. Click **Finish** when the Completing the Certificate Manager Import Manager Wizard window displays.

   e. Click **Yes** to confirm the installation of the certificate when the confirmation window displays.

3. The Account Login screen (shown below) prompts you for a user name and password. Use the default user name and password from the settings tag attached to the interconnect tray, and then click **Log In**.



After the default user name and password have been verified, the summary window appears.



The Integrated Administrator summary window provides general information about the Integrated Administrator, such as the user currently logged on, enclosure name and status, and Integrated Administrator IP address and name.

Additional Steps

HP recommends performing the following tasks:

- Change the Administrator password
- Set the date and time
- Name the enclosure and rack
- Set up groups, users, and access privileges

For detailed instructions on performing these tasks, see the appropriate sections in Setting Up the System on page 67.

Help

Additional assistance is available by means of the Integrated Administrator help option. These links provide summary information about the features of Integrated Administrator and helpful information for optimizing the operation of Integrated Administrator.

4 Web Browser Interface

This chapter provides information for navigating the Integrated Administrator Web-based user interface:

NOTE: Values appearing in the screens of this chapter are for illustrative purposes only.

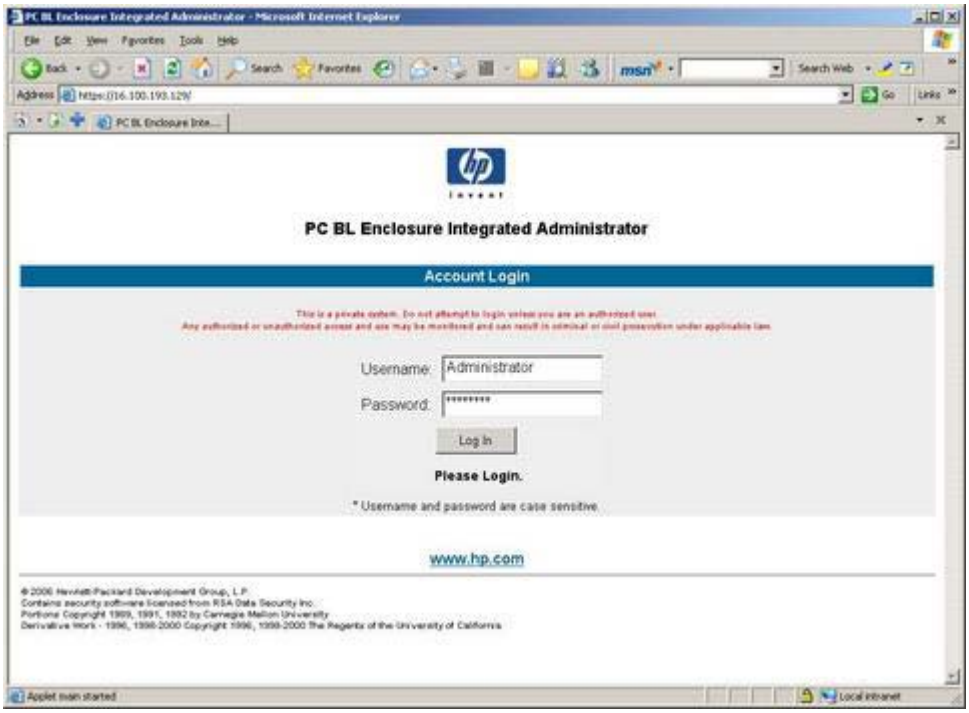
Accessing the Web-based User Interface

Accessing the Web-based user interface is not supported from the console (serial) connector.

To access the Integrated Administrator Web-based user interface with HTTP:

1. Get the DNS name from the settings tag attached to the interconnect tray.
2. Open a Web browser and type the IP address or DNS name for the enclosure to access.

△ **CAUTION:** If your network does not provide DHCP and either Dynamic DNS or WINS services, you need to configure a static IP address. See Determining the IP Address using the Local Console on page 11.



3. Type the user name and password at the **Login** prompt.

Web-Based Navigation

The Web-based user interface displays information and receives input in the following areas:

- Top panel
- Left panel
- Deck panel

Top panel

The following illustration shows the location of the top panel.

The top panel information is displayed at all times, including the following items:

- Enclosure name
- Current user
- Tabs

The Integrated Administrator top panel provides real-time event notifications for an enclosure according to two categories: caution and critical. When an event occurs, the Integrated Administrator notifies the user by generating an icon that the user can click to view more details:

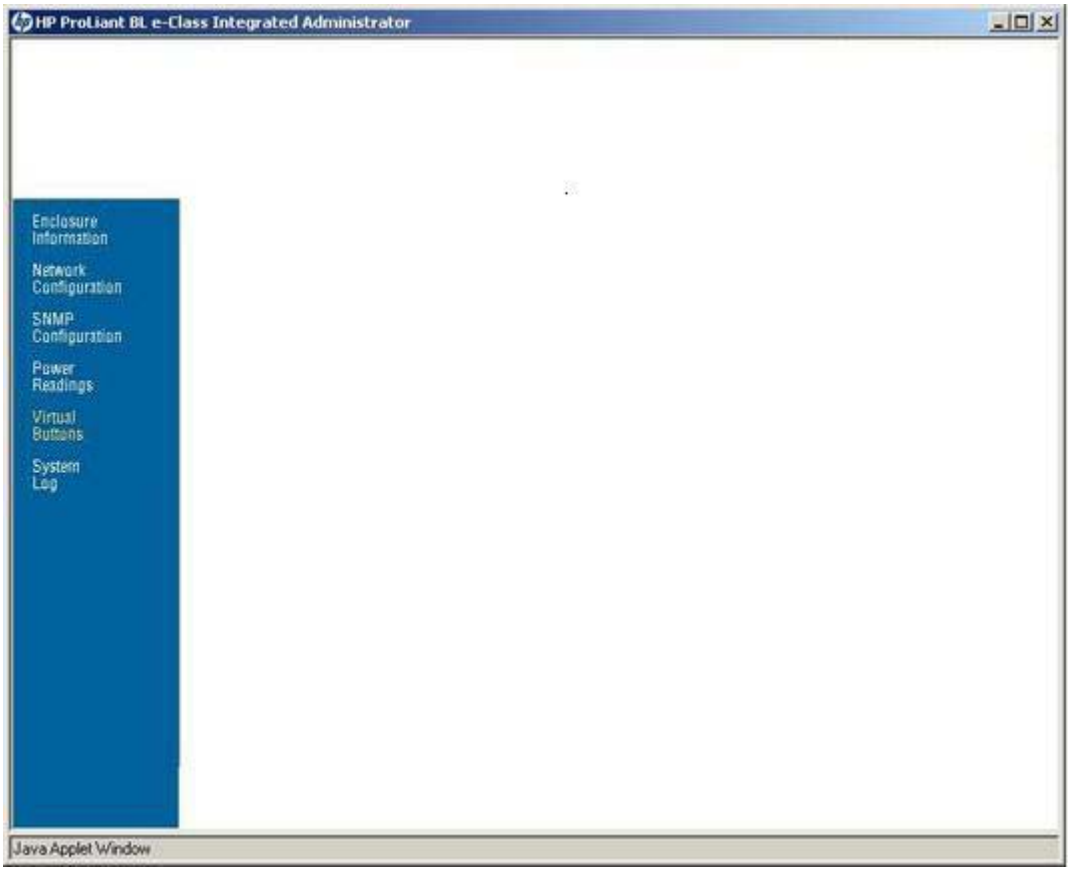
Icon	Descripton
	Caution
	Critical

Two buttons appear on the top panel:

- **Printable View** — Opens a separate window that shows information for cutting and pasting purposes.
- **Log Out** — Logs you out of the Web-based user interface.

Left panel

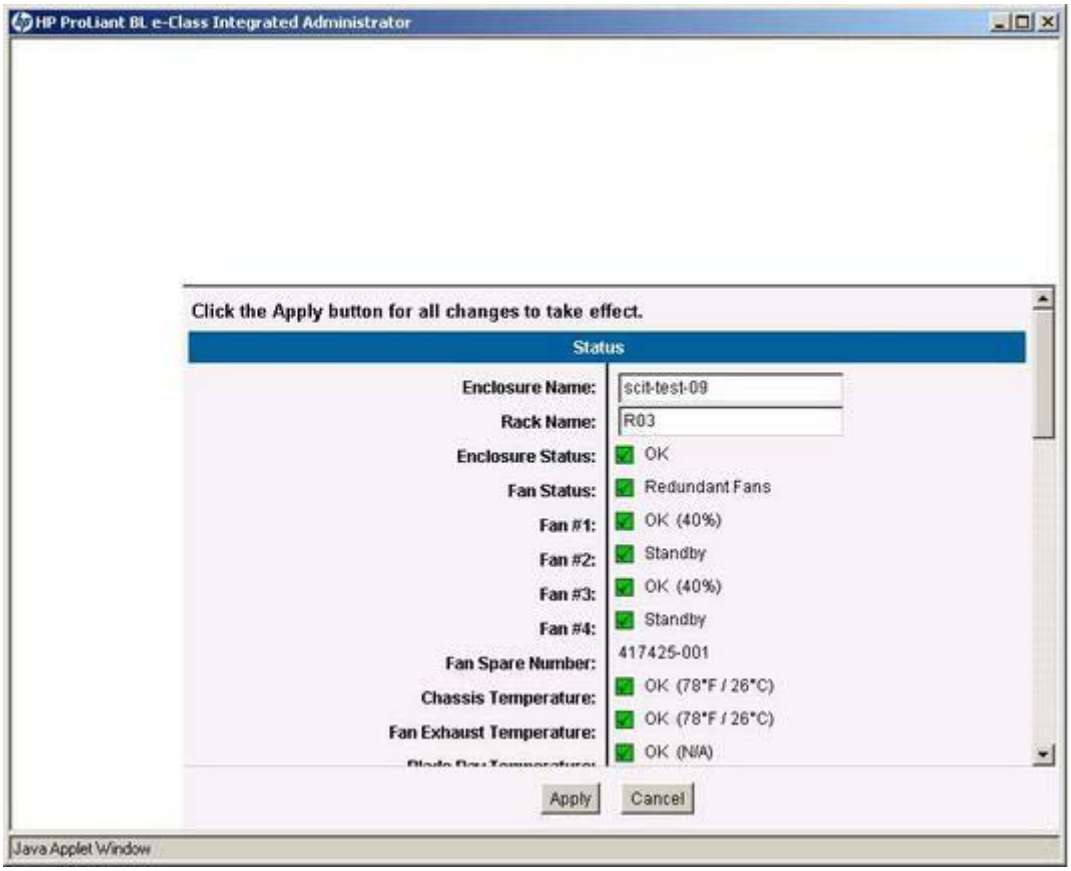
The following illustration shows the location of the left panel.



The left panel displays which screens are available under each tab. Information appearing in the left panel depends on which tab the user chooses from within the top panel.

Deck panel

The illustration below indicates the position of the deck panel.



The deck panel displays the areas of information provided by the available screens under each tab. Information appearing in the deck panel depends on the option chosen by the user from within the top panel and the left panel.

Enclosure Tab

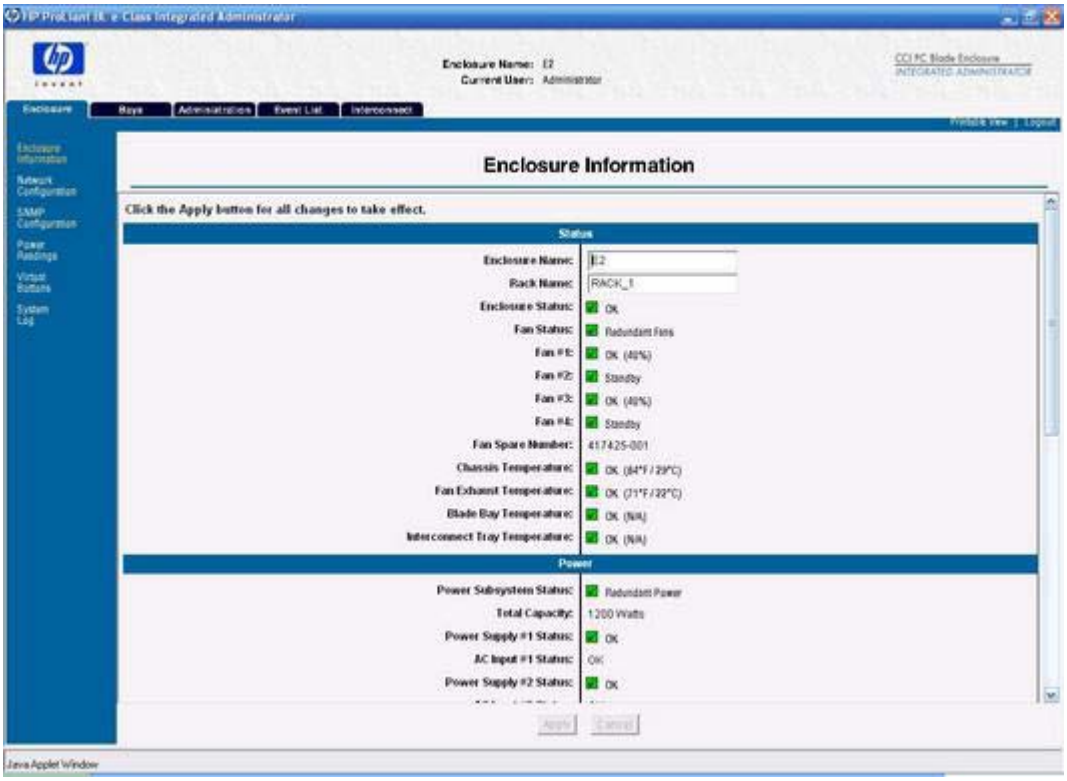
The Enclosure tab provides access to the following screens:

- Enclosure Information
- Network Configuration
- SNMP Configuration
- Virtual Buttons
- System Log

Enclosure Information

All users have read access to the information in this screen.

The following illustration shows the information presented on the Enclosure Information screen (status area, one of six shown).



The Enclosure Information screen enables an enclosure administrator to update the rack name, enclosure name, asset tag, time zone, date, and time, as well as observe the status and general information for every component in the enclosure.

Two buttons appear on the Enclosure Information screen:

- **Apply** — Saves changes made to the screen.
- **Cancel** — Restores all fields on the screen to their original values.

The following table describes the information displayed in the areas that comprise the Enclosure Information screen.

Table 4-1 Enclosure Information Field Descriptions — Status Area

Field	Possible Values	Description
Status Area		
Enclosure Name	Maximum 32 characters including all alphanumeric, dash, and underscore characters.	Name of enclosure. Only enclosure administrators have write access to this field. For the default enclosure name, see Factory Default Settings on page 128.
Rack Name	Maximum 32 characters including all alphanumeric, dash, and underscore characters.	Name of rack. Only enclosure administrators have write access to this field. For the default rack name, see Factory Default Settings on page 128.

Table 4-1 Enclosure Information Field Descriptions — Status Area (continued)

Enclosure Status	OK, Degraded, or Failed.	Status of the enclosure.
Fan Status	Redundant or non-redundant.	Redundant: all fans are functional. Non-redundant: at least one fan is not functional.
Fan #1 — Fan #4	OK, Standby, Degraded, Failed, or Testing. Percentage of full fan speed.	Status of fans 1 through 4.
Fan Spare Number		The spare number for the fans installed in the enclosure.
Temperature	OK, Warm, Caution, or Critical.	Enclosure component temperature sensor.

Table 4-2 Enclosure Information Field Descriptions — Power Area

Field	Possible Values	Description
Power Area		
Power Subsystem Status	Redundant or Non-redundant.	Redundant: both power supplies are functional. Non-redundant: one power supply is not functional.
Total Capacity	Watts.	Total capacity of the power supplies.
Power Supply #1 and #2 Status	OK, Degraded, or Failed.	Status of power supply #1 and power supply #2.
AC Input #1 and #2 Status	OK, Degraded, or Failed.	Status of AC input to power supply #1 and AC input to power supply #2.
Power Supply Spare Number		The spare number for the power supplies installed in the enclosure.

Table 4-3 Enclosure Information Field Descriptions — General Area

Field	Possible Values	Description
General Area		
Enclosure Type		Enclosure product type.
Option Part Number		Part number for the enclosure.
Serial Number		Serial number for the enclosure.
Asset Tag	Maximum 31 characters including all alphanumeric, dash, and underscore characters	Asset tag Only enclosure administrators have write access to this field. For the default asset tag value, see Factory Default Settings on page 128.
Interconnect Tray Type	HP PC Blade Enclosure Interconnect Switch HP PC Blade Enclosure RJ-21 Interconnect Switch HP PC Blade Enclosure RJ-45 Interconnect Switch	Type of interconnect tray.
Interconnect Tray Part Number		Part number for the interconnect tray.

Table 4-3 Enclosure Information Field Descriptions — General Area (continued)

Interconnect Tray Spare Number	Spare number for the interconnect tray.
Interconnect Tray Serial Number	Serial number for the interconnect tray.

Table 4-4 Enclosure Information Field Descriptions — Integrated Administrator Area

Field	Possible Values	Description
Integrated Administrator Area		
Hardware Version		Hardware version of the Integrated Administrator of the enclosure.
Software Version		Software version of the Integrated Administrator of the enclosure.

Table 4-5 Enclosure Information Field Descriptions — Network Area

Field	Possible Values	Description
Network Area		
IP Address	###.###.###.###, where ### ranges from 0 to 255.	The IP address of the Integrated Administrator.
DHCP	Enabled or Disabled.	Shows the status of the Dynamic DNS This field appears only if DHCP is enabled.
MAC Address	##:##:##:##:##:## where ## ranges from 00 to FF.	The MAC address of the Integrated Administrator.

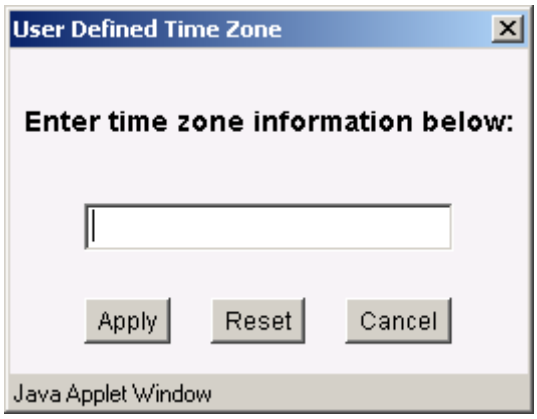
Table 4-6 Enclosure Information Field Descriptions — Date and Time Area

Field	Possible Values	Description
Date and Time Area		
Time Zone	Drop-down box with standard time zones listed	Time zone assigned to the enclosure For the default time zone, see Factory Default Settings on page 128. For a list of all supported time zones, see Time Zone Settings on page 130. For a detailed description of how to set the time zone of the enclosure to a value not listed in the drop down box, select Other.
Date	mm/dd/yy	The date assigned to the enclosure
Time	hh:mm (24-hour format)	The time assigned to the enclosure

* This section of the screen is not available on Linux browsers. If you are using a Linux system, use the command line interface to change the date, time, and time zone.

Only enclosure administrators have access to the Date and Time information. If those fields are not being modified, the Integrated Administrator updates these fields every 20 seconds. If automatic time configuration is enabled, the date and time fields are grayed out and cannot be modified.

If you select Other for time zone, use the following window to set a user-defined time zone:



Three buttons appear on this window:

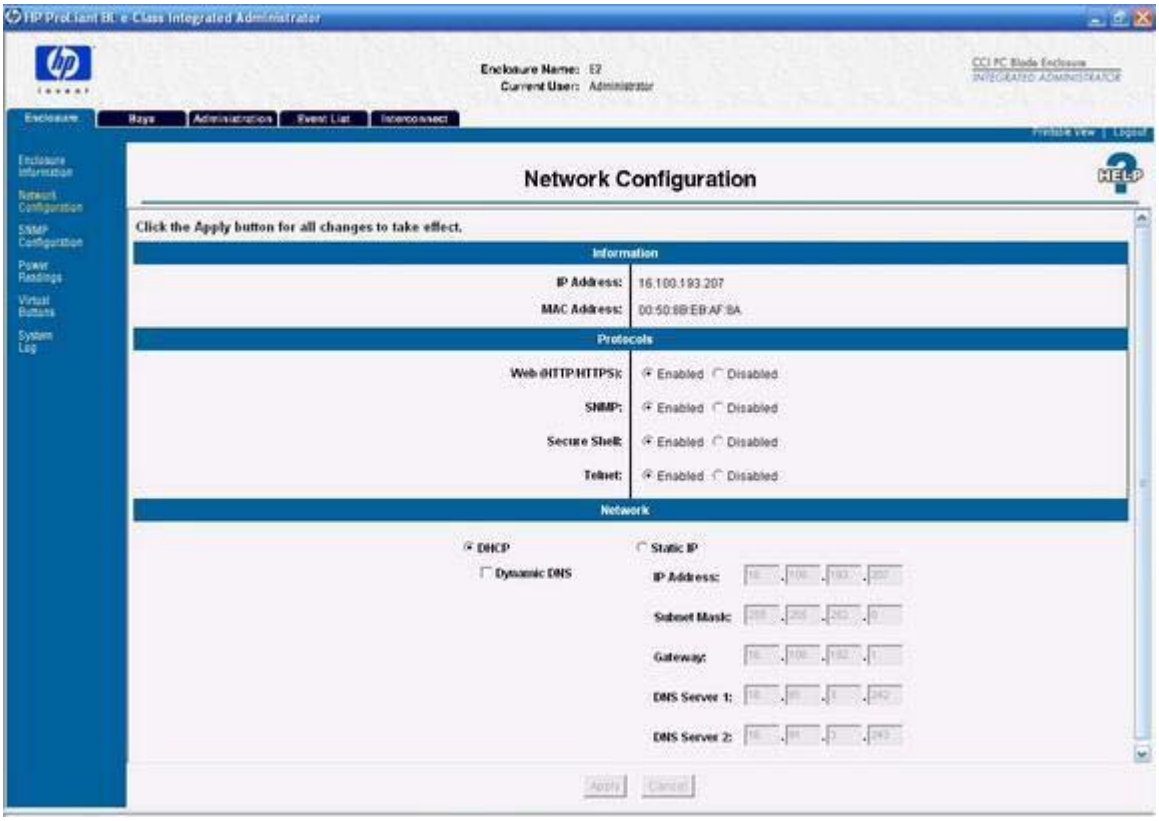
- **Apply** — Applies the new time zone.
- **Reset** — Clears the time zone text box.
- **Cancel** — Cancels all changes and closes the window.

For more information on accepted time zones, refer to Time Zone Settings on page 130.

Network Configuration

NOTE: Only enclosure administrators have access to these settings.

The Network Configuration screen (shown below) enables the enclosure administrator to modify the network settings of an enclosure. These settings are specific to the enclosure and do not affect the network configurations for blade PCs.



Two buttons appear at the bottom of this screen:

- **Apply** — Saves changes made to the screen.
- **Cancel** — Restores all fields on the screen to their original values.

△ **CAUTION:** Both the Web and Secure Shell protocols must be enabled to allow access to the Web-based user interface.

The following table describes the information displayed in the areas that comprise the Network Configuration screen.

Table 4-7 Network Configuration Field Descriptions — Information Area

Field	Possible Values	Description
Information Area		
IP Address		The IP address of the Integrated Administrator.
MAC Address		The MAC address of the Integrated Administrator.

Table 4-8 Network Configuration Field Descriptions — Protocols Area

Field	Possible Values	Description
Protocols Area		
Web (HTTP/HTTPS)	Enabled or Disabled.	The default setting is Enabled.

Table 4-8 Network Configuration Field Descriptions — Protocols Area (continued)

SNMP	Enabled or Disabled.	The default setting is Enabled.
Secure Shell	Enabled or Disabled.	The default setting is Enabled.
Telnet	Enabled or Disabled.	The default setting is Enabled.

Table 4-9 Network Configuration Field Descriptions — Network Area

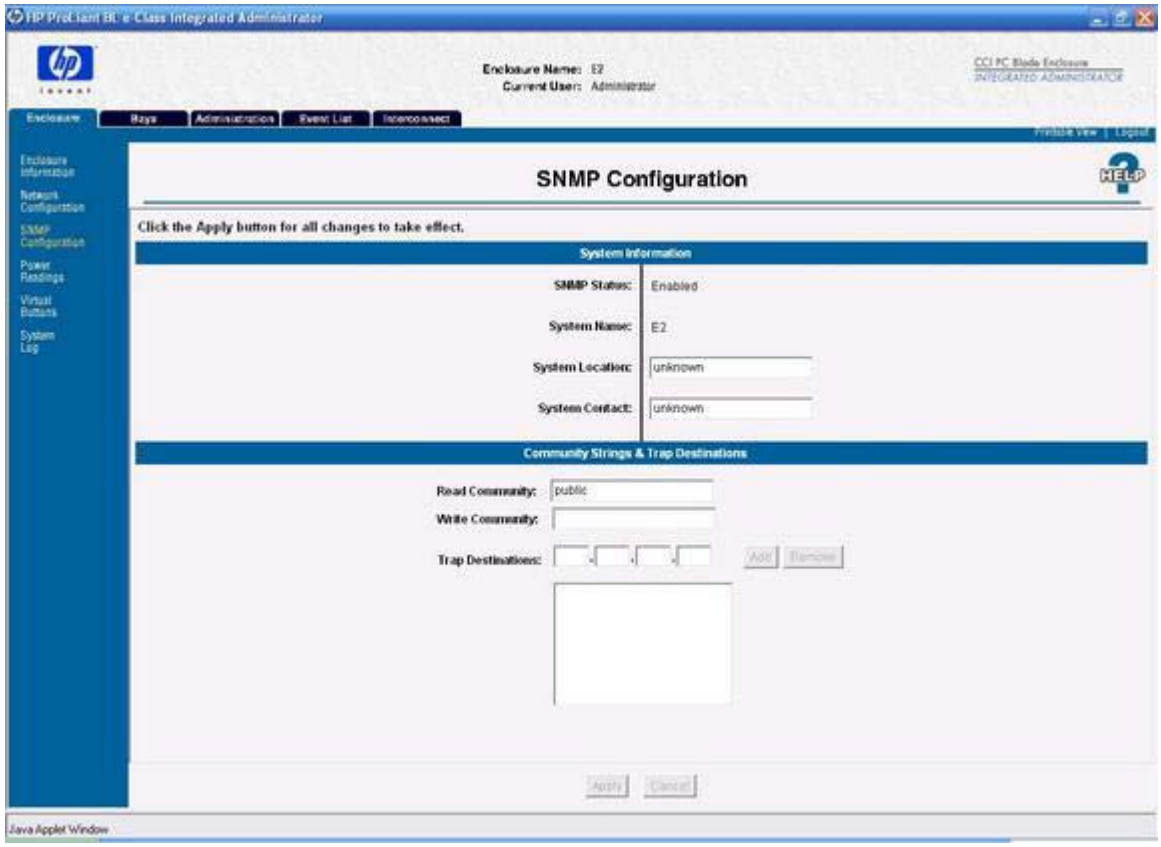
Field	Possible Values	Description
Network Area		
DHCP		Gets the IP address of the Integrated Administrator from the DHCP.
Static IP		Sets a static IP address of the Integrated Administrator.
Dynamic DNS		Determines whether the Integrated Administrator uses Dynamic DNS.
IP Address	###.###.###.###, where ### ranges from 0 to 255.	Static IP address for the Integrated Administrator (mandatory if Static IP is selected).
Subnet Mask	###.###.###.###, where ### ranges from 0 to 255.	Subnet mask for the Integrated Administrator (mandatory if Static IP is selected).
Gateway Address	###.###.###.###, where ### ranges from 0 to 255.	Gateway address for the Integrated Administrator (optional field if Static IP is selected).
DNS Server 1	###.###.###.###, where ### ranges from 0 to 255.	The IP address for the primary DNS server (optional field if Static IP is selected).
DNS Server 2	###.###.###.###, where ### ranges from 0 to 255.	The IP address for the secondary DNS server (optional field if Static IP is selected).

SNMP Configuration

The SNMP Configuration screen (shown below) enables an enclosure administrator to modify the SNMP settings of an enclosure. These settings are specific to the enclosure and do not affect the network configurations for blade PCs.

Two buttons appear at the bottom of this screen:

- **Apply** — Saves changes made to the screen.
- **Cancel** — Restores all fields on the screen to their original values.



The following table describes the information presented on the SNMP Configuration screen:

Table 4-10 SNMP Configuration Field Descriptions — System Information Area

Field	Possible Values	Description
System Information Area		
SNMP Status	Enabled or Disabled	Displays if SNMP is enabled or disabled.
System Name		The name of the enclosure.
System Location	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	The SNMP location of the enclosure For the default SNMP contact, see Factory Default Settings on page 128.
System Contact	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	The SNMP contact of the enclosure For the default SNMP contact, see Factory Default Settings on page 128.

Table 4-11 SNMP Configuration Field Descriptions — Community Strings and Trap Destinations Area

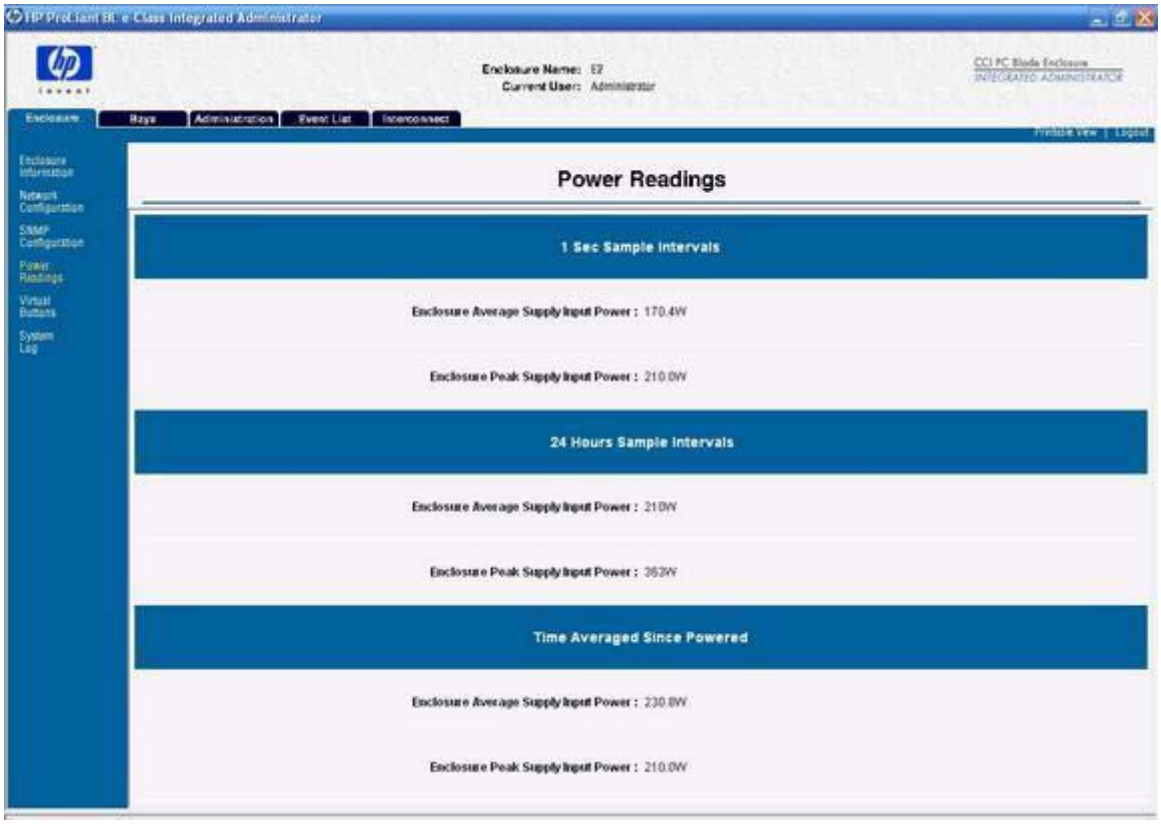
Field	Possible Values	Description
Community Strings and Trap Destinations Area		
Read Community	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	Displays the SNMP read community string If this is left blank, “public” is assigned.

Table 4-11 SNMP Configuration Field Descriptions — Community Strings and Trap Destinations Area (continued)

		For the default read Community string, see Factory Default Settings on page 128.
Write Community	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	Sets the SNMP write community string If this is left blank, SNMP SET commands are disabled. For the default write Community string, see Factory Default Settings on page 128.
Add		Adds an IP address to the list of trap destinations.
Remove		Removes the selected IP addresses from the list of trap destinations.

Power Readings

The Power Readings screen provides power consumption estimates for the enclosure.

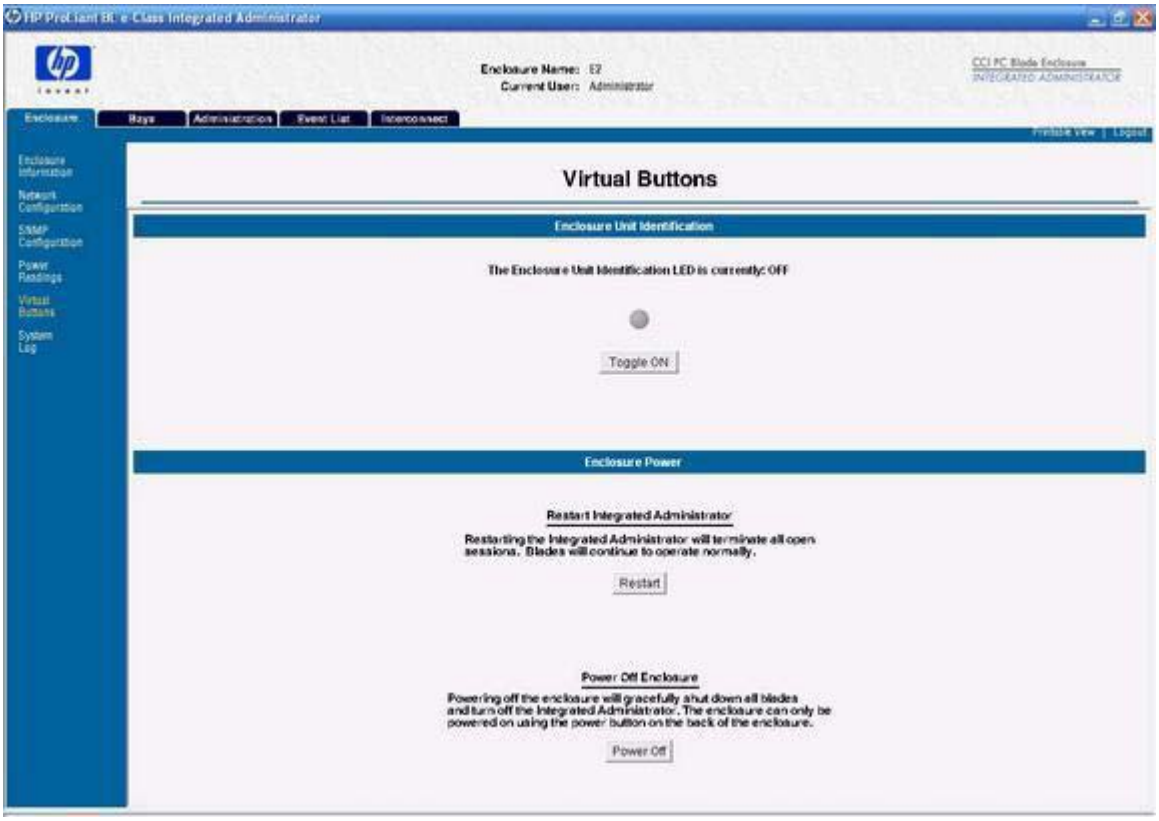


NOTE: The screen may differ from the image shown here.

Virtual Buttons

NOTE: Only enclosure administrators can execute these commands.

The Virtual Buttons screen (shown below) enables an enclosure administrator to modify the power state of the enclosure and Unit Identification LED from a remote location to facilitate troubleshooting by technicians in the data center.



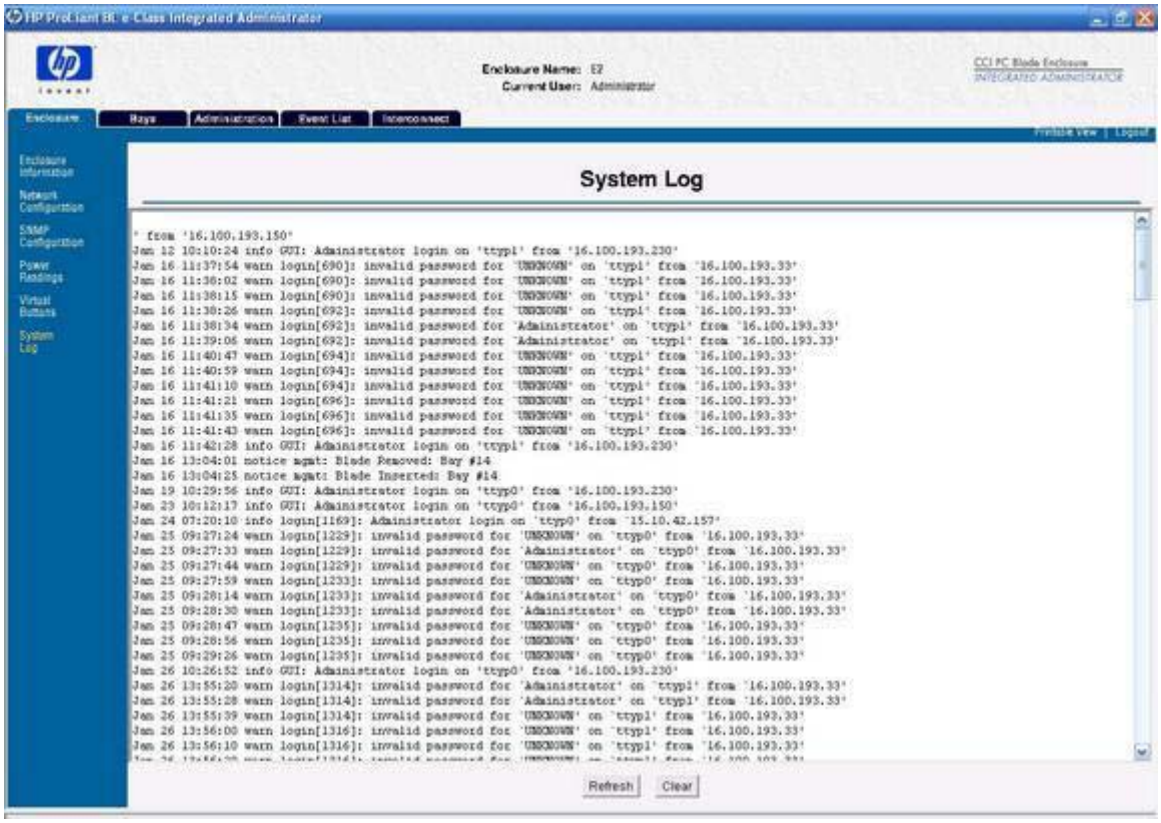
The **Toggle On/Toggle Off** button remotely changes the state of the enclosure Unit Identification LED. The illustration below shows the information presented in the Enclosure Power area of the Virtual Buttons screen:

You can select the appropriate function with the following buttons:

- **Restart Integrated Administrator** — Restarts the Integrated Administrator and does not affect the blade PCs. Click Restart Integrated Administrator only at the direction of HP support personnel. Click Apply for these settings to take effect.
- **Power Off Enclosure** — Attempts a graceful shutdown of the system for 5 minutes, after which time this command powers down all components of the enclosure immediately. Whenever possible, HP recommends that you use the operating system shutdown procedures before powering down a blade PC or enclosure. After the enclosure is powered off, powering on can only occur by local access to the system.

System Log

The System Log screen (shown below) provides an enclosure administrator with a chronological list of events and fixes associated with the enclosure.



Two buttons appear at the bottom of this screen:

- **Refresh** — Refreshes the screen.
- **Clear** — Clears the system log.

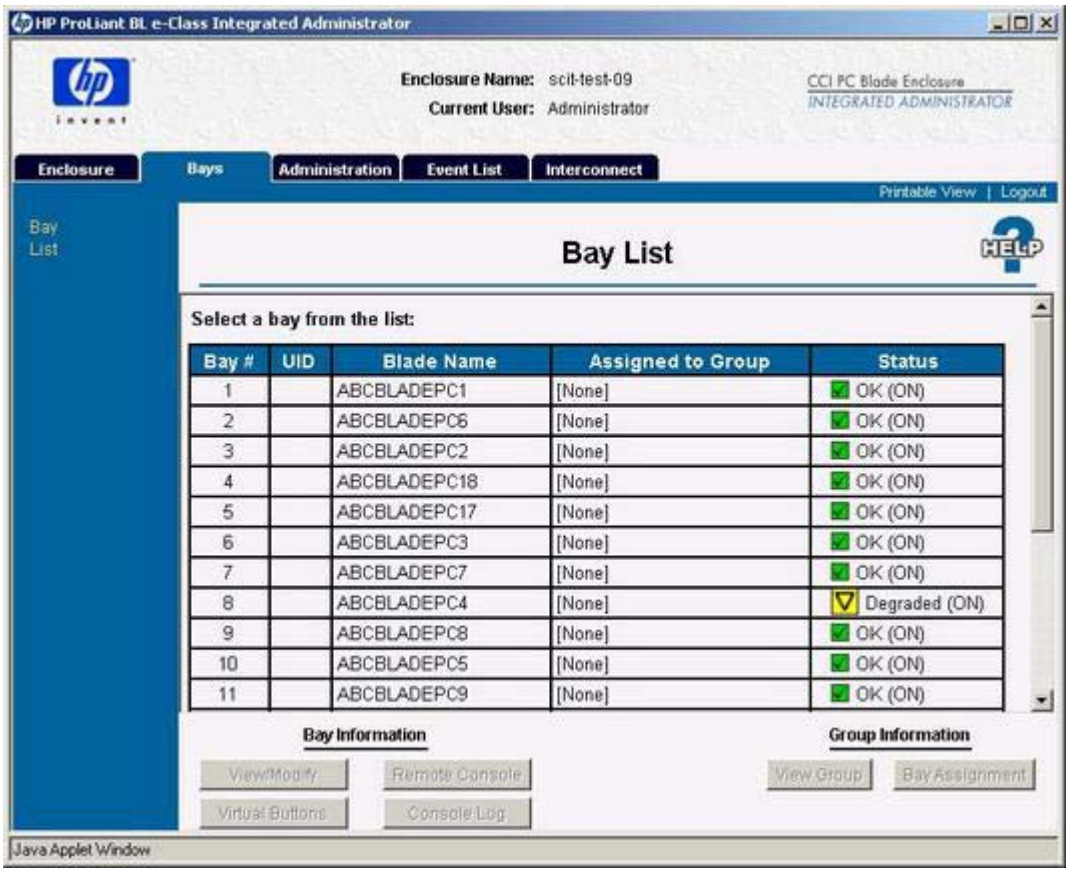
Bays Tab

The Bays tab provides access to the following screens:

- Bay List
- Bay Information
- Remote Console
- Virtual Buttons
- Console Log

Bay List

The Bay List screen (shown below) enables an enclosure administrator to observe and update the assignment of groups to blade PC bays, as well as monitor the status of each blade PC installed in the enclosure.



Group administrators and group members with permissions can view the blade PC bays assigned to their groups.

The following table describes the information presented in the Bay List screen:

Table 4-12 Bay List Field Descriptions

Field	Possible Values	Description

Table 4-12 Bay List Field Descriptions (continued)

Bay #	1-20	Blade PC number.
UID		Displays a blue circle if the unit identification (UID) LED of the blade is lit.
Blade PC Name		Name of the blade PC in that blade PC bay as defined by the operating system of the blade PC. **NOTE:** Without the blade PC health driver properly installed, the Integrated Administrator cannot obtain the blade PC name.
Assigned to Group		Name of the group that owns that bay.
Status	OK, Degraded, or Failed	The status and power state of the blade PC.

The following table lists permissions that are related to the action buttons of the Bay List screen

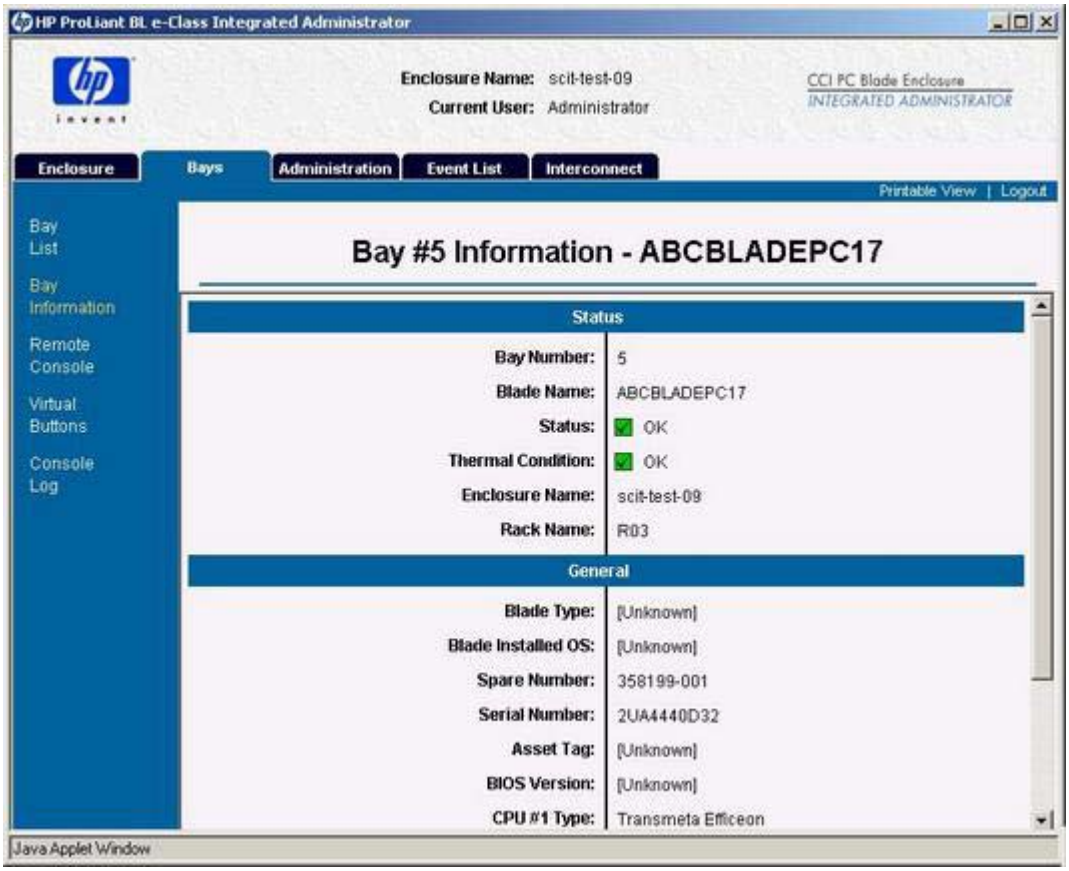
Table 4-13 Bay List Action Buttons and Permissions

Field	Possible Values	Description
View/Modify	Opens the Blade Information screen.	Enclosure administrators, group administrators, and group members with permissions.
Remote Console	Opens the Remote Console screen.	Enclosure administrators, and group administrators with permissions.
Console Log	Opens the Console Log screen.	Enclosure administrators, group administrators, and group members with permissions.
View Group	Opens the View/Modify Group screen.	Enclosure administrators only.
Bay Assignment	Opens the Bay Assignment dialog box. **NOTE:** If a blade PC is to be re-assigned, it must be unassigned first.	Enclosure administrators only.

Bay Information

△ **CAUTION:** Be sure the Integrated Administrator displays up-to-date blade PC information by rebooting the blade PC after installing the blade PC health driver.

The Bay Information screen (shown below) enables an enclosure administrator to observe the status and general information for a blade PC in a given blade PC bay. Group administrators and group members with View rights to the blade PC bay can also observe this information.



To be sure that the Bay Information screen displays the optimal number of possible values, you must have the blade PC health driver installed.

The following table describes the information presented on the Bay Information screen for all enclosure administrators and for group members and groups with rights to the blade PC bay.

Table 4-14 Bay Information Field Descriptions — Status Area

Field	Possible Values	Description
Status Area		
Bay Number		Bay number.
Blade PC Name		Name of blade PC as specified with the blade PC operating system.
Status	OK, Degraded, or Failed	Status of the blade PC.
Thermal Condition	OK, Warm, Caution, or Critical	Thermal condition of the blade.
Enclosure Name		Name of enclosure. For the default enclosure name, see Factory Default Settings on page 128.

Table 4-15 Bay Information Field Descriptions — General Area

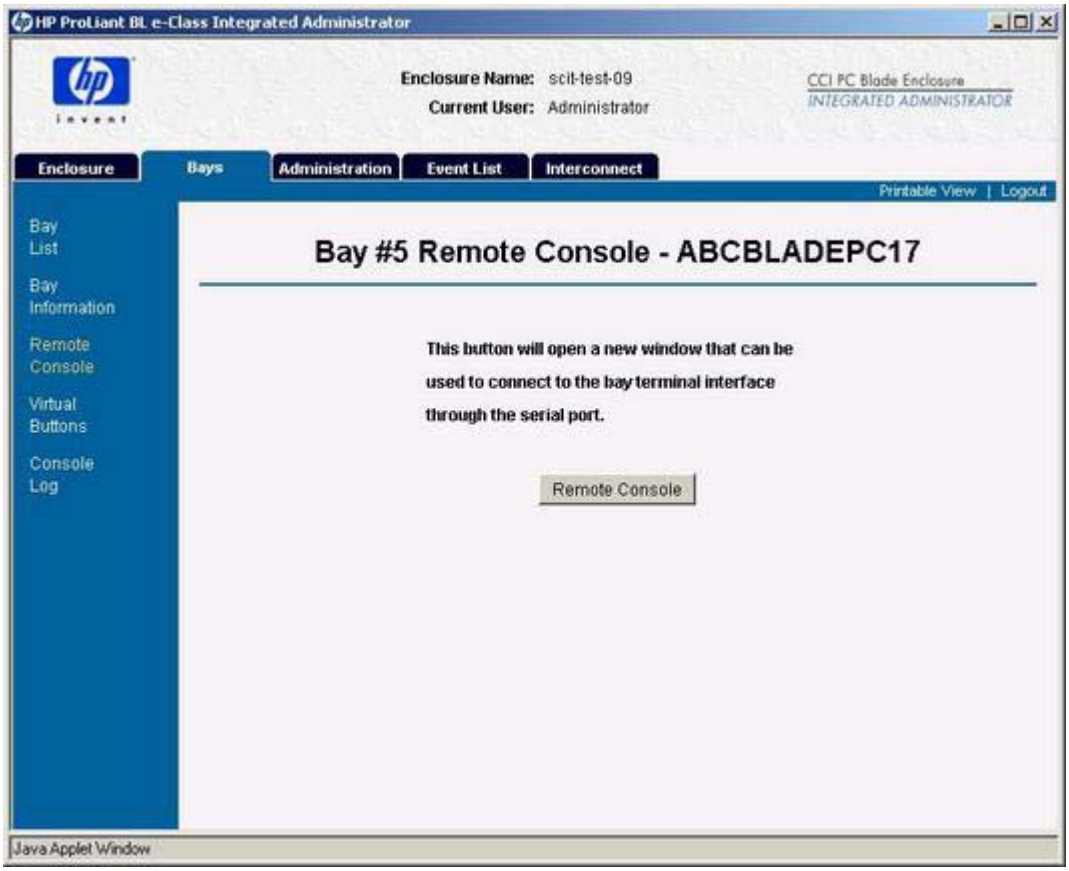
Field	Possible Values	Description

Table 4-15 Bay Information Field Descriptions — General Area (continued)

General Area		
Blade PC Type		Product name of the blade PC.
Blade PC Installed OS		Operating system installed on the blade PC.
Spare Number		Spare number of the blade PC.
Serial Number		Serial number of the blade PC.
Asset Tag		Asset tag number of the blade PC.
BIOS Version	mm/dd/yy	ROM version on the blade PC.
CPU # Type		Type of processor on the blade PC.
CPU # Max Speed		Speed associated with the blade PC processor.
Installed RAM		Amount of memory installed on the blade PC.
NIC #1 and #2 MAC Addresses	##:##:##:##:##:##, where ## ranges from 00 to FF.	MAC address of the NIC 1 interface and the NIC 2 interface.

Remote Console

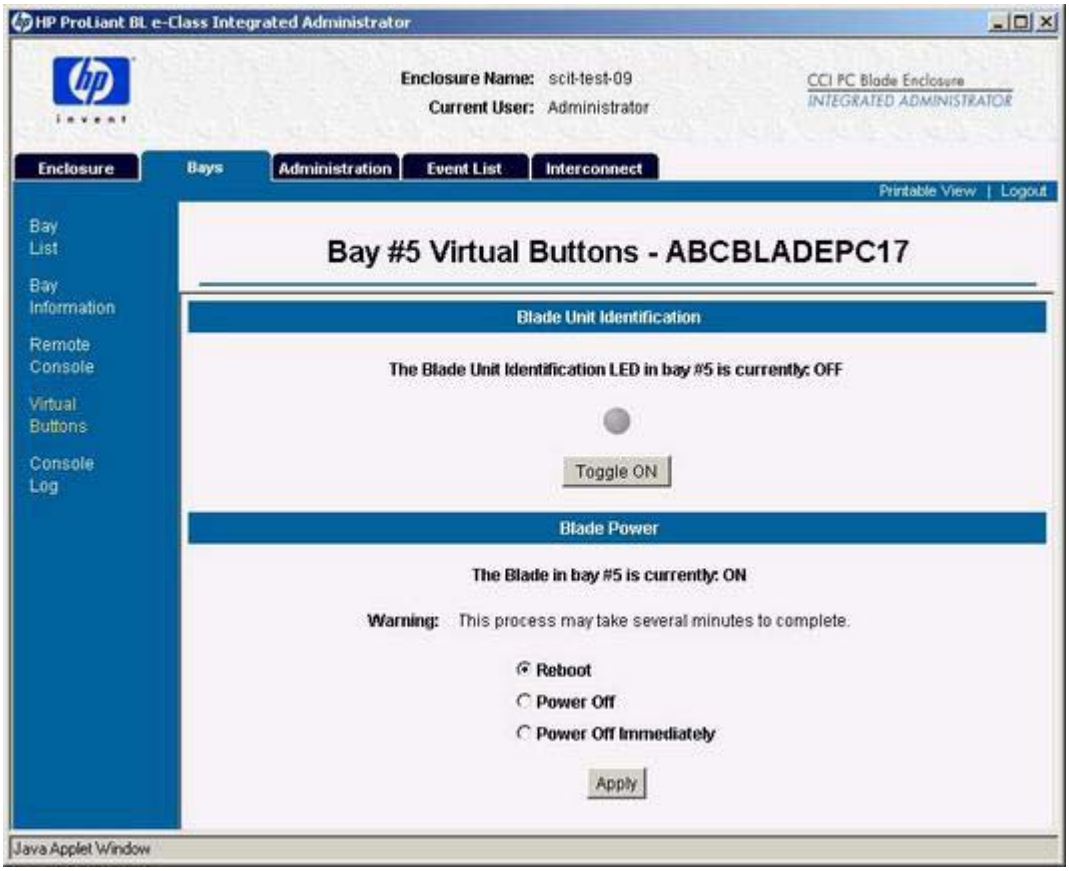
Enclosure administrators and group administrators with access to the bay can click Remote Console to open a remote text-based console (shown below) to the blade PC in the bay.



For information on establishing remote console connectivity, see Enabling Remote Console Sessions to Blade PCs on page 79.

Virtual Buttons

Enclosure administrators and group administrators with permissions can use the Virtual Buttons screen (shown below) to modify the state of the power state and Unit Identification LED of a blade PC in order to facilitate troubleshooting from a remote location.



The Virtual Buttons screen enables group administrators and enclosure administrators to reboot, power off, or identify the blade PC with the following items:

- The **Toggle On/Off** button remotely changes the state of the blade PC Unit Identification LED.
- You can select the appropriate function in the Blade PC Power area using the following radio buttons:
  - **Reboot** reboots the blade PC.
  - **Power Off** attempts a graceful shutdown of the blade PC for 5 minutes, after which time this command powers down the blade PC immediately.
  - **Power Off Immediately** powers off the blade PC forcefully.

△ **CAUTION:** Without the blade PC health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shut down a blade PC. This condition can result in the permanent loss of critical data.

NOTE: Click **Apply** for these settings to take effect.

NOTE: Whenever possible, HP recommends that you use the operating system shutdown procedures before powering down a blade PC or enclosure. Once the enclosure is powered off, powering on can only occur with local access to the system.

Console Log

NOTE: Only group members, group administrators, and enclosure administrators can view a console log of a blade PC.

The Console Log screen displays the console log for the specified bay. The console log of the bay is not stored between reboots of the Integrated Administrator, so the information will only include what has taken place since the last power on of the Integrated Administrator.

The data captured in the console log is all output from the serial console of the blade PC that occurred while no one was connected to the console. For security reasons, console output during a user connection session is not logged.

The Refresh button refreshes the console log for the current blade PC.

Administration Tab

For an explanation of user rights associated with the Integrated Administrator, see Enabling Remote Console Sessions to Blade PCs on page 79.

Under the Administration tab, you can access the following screens:

- User List
- Group List
- Add User
- Add Group
- View/Modify User
- View/Modify Group

User List

The User List screen (shown below) enables an appropriate group administrator or enclosure administrator to observe and update user access to groups and blade PC bays.

The following table lists the permissions related to the action buttons of the User List screen.

Table 4-16 User List Action Buttons and Permissions

Button	Function	Permissions
View/Modify User	Opens the View/Modify User screen.	Enclosure administrators can access and modify the information for any user. Users can access and modify the information for own account.
Remove User	Removes the selected user (unless the account is your own).	Only enclosure administrators can execute this command.

The following table describes the information presented in the User List screen.

Table 4-17 User List Field Descriptions

Button	Function	Permissions

Table 4-17 User List Field Descriptions (continued)

User Name		User login name.
Full Name		User full name.
Account Type	Administrator or User	Shows if the user is an enclosure administrator.
Account Status	Enabled or Disabled	Shows if the user's account is enabled.
Group Membership		Shows the groups in which the user has membership.

Group List

The Group List screen (shown below) enables an enclosure administrator to observe and update the assignment of groups and users to blade PC bays.

Two buttons appear on this screen:

- **View/Modify Group**—Opens the View/Modify Group screen.
- **Remove Group**—Removes the selected group.

NOTE: Enclosure administrators can view and modify the information for all groups. Group administrators and group members can view the information for the groups in which they are members.

Table 4-18 Group List Field Descriptions

Field	Description
Group Name	Group name

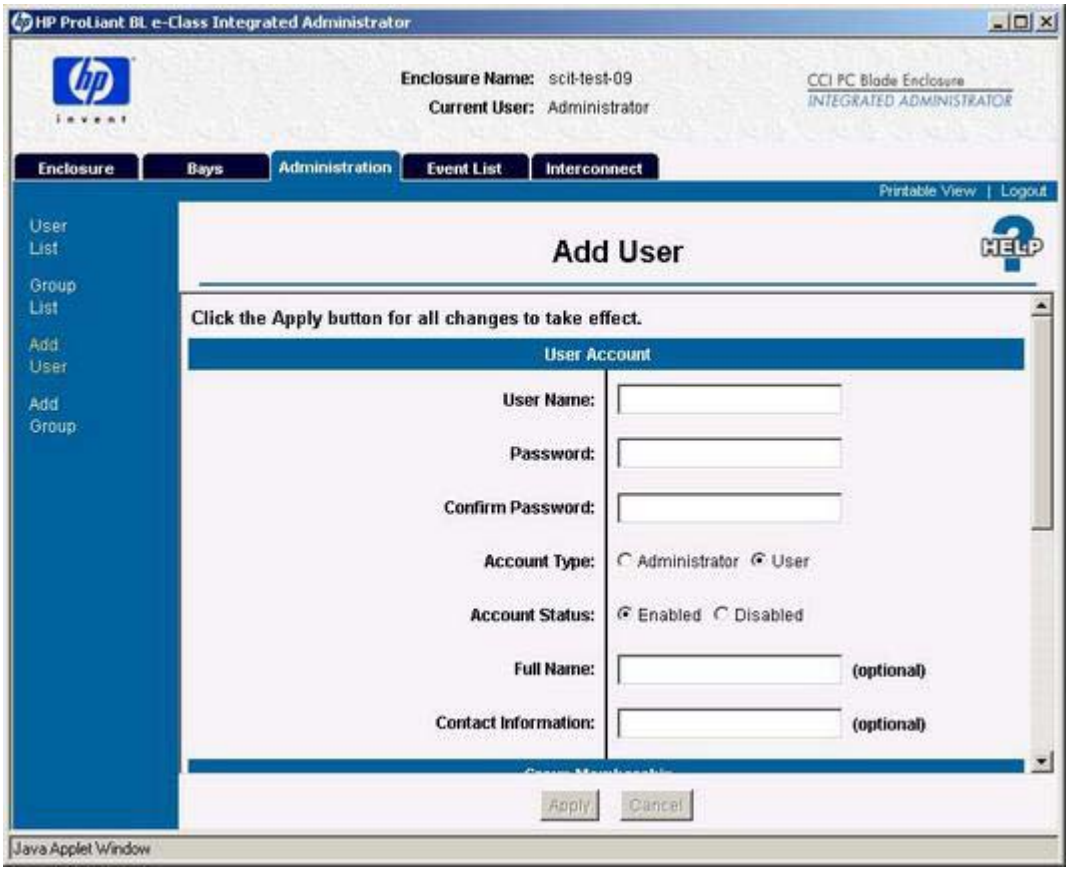
Table 4-18 Group List Field Descriptions (continued)

Assigned Bays	Blade PC bays that the group owns
Group Members	Users with membership in the group

Add User

NOTE: Only enclosure administrators have access to this area of the Integrated Administrator.

The Add User screen (shown below) enables an enclosure administrator to create a user profile, including group and blade PC bays assignments.



Two buttons appear on this screen:

- **Apply**—Saves changes made to this screen.
- **Cancel**—Restores all fields on this screen to their original values.

The following table describes the fields /of the Add User screen.

Table 4-19 Add User Field Descriptions

Field	Possible Values	Description
User Name	1-13 characters including alphanumeric, dash, and underscore characters.	Login name of the user.

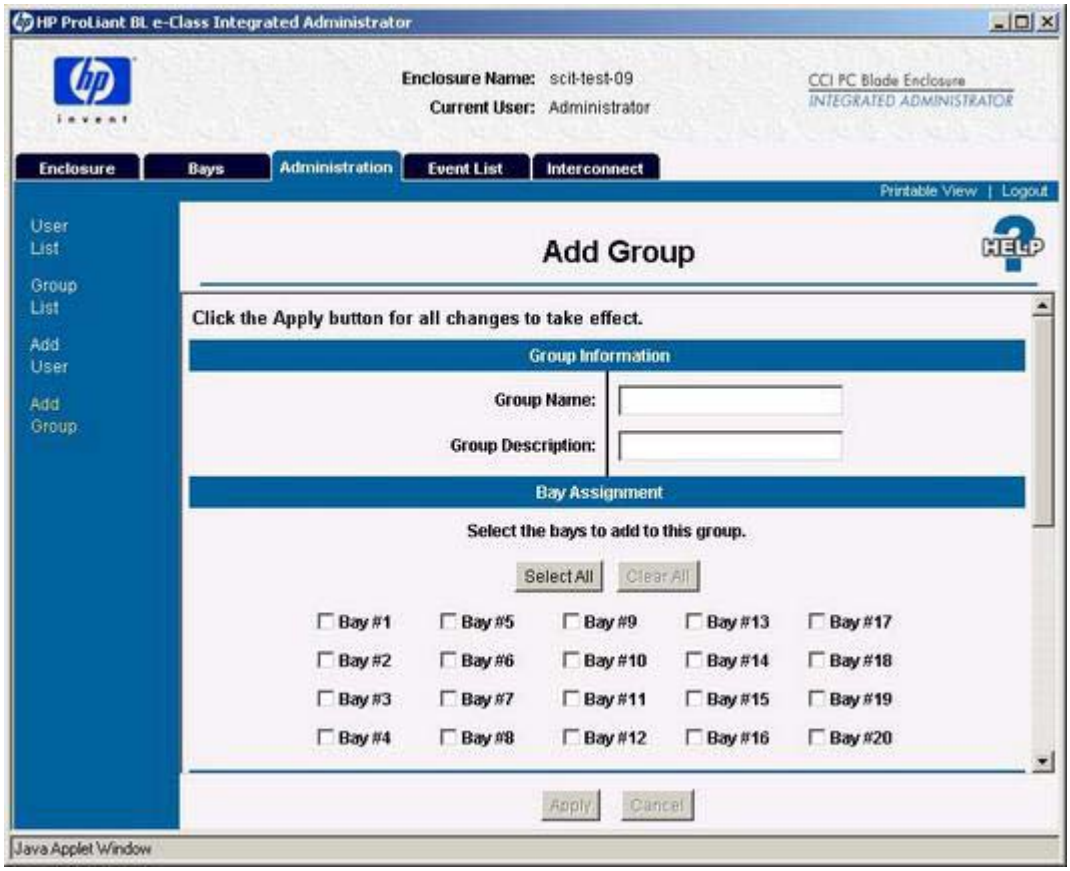
Table 4-19 Add User Field Descriptions (continued)

	The user name must begin with a letter. A maximum of 25 users can be created in addition to the reserve accounts.	**NOTE:** "Administrator," "switcha,"switchb," and "all" are reserved names and cannot be used. This restriction is not case-sensitive.
Password	3-8 characters including all printable characters	User's password.
Confirm Password	3-8 characters including all printable characters	User's password.
Account Type	Radio buttons (Administrator and User)	Determines if the user has enclosure administrator rights.
Account Status	Radio buttons (Enabled and Disabled)	Determines if the user's account is enabled.
Full Name (optional)	1-20 characters Accepts only alphanumeric, dash, underscore, and space characters	Full name of user.
Contact Information (optional)	1-20 characters Accepts only alphanumeric, dash, underscore, and space characters	Optional user contact information.
Group Names	All groups are listed	A list of all possible groups.
Group Membership	x number of groups (all groups in which the user has membership)	A list of all groups of which the user is a member.
Add User [View]>>>		Adds the user to the selected groups in the **Group Names** text box with View rights for group members These groups appear in the **Group Membership** text box. The user loses View/Modify rights if they previously had them.
Add User [View/Modify]>>>		Adds the user to the selected groups in the **Group Names** text box with View/ Modify rights for group administrators or view rights for group members.
<<<		Removes the user from the selected groups in the **Group Membership** text box.

Add Group

NOTE: Only enclosure administrators have access to this area of the Integrated Administrator.

The Add Group screen (shown below) enables an enclosure administrator to create a group profile, including user and blade PC bays assignments.



NOTE: Grayed-out check boxes are unavailable because they are already assigned to another group.

Two buttons appear on this screen:

- **Apply**—Saves changes made to this screen.
- **Cancel**—Restores all fields on this screen to their original values.

Table 4-20 Add Group Field Descriptions — Group Information Area

Field	Possible Values	Description
Group Information Area		
Group Name	1-13 characters including alphanumeric, dash, and underscore characters. The group name must begin with a letter. A maximum of 20 users can be created.	Name of group.
Group Description (optional)	1-20 characters Accepts only alphanumeric, dash, and underscore characters.	Description of group.

Table 4-21 Add Group Field Descriptions — Bay Assignment Area

Field	Possible Values	Description
Bay Assignment Area		

Table 4-21 Add Group Field Descriptions — Bay Assignment Area (continued)

Bay 1 - Bay 20	Determines which bays the group owns. Only one group can own a particular bay. If a check box is disabled, another group already owns the bay.
Select All	Selects all check boxes of the bays.
Clear All	Clears all check boxes of the bays.

Table 4-22 Add Group Field Descriptions — Group Membership Area

Field	Possible Values	Description
Group Membership Area		
User Names	All users and enclosure administrators are listed.	A list of all possible users.
Group Members	x number of users (all users that are members of the group).	A list of all users that are members of the group.
Add User [View]>>>		Adds selected users in the User Names text box to the group with View rights for group members. Users lose View/Modify rights for group administrators if they previously had them.
Add User [View/Modify]>>>		Adds selected users in the User Names text box to the group with View/Modify rights for group administrators.
<<<Remove User		Removes selected users in the Group Members text box from the group.

View/Modify User

You can access the View/Modify User screen by clicking any row in the User List and then clicking View/Modify User. The View/Modify User screen provides the same functions and has the same access as the Add User screen. See the “Add User” section in this chapter.

View/Modify Group

You can access the View/Modify Group screen by clicking any row in the Group List and then clicking View/Modify Group. The View/Modify Group screen the provides same functions and has the same access as the Add Group screen. See the Add Group on page 41 section in this chapter.

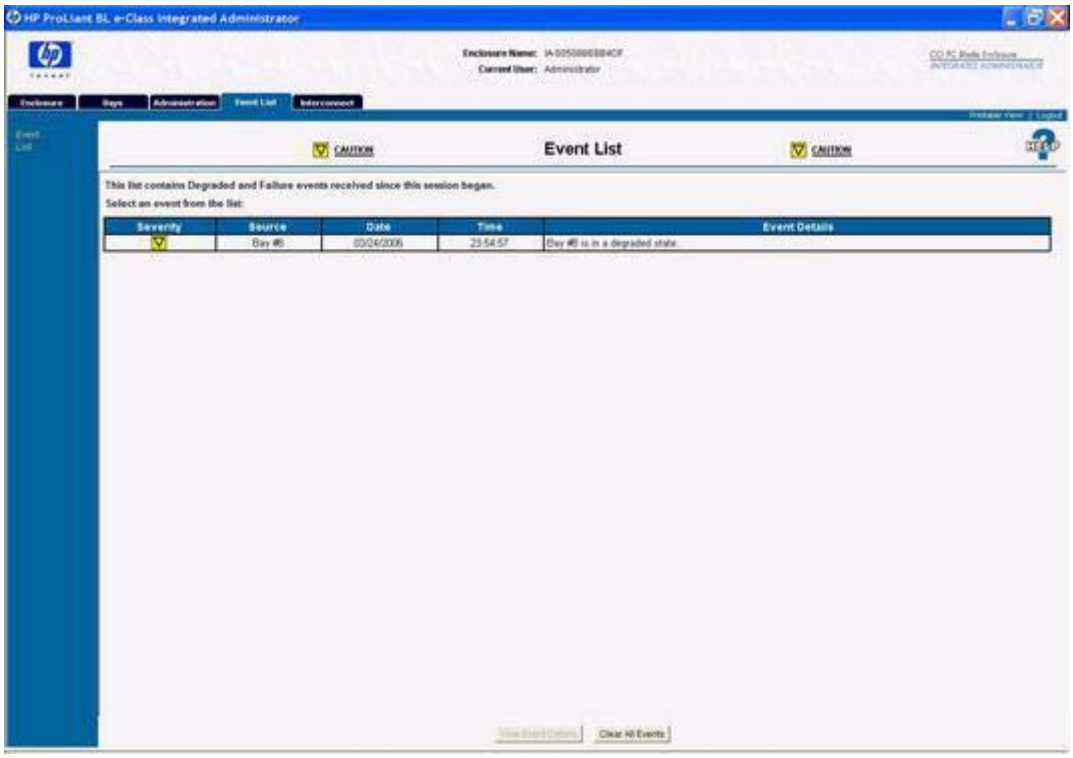
Event List Tab

The Event List differs from the System Log in the following ways:

- Any user can view the Event List. Only enclosure administrators can access the System Log.
- The messages in the Event List are limited to cautions and critical failures. Refer to the enclosure System Log for information on both failures and fixes.
- The Event List only displays messages received since the user logged into the Integrated Administrator. The System Log displays every message generated by the enclosure diagnostics.

The Event List screen (shown below) provides the following information for each event:

- Severity
- Source
- Date
- Time
- Event Details (the example below indicates a fan failure)



The Integrated Administrator provides real-time event notifications for an enclosure according to two categories of severity (caution and critical) described in the following table. For detailed information regarding the Event List, including a comprehensive list of event messages, see Event Icons and Details on page 126.

Table 4-23 Event Notification Icons

Icon	Description

Table 4-23 Event Notification Icons (continued)

	Caution — An event that does not prevent the enclosure from operating, maintaining power, or serving its user community When a caution event occurs, a reasonable guarantee that operability can persist no longer exists.
	Critical — An event that prevents the continued operation of the enclosure. When a critical event occurs, the inoperability of the enclosure is imminent.

Interconnect Tab

The Interconnect Tray screen (shown below) allows anyone to view information about the interconnect tray. It allows enclosure administrators to connect to the remote console of one of the interconnect switches if installed.

The following table describes the information displayed in the areas that comprise the Interconnect Tray screen.

Table 4-24 Interconnect Tray Screen Field Descriptions — Interconnect Tray Information Area

Field	Possible Values	Description
Interconnect Tray Information Area		
Status	OK, Degraded, or Failed	Status of the interconnect tray.
Temperature	OK, Warm, Caution, or Critical	Thermal status of the interconnect tray.
Switch A Status	OK, Degraded, or Failed	Status of Switch A. This will only be displayed if an interconnect switch is installed.
Switch B Status*	OK, Degraded, or Failed	Status of Switch B. This will only be displayed if an interconnect switch is installed.
Manufacturer		Manufacturer of the interconnect tray.
Product Name		Product name of the interconnect tray.

Table 4-24 Interconnect Tray Screen Field Descriptions — Interconnect Tray Information Area (continued)

Interconnect Tray Part Number	Spare part number of the interconnect tray.
Interconnect Tray Serial Number	Serial number of the interconnect tray.

Table 4-25 Interconnect Tray Screen Field — Switch Terminal Console Area (only present if an interconnect switch is installed)

Field	Possible Values	Description
Switch Terminal Console Area (only present if an interconnect switch is installed)		
Switch A button		Opens a new window to the remote console of switch A.
Switch B button*		Opens a new window to the remote console of switch B.
* e-Class switches only.		

5 Command Line Interface

This chapter provides reference material for operating the Integrated Administrator Command Line Interface (CLI). This chapter provides command line related information with the following sections:

- Accessing the Command Line Interface
- Operating the Command Line Interface
  - General commands
  - General management commands
  - User account commands
  - Enclosure network configuration commands
  - Enclosure management commands
  - Blade PC management commands
- Functionality exclusive to the command line interface

  For a detailed explanation of the command line conventions used in this document, see Command Line Conventions on page 118.

  For easy reference, the index of this book also provides a comprehensive listing of the commands supported by the Integrated Administrator.

Accessing the Command Line Interface

You can access the CLI remotely through the management (10/100 Ethernet) connector, locally through the console (serial) connector on the rear panel of the enclosure, or through any uplink depending on VLAN configuration.

Accessing Remotely through the Management Connector

To access the Integrated Administrator command line interface remotely through the management (10/100 Ethernet) connector:

1. Get the default host name from the settings tag attached to the interconnect tray.
2. Open a Telnet or Secure Shell application and type the IP address or DNS name for the enclosure you wish to access.

△ **CAUTION:** Using Telnet instead of Secure Shell means your remote session, including password, appears in clear text on that network.

3. Type the user name and password into the **Login** prompt.

Accessing Locally through the Console Connector

To access the Integrated Administrator locally through the serial connector:

1. Connect a local client device, such as a laptop computer, to the serial connector using the null-modem cable that ships with the enclosure.

NOTE: Client devices must satisfy the requirements provided in Requirements for Local Client Devices on page 11.

2. Open the terminal emulator and press Enter to get the login prompt.
3. Type the user name and password.

Operating the Command Line Interface

General Commands

The following table describes the information displayed in the areas that comprise the Enclosure Information screen.

Table 5-1 General Commands

Command	Description	Restrictions
CLEAR SCREEN	Clears the terminal screen	None
EXIT	Exits the command line interpreter	None
HELP {<ommand>} |Tree	If a command is given, the usage and help text for the command are shown in a tree format. If no argument is given, all base commands are displayed.	None
LOGOUT	Exits the command line interpreter	None
QUIT	Exits the command line interpreter	
SLEEP	Pauses the sessions for a fixed period of time. Useful for adding delays to scripts. The <seconds> field can be any whole umber from 1 - to 86400. Once the pause has started, no way exists to continue the session before time runs out, but you can terminate the session and start another one.	None

General Management Commands

The following table describes the information displayed in the areas that comprise the Enclosure Information screen.

Table 5-2 General Management Commands

Command	Description	Restrictions
CLEAR SSESSION SWITCH [A | B]	Terminate a Terminal session from the enclosure. This is not a graceful termination. The connected user loses any unsaved work.	Group administrators may only execute thus command for the blade PC bays to which they have access.
CLEAR SSHKEY	Remove the contents of the Secure Shell authorized keys file. After performing this command, you will not be able to login using the public key-based authentication.	Only enclosure administrators may execute this command.
CONNECT SWITCH [A | B]	Opens a remote console connection to switch A or B. A single switch cannot support multiple, simultaneous remote console sessions.	Only enclosure administrators may execute this command.
DOWNLOAD CERTIFICATE <url>	Download a CA supplied PKCS#7 file to replace the current security certificate on the system. Supported protocols are http, ftp, and tftp. Format the URL as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by augmenting the host part in the above format with username:password@host.	Only enclosure administrators may execute this command.

Table 5-2 General Management Commands (continued)

DOWNLOAD SSHKEY	Downloads an authorized key file to use with Secure Shell v2, which can contain the public keys for any enclosure administrator. Supported protocols are http, ftp, and tftp. Format the URL as protocol//host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	Only enclosure administrators may execute this command.
GENERATE CERTIFICATE REQUEST	Generates a PKCS#10 certificate request.	Only enclosure administrators may execute this command.
GENERATE CERTIFICATE SELFSIGNED	Generates a self-signed certificate.	Only enclosure administrators may execute this command.
PING {<number>} {<IP address>} | <server name>}	Sends ICMP echo messages to a remote IP device. If <number> is omitted, only 5 packets are sent. Packets are sent out at 1-second intervals.	The <IP address> must be in the form "###.###.###.###" where ### ranges from 0 to 255.
SET DISPLAY EVENTS [ON | OFF]	Turns event notification on or off. The Integrated Administrator preservers this setting across all logins.	None
SET EXPERT {MODE} [ON | OFF]	Turns EXPERT MODE on or off. When EXPERT MODE is on, the system will not prompt the user to confirm actions. Users should exercise caution when working in EXPERT MODE as many actions are not reversible.	None
SET FACTORY	Sets the Integrated Administrator back to its factory defaults. The Administrator account password does not change. The Integrated Administrator is restarted after all the changes are made. Note: This command removes all groups, users, and other customization from the memory of the enclosure, and the information is unrecoverable.	Only the "Administrator" account may execute this account.
SET SCRIPT MODE [ON | OFF]	When SCRIPT MODE is on, the following commands require a password argument: ADD USER, SET USER PASSWORD, or SET PASSWORD. Default values require user interaction.	None
SHOW SESSIONS	Displays the connection to each bay and switch if one exists. Only one user may connect to each bay and switch at a time. It also shows each user that is currently logged in, the user's port number, connect time, and remote system name.	Users may not run this command. Group members and group administrators may only see the sessions for bays assigned to groups to which they belong. Enclosure administrators see all sessions
SHOW SSHFINGER PRINT	Displays the key fingerprint of the host SSH pubic key of the Integrated Administrator. This can be used from the serial console to validate the identity of the Integrated Administrator before initializing an SSH connection across a network.	None
SHOW SSHKEY	Displays the contents of the existing Secure Shell authorized keys file that is being used for enclosure administrator key-based authentication.	Only enclosure administrators may execute this command.
SHOW ENCLOSURE POWER	Display power consumption estimates for the enclosure, including all sub-components. This information includes overall power consumption of the enclosure, as well as peak and average supply input and output power.	This command provides only estimated power usage. Use it only as reference information.

User Account Commands

Table 5-3 User Account Commands

Command	Description	Restrictions
ADD GROUP <group name>	Adds a group to the system The default group description is blank.	Only enclosure administrators may execute this command. A maximum of 20 groups may be added to the system. The <group name> must be unique to all other group names and user names and is case-sensitive. It must be 1-13 characters long and can include alphanumeric, dash, and underscore characters. It must begin with a letter. **NOTE:** Administrator, “switcha,” “switchb,” and “all” are reserved names and cannot be used. This restriction is not case-sensitive. See Factory Default Settings on page 128 for factory default groups accounts.
ADD USER <user name> {<password>}	Adds a user to the system If a password is not given, the user is prompted for one. If SCRIPT MODE is enabled, the password is not optional and must be provided.	Only enclosure administrators may execute this command. A maximum of 25 users may be added in addition to the reserved accounts. The <user name> must be unique to all other group names and user names and is case-sensitive. It must be 1-13 characters long and can include alphanumeric, dash, and underscore characters. It must begin with a letter. The <password> must be 3-8 characters long and includes all printable characters. If a password is not entered, the user is prompted for one. **NOTE:** Administrator, “switcha,” “switchb,” and “all” are reserved names and cannot be used. This restriction is not case-sensitive. See Factory Default Settings on page 128 for factory default user accounts.
ASSIGN ADMINSTRA- TOR (RIGHTS)	Promotes a user to have enclosure administrator permissions.	Only enclosure administrators may execute this command.

Table 5-3 User Account Commands (continued)

<user name>	Group membership is not detected in case of enclosure administrator rights are removed at a later time.	The <user name> is case-sensitive.
ASSIGN BAY [ALL | <bay number> {[, | -] <bay number>}] <group name>	Assigns one or more bays to a group. If a bay is already assigned to a group, it must first be unassigned before executing this command.	Only enclosure administrators may execute this command. The <group name> is case-sensitive.
ASSIGNS USER <user name> <group name> {[VIEW | MODIFY]}	Assigns a user to a group with View rights (for group members) or View/Modify rights (for group administrators) If View or View/Modify is not specified, View is chosen by default.	Only enclosure administrators may execute this command. The <user name> is case-sensitive.
DISABLE USER <user name>	Disables a user account. The user is immediately logged out of the system and prevented from log in until the account us enabled.	Only enclosure administrators may execute this command. The <user name> is case-sensitive. The administrator account cannot be disabled.
ENABLE USER <user name>	Enables a user account that was previously disabled by the DISABLE USER command	Only enclosure administrators may execute this command. The <user name> is case-sensitive.
REMOVE GROUP [ALL | <group name>]	Removes a group and automatically unassigns all bays within the group.	Only enclosure administrators may execute this command. The <group name> is case-sensitive.
REMOVE USER [ALL | <user name>]	Removes a user from the system. If **ALL** is specified, the command is run for all users except the default system accounts.	Only enclosure administrators may execute this command. The <user name> is case-sensitive. **NOTE:** Administrator, “switcha,” and “switchb,” cannot be removed.
SET GROUP {DESCRIPTION} <group name> <description>	Sets a group’s description.	Only enclosure administrators may execute this command. The <description> must be 1-20 characters long and can include alphanumeric, dash, and underscore characters. The default group description is blank. If spaces are part of the contact information, enclose the information in quotes.
SET PASSWORD {<password>}	Sets the password of the user currently logged into the Integrated Administrator. If a password is not given on the command line, the user is prompted for one. **NOTE:** This command is not valid in SCRIPT MODE if password is not specified.	The <password> must be 3-8 characters long and can include all printable characters.

Table 5-3 User Account Commands (continued)

SET USER CONTACT {<user name>} <contact info>	If no <user name> exists, the command modifies the contact info of the user that executed the command.	Only enclosure administrators may modify another user's contact information. The <user name> is case-sensitive. The <contact info> must be 1-20 characters long and can include alphanumeric, dash, underscore, and space characters. The default contact information is blank. If spaces are part of the contact information, enclose the information in quotes.
SET USER FULL NAME {<user name>} <full name>	Sets a user's full name. If no <user name> exists, the command modifies the full name of the user that is currently logged in.	Only enclosure administrators may modify another user's full name. The <user name> is case-sensitive. The <contact info> must be 1-20 characters long and can include alphanumeric, dash, underscore, and space characters. The default full name is blank. If spaces are part of this information, enclose the information in quotes.
SET USER PASSWORD <user name>	Sets a user's password. If you do not supply a password on the command line, you are prompted for one. **NOTE:** This command is not valid in SCRIPT MODE if password is not specified.	Only enclosure administrators may modify another user's password. Only the Administrator account may modify the password of the Administrator account. The <user name> is case-sensitive. The <new password> must be 3-8 characters long and can include all printable characters.
SHOW GROUP [<group name> | ALL]	Displays the group's description, a list of members with View permission, a list of members with View/Modify permission, number of bays, and a list of each of the bay the group manages.	Group members and group administrators only see the groups in which they have membership. Users may not execute this command. The <group name> is case-sensitive. If spaces are part of this information, enclose the information in quotes.
SHOW USER [<user name> | ALL]	Displays the user's full name, contact, whether the user has administrator rights, whether the account is enabled, and the groups for which the user has View or View/Modify permissions. If **ALL** is entered, this information is given for every user and an asterisk before the user name denotes the current user.	Only enclosure administrators may view another user's information. The <user name> is case-sensitive. Users who do not have enclosure administrator

Table 5-3 User Account Commands (continued)

		permissions only see their user information.
UNASSIGN ADMINSTRATOR (RIGHTS) <user name>	Takes enclosure administrator rights from a user.	Only enclosure administrators may execute this command. The Administrator account cannot have enclosure administrator rights taken away. The <user name> is case-sensitive.
UNASSIGN USER <user name> <group name>	Removes the user from the specified group.	Only enclosure administrators may execute this command. The <user name> and <group name> are case-sensitive.

Enclosure Network Configuration Commands

Table 5-4

Command	Description	Restrictions
ADD SNMP TRAPRECEIVER <ip address>	Adds an IP address to receive SNMP traps. Only v1 traps are supported. Traps are directed to the SNMP default port of 162.	Only enclosure administrator may execute this command.
DISABLE SECURESH	Disables Secure Shell account to the Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE SNMP	Disables SNMP support for the Integrated Administrator. Does not clear the SNMP trap receivers that have been configured. SNMP trap receivers can still be added and removed. If SNMP is disabled, Systems Insight Manage agents do not work properly.	Only enclosure administrators may execute this command.
DISABLE TELNET	Disables Telnet access to the Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE WEB	Disables HTTP and HTTPS access to the Integrated Administrator. This command prevents access to the Web-based user interface.	Only enclosure administrators may execute this command.
DOWNLOAD CONFIG <url>	Downloads a previously saved configuration file from a specific IP host. The files are auto-executed in script mode. The file is not allowed to change the password of the Administrator account. Supported protocols are http, ftp, and tftp. Format the URL as `protocol://host/path/file`. If your ftp server does not support anonymous connections, you can specify a user name and password by replacing the host part in the previous format with username:password@host.	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.

(continued)

ENABLE SECURESH	Enables Secure Shell account to the Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE SNMP	Enables SNMP support for the Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE TELNET	Enables Telnet access to the Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE WEB	Enables HTTP and HTTPS access to the Integrated Administrator.	Only enclosure administrators may execute this command.
REMOVE SNMP TRAPRECEIVER <ip address>	Removes an IP address from the list of systems to receive SNMP traps	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET DNS <primary address> {<secondary address>}	Sets the primary and secondary DNS server addresses These servers are only used if the system is currently configured to use a static IP address.	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET GATEWAY <ip address>	Sets the network default gateway This gateway is only used if the system is configured to use a static IP address.	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET IPCONFIG [DHCP {DYNAMICDNS} | STATIC <P address> <netmask>]	Sets up the Integrated Administrator IP configuration The gateway and DNS addresses are cleared. The optional DYNAMICDNS argument enables Dynamic DNS.	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET SNMP COMMUNITY [READ | WRITE] <community name>	Sets the community name for the read or write SNMP community The default names for the read and write community are **public** and blank, respectively. If a blank write community name is given, SNMP set commands are disabled until a non-empty community name is given.	Only enclosure administrators may modify another user's contact information. The write <community name> must be 1-20 characters long, and the read <community name> must be 1-20 characters long. Both can include alphanumeric, dash, and underscore characters. The default read community name is **public**. The default write community name is blank.

(continued)

SET SNMP CONTACT <contact>	Configures the name of the system contact.	Only enclosure administrators may execute this command. The <contact> must be 1-20 characters long and can include alphanumeric, dash, underscore, and space characters. If spaces are part of this information, enclose the information in quotes.
SET SNMP LOCATION <location>	Configures the SNMP location of the enclosure. The default location is blank.	Only enclosure administrators may execute this command. The <location> must be 1-20 characters long and can include alphanumeric, dash, underscore, and space characters. If spaces are part of this information, enclose the information in quotes.
SHOW NETWORK	Displays the DHCP state, Dynamic DNS state, IP address, subnet mask, gateway address, primary and secondary DNS addresses, HTTP and HTTPS server status, SNMP status, Secure Shell status, and Telnet status of the enclosure.	None
SHOW SNMP	Displays the SNMP system name, location, and contact, read community name, write community name, and a list of the trap destinations.	Only enclosure administrators may execute this command.

Enclosure Management Commands

Table 5-5

Command	Description	Restrictions
CLEAR SYSLOG ENCLOSURE	Clears the enclosure system log.	Only enclosure administrators may execute this command. Once deleted, this information cannot be restored.
POWEROFF ENCLOSURE {FORCE}	Performs a graceful shutdown of the enclosure. Each blade is first gracefully shut down. If the FORCE argument is given, the enclosure and all blades are immediately shutdown.	Only enclosure administrators may execute this command.
RESTART	Restarts the Integrated Administrator. This does not affect operation of bays in the system.	Only enclosure administrators may execute this command.
SET DATE MMDDhhmm {{CC}YY} {TZ}	Sets the date of the enclosure with the following definitions: • MM: month • DD: day • hh: hour (24-hour format) • mm: minute • CC: century	Only enclosure administrators may execute this command. • MM is an integer from 1-12 • DD is an integer from 1-31

(continued)

	• YY: year • TZ: time zone (case-sensitive) If the time zone is left blank, the current time is left in effect.	• hh is an integer from 0-23 • mm is an integer from 0-59 For a list of time zones, see Time Zone Settings on page 130. NTP must be disabled before manually setting the date and time.
SET ENCLOSURE ASSET {TAG} <asset tag>	Changes the enclosure asset tag	Only enclosure administrators may execute this command. The <asset tag> must be 1-31 characters long and can include alphanumeric, dash, and underscore characters. The default enclosure asset tag is blank. To set a blank asset tag, specify the blank value using the quotes.
SET ENCLOSURE NAME <enclosure name>	Changes the enclosure name	Only enclosure administrators may execute this command. The <enclosure name> must be 1-32 characters long and can include alphanumeric, dash, and underscore characters. < The default enclosure name is IA-MAC, where MAC is replaced with the actual MAC address.
SET ENCLOSURE UID [ON | OFF]	Turns the enclosure Unit Identification LED on or off	Only enclosure administrators may execute this command.
SET RACK NAME <rack name>	Sets the name for the rack where that enclosure resides	Only enclosure administrators may execute this command. The <rack name> must be 1-32 characters long and can include alphanumeric, dash, and underscore characters. The default rack name is **UnnamedRack**.
SHOW CONFIG	Displays the script required to recreate the settings of the enclosure Passwords are not included for any user.	Only the enclosure administrators may execute this command.
SHOW DATE	Displays the current date, time, and time zone of the internal clock of the enclosure.	None
SHOW DISPLAY	Displays whether event notification is on or off.	None
SHOW ENCLOSURE FAN [fan number> | ALL]<	Displays the status, redundancy, and partner, speed, part number for the requested fan. If **ALL** is entered, this information is shown for all fans.	None

(continued)

SHOW ENCLOSURE INFO	Displays the enclosure name, type, part number, serial number, and asset tag; the Integrated Administrator software and hardware version; Integrated Administrator MAC address, and the interconnect tray type, part number, and serial number	None
SHOW ENCLOSURE POWER SUPPLY [<power supply number> | ALL]	Displays the power supply status, AC input status, capacity, input voltage range #1 (measured in Volts), input voltage range #2 (if necessary, measured in Volts), input frequency range (measured in Hertz), part number, serial number, and hardware revision for the specified power supply if one is specified or for all power supplies if ALL is given.	None
SHOW ENCLOSURE STATUS	Under an enclosure status heading, this command displays the health, Integrated Administrator health, and unit identification LED of the enclosure. Under a power status heading, this command displays the power status and capacity.	None
SHOW ENCLOSURE TEMP	Displays the locale, status (OK, warm, degraded, or failed), temperature in degrees Fahrenheit, and temperature sensors.	None
SHOW RACK NAME <rack name>	Shows the name for the rack where the enclosure resides The default rack name is **UnnamedRack**.	None
SHOW SYSLOG ENCLOSURE	Displays the syslog of the enclosure with 22 lines per screen. Typing **q** quits the command, any other key shows the next screen if more information exists to display. Typing **c** continuously displays the System Log without page breaks.	Only enclosure administrators may execute this command.
SHOW TRAY INFO	Displays the manufacturer, product name, part number, serial number, and spare number of the interconnect tray.	None
UPDATE IMAGE <url>	Downloads a new image from a blade over the network and uses the image to update the firmware of the enclosure.	Only enclosure administrators may execute this command. URL can be any of the following: • http://host/path • tftp://host/path • ftp://username:password • @host/path • ftp://host/path where host is a fully qualified domain name or an IP address and path is the pathname of the flash image to download
UPLOAD CONFIG <url>	Upload the current runtime configuration to the specified FTP or TFTP server.	Only enclosure administrators may execute this command.

Blade PC Bay Management Commands

Table 5-6

Command	Description	Restrictions
CLEAR BAY BOOT [FIRST | ONCE | ALWAYS] [ALL | <ay number> {[, | -] <bay number>}]	Clears the setting for the IPL to be passed to the blade at the next reboot. The FIRST argument resets the IPL for all subsequent reboots. The ONCE argument resets the IPL for the next reboot only. The Always argument resets the IPL for every reboot. This command is only valid for present blades. This command may require a firmware update for the BIOS ROM of certain HP blade PCs.	Only enclosure administrators may execute this command.
CLEAR SESSION BAY <bay number>	Terminates a Terminal session from the enclosure. This is not a graceful termination. The connected user loses any unsaved work.	Enclosure administrators may execute this command for blade PC bays and the interconnect switch.
CONNECT BAY <bay number>	Opens a remote console session to the blade PC with that blade PC bay number. A blade PC can only support one remote console session at a time.	Only enclosure and group administrators may execute this command.
GENERATE NMI <bay number>	Generates an NMI on the specified blade. The consequences of an NMI are operating system specific.	Only enclosure and group administrators may execute this command.
POWEROFF BAY <bay number> {[, | -] <bay number>} {FORCE}	Performs a graceful shutdown of the blade PC in the specified bay. If the FORCE argument is given, the blade PC is immediately shut down. This means the blade PC could lose data or become unstable. If no blade PC is in the specified bay, the user is told that the bay is empty.	Only enclosure and group administrators may execute this command.
POWERON BAY <bay number> {[, | -] <bay number>} {[PXE | HDD | RBSU]}	Powers on the specified blade PC. If no blade PC is in the specified bay, the user is told that the bay is empty. The optional boot arguments may require a firmware update for the BIOS ROM of certain HP blade PCs. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Only enclosure and group administrators may execute this command.
REBOOT BAY <bay number> {[, | -] <bay number>} {FORCE} {[PXE | HDD | RBSU]}	Sends a request to the blade PC to perform a graceful shutdown. The blade PC is then powered on. If no blade PC is in the specified bay, the user is told that the bay is empty. The optional boot arguments may require a firmware update for the BIOS ROM of certain HP blade PCs. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Only enclosure and group administrators may execute this command.
SET BAY BOOT FIRST [HDD | PXE] <bay number> {[, | -] <bay number>}	Sets the IPL for each subsequent reboot. This setting is only valid for present blades and is cleared if a blade is removed.	Only enclosure administrators may execute this command.

(continued)

	This command may require a firmware update for the BIOS ROM of certain HP blade PCs.	
SET BAY BOOT ONCE [HDD | PXE | RBSU] <bay number> {[, | -] <bay number>}	Sets the boot device to be used on the next boot of the bay(s) specified. This setting is only valid on present blades and is cleared if the blade is removed. This command may require a firmware update for the BIOS ROM of certain HP blade PCs.	Only enclosure and group administrators may execute this command.
SET BAY UID <bay number> {[, | -] <bay number>} [ON | OFF]	Turns a Unit Identification LED on the blade PC on or off.	Only enclosure and group administrators may execute this command.
SHOW BAY INFO [ALL | <bay number> {[, | -] <bay number>}]	Displays the following fields: Assigned to group, type, name, installed operating system, part number, serial number, asset tag, BIOS version, all CPU types and associated maximum speeds, memory, NIC #1 MAC, and NIC #2 MAC. If no blade PC is in the bay, the user is shown the assigned to group and the blade PC type.	Group members and group administrators only see information for the bays in their groups.
SHOW BAY LIST [ALL | <group name>]	Displays the assigned to group, remote console user, and blade PC name for each bay in a particular group if a group name is specified or all bays if ALL is specified.	Group members and group administrators only see information for the bays in their groups.
SHOW BAY STATUS [ALL | <bay number> {[, | -] <bay number>}]	Displays the power (On or Off), assigned to group, remote console user, health, thermal (OK, warm, degraded, or failed), Unit Identification LED (On or Off), and power state for the blade PC.	Group members and group administrators only see information for the bays in their groups.
SHOW BAY POWER [ALL | <bay number> {[, | -] <bay number>}]	Displays the actual DC power consumption and temperature of key blade PC components.	Group members and group administrators only see information for the bays in their groups.
SHOW SYSLOG BAY <bay number>	Displays the syslog of the specified blade with 22 lines per screen. Typing **q** quits the command; any other key shows the next screen if more information is available to display. The system log of the blade PC is not stored between reboots, so the information only includes what has taken place since the last power on of the Integrated Administrator. Typing **c** continuously displays the System Log without page breaks.	Group members and group administrators only see information for the bays in their groups.
UNASSIGN BAY [ALL | <bay number> {[, | -] <bay number>}]	Removes the bay(s) from their assigned group.	Only enclosure administrators may execute this command.

Command Line Event Messages

Table 5-7 Command Line Event Messages

Message	Possible Cause
User Event Messages	

Table 5-7 Command Line Event Messages (continued)

User Permission Change	One of the following has occurred: • A user has been added, removed, or modified. • A user's group membership has been modified. The blade PC bay membership has been changed for a group with at least one user.
Enclosure Event Messages	
Enclosure Shutdown	The enclosure is being shut down
Enclosure Status Change	The Integrated Administrator detected a change in status due to a change in the state of one or more hardware components or blade PC readings.
Fan Inserted	A fan has been inserted.
Fan Removed	A fan has been removed.
Fan Status Change	The status of fan has changed.
Power Supply Inserted	A power supply has been inserted.
Power Supply Overload	The power system is overloaded. Check each power supply status to determine cause.
Power Supply Redundancy Change	The power supplies are now either redundant or no longer redundant.
Power Supply Removed	A power supply has been removed.
Power Supply Status Change	The status of a power supply has changed.
Restart Event	The Integrated Administrator is about to restart.
Thermal Status Change	The state of a thermal sensor has changed.
Bay Event Messages	
Bay Event	A blade PC bay has been assigned or unassigned from a group.
Blade Inserted	A blade PC was inserted into the enclosure.
Blade Removed	A blade was removed from the enclosure.
Blade Status Change	Health driver detected a change in status due to a change in the state of one or more hardware components or blade PC readings.

Functionality Exclusive to the Command Line Interface

The following table identifies functions or capabilities available to the Command Line Interface (CLI) and unavailable when using the Web-based interface.

Table 5-8 Functions Exclusive to the Command Line Interface — General and General Management Commands

Function	Description	Capability Exclusive to CLI
General Commands		
Sleep <seconds>	Pauses the sessions for a fixed period of time. Useful for adding delays to scripts. The <seconds> field can be any whole number from 1 – 86400. Once the pause has started, no way exists to continue the session before time runs out, but you can terminate the session and start another one.	None
General Management Commands		
CLEAR SESSION SWITCH [A | B]	Terminates a Terminal session from the enclosure This is not a graceful termination. The connected user loses any unsaved work.	All
CLEAR SSHKEY	Removes the contents of the Secure Shell authorized keys file. After performing this command, you will not be able to login using public key-based authentication.	Only enclosure administrators may execute this command.
DOWNLOAD CERTIFICATE <url>	Downloads a CA supplied PKCS#7 file to replace the current security certificate on the system. Supported protocols are http, ftp, and tftp. Format the URL as **protocol://host/path/file**. If your ftp server does not support anonymous connections, you can specify a username and password by augmenting the host part in the above format with username:password@host.	All
DOWNLOAD SSHKEY	Downloads an authorized key file to use with Secure Shell v2 which can contain the public keys for any enclosure administrator. Supported protocols are http, ftp, and tftp. Format the url as **protocol://host/path/file**. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	Only enclosure administrators may execute this command.
GENERATE CERTIFICATE REQUEST	Generates a PKCS#10 certificate request	All
GENERATE CERTIFICATE SELFSIGNED	Generates a self-signed certificate	All
PING {<number>} [<IP address> | <server name>]	Sends ICMP echo messages to a remote IP device If <number> is omitted, only 5 packets are sent. Packets are sent out at 1-second intervals.	All
SET DISPLAY EVENTS [ON | OFF]	Turns event notification on or off	All
SET EXPERT {MODE} [ON | OFF]	Turns EXPERT MODE on or off. When EXPERT MODE is turned on, the system will not prompt the user to confirm actions. Users should exercise caution when working in EXPERT MODE as many actions are not reversible.	None
SET FACTORY	Sets the Integrated Administrator back to its factory defaults	All

Table 5-8 Functions Exclusive to the Command Line Interface — General and General Management Commands (continued)

	The password of the Administrator account does not change. The Integrated Administrator is restarted after all the changes are made. **NOTE:** This command removes all groups, users, and other customization from the memory of the enclosure, and the information is unrecoverable.	
SET SCRIPT MODE [ON | OFF]	When SCRIPT MODE is on, all prompting and verifications of entries cease. If SCRIPT MODE is on, the following commands require a password argument: ADD USER, SET USER PASSWORD, or SET PASSWORD. An enclosure administrator must change the password so that the user can log in to the system. Default values are used for any parameters that would normally require user interaction.	All
SHOW EXPERT {MODE}:	Displays the current EXPERT MODE setting for the current user.	None
SHOW SESSIONS	Displays the connection to each bay and switch if one exists. Only one user may connect to each bay and switch at a time. It also shows the users that are currently logged in, their port number, connect time, and remote system name.	All
SHOW SSHFINGERPRINT	Displays the key fingerprint of the host SSH public key for the Integrated Administrator. This can be used from the serial console to validate the identity of the Integrated Administrator before initializing an SSH connection across a network.	None
SHOW SSHKEY	Displays the contents of the existing Secure Shell authorized keys file that is being used for enclosure administrator key-based authentication.	Only enclosure administrators may execute this command.
DOWNLAOD CONFIG <url>	Downloads a previously saved configuration file from a specific IP host. The file is auto-executed in SCRIPT MODE. The file is not allowed to change the password of the Administrator account. Supported protocols are http, ftp, and tftp. Format the URL as **protocol://host/path/file**. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	All

Table 5-9 Functions Exclusive to the Command Line Interface — Enclosure Management Commands

Function	Description	Capability Exclusive to CLI
Enclosure Management Commands		
SHOW CONFIG	Displays the script required to recreate the settings of the enclosure. Passwords are not included for any user.	All
SHOW ENCLOSURE FAN [<fan number> | ALL]	Displays the status, redundancy, partner, speed, and part number for the requested fan.	The command line adds the fan partner.
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]	Displays the status of the power supply, AC input status, capacity, input voltage range #1 (measured in Volts), input voltage range #2 (measured in Volts), input frequency range	The command line adds the input voltage ranges, input frequency range, serial

Table 5-9 Functions Exclusive to the Command Line Interface — Enclosure Management Commands (continued)

	(measured in Hertz), part number, serial number, and hardware revision for the specified power supply if one is specified or for all power supplies if ALL is given.	number, and hardware revision.
SHOW ENCLOSURE STATUS	Under an enclosure status heading, this command displays the health of the enclosure, Integrated Administrator health, and unit identification LED. Under a power status heading, this command displays the power status and capacity.	The command line adds the Integrated Administrator health.
UPDATE IMAGE <URL>	Downloads a new image from a server over the network and uses the image to update the firmware of the enclosure.	All
UPLOAD CONFIG <url>	Uploads the current runtime configuration to the specified FTP or TFTP server.	All
CLEAR SESSION BAY <bay number>	Terminates a Terminal session from the enclosure.	All
CLEAR BAY BOOT [FIRST | ONCE] [ALL | <bay number> {[, | -] <bay number>}]	Clears the setting for the IPL to be passed to the blade at the next reboot. The “FIRST” argument resets the IPL for all subsequent reboots. The “ONCE” argument resets the IPL for the next reboot only. This command is only valid for present blades. This command may require a firmware upgrade for the BIOS ROM of certain HP blade PCs.	Only enclosure and group administrators may execute this command.
GENERATE NMI <bay number>		
POWERON BAY <bay number> {[, | -] <bay number>} {[PXE | HDD | RBSU]}	Powers on the specified blade PC. If no blade PC is in the specified bay, the user is told that the bay is empty. The optional boot arguments may require a firmware upgrade for the BIOS ROM of certain HP blade PCs. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Allows for optional boot argument
REBOOT BAY <bay number> {[, | -] <bay number>} {FORCE} {[PXE | HDD | RBSU]}	Sends a request to the blade PC to perform a graceful shutdown. The blade PC is then powered on. If no blade PC is in the specified bay, the user is told that the bay is empty. The optional boot arguments may require a firmware upgrade for the BIOS ROM of certain HP blade PCs. Adding an optional boot argument with force the blade to abandon the regular boot order and force a boot using the specified method.	Allows for optional boot argument
SET BAY BOOT FIRST [HDD | PXE] <bay number> {[, | -] <bay number>}	Sets the IPL for each subsequent reboot. This setting is only valid for present blades and is cleared if a blade is removed. This command may require a firmware upgrade of the BIOS.	Only enclosure administrators may execute this command
SET BAY BOOT ONCE [HDD | PXE | RBSU] <bay number> {[, | -] <bay number>}	Sets the boot device to be used on the next boot of the bay(s) specified. This setting is only valid on present blades and is cleared if the blade is removed.	Only enclosure administrators may execute this command.

Table 5-9 Functions Exclusive to the Command Line Interface — Enclosure Management Commands (continued)

	This command may require a firmware upgrade for the BIOS ROM of certain HP blade PCs.	
SHOW BAY LIST [ALL | <group name>]	Displays the assigned to group, remote console user, and blade PC name for each bay in a particular group if a group name is specified or all bays if ALL is specified.	The command line displays the remote console user.
SHOW SYSLOG BAY <bay number>	Displays the syslog of a specified blade with 22 lines per screen. Typing **q** quits the command; any other key shows the next screen if more information is available to display. The system log of the blade PC is not stored between reboots, so the information only includes what has taken place since the last power on of the Integrated Administrator. Typing **c** displays the System Log continuously without page breaks.	All
ADD IPMANAGER <IP address>	Adds an IP address to the list of clients allowed to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE ALERTMAIL	Disables sending e-mail for Integrated Administrator alerts.	Only enclosure administrators may execute this command.
DISABLE IPSECURITY	Allows all clients to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE NTP	Disables automatic updates of the date and time to the Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE ALERTMAIL	Enables sending e-mail for Integrated Administrator alerts.	Only enclosure administrators may execute this command.
ENABLE IPSECURITY	Restricts clients from being able to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE NTP	Enables automatic time and date updates to Integrated Administrator.	Only enclosure administrators may execute this command.
REMOVE IPMANAGER <IP address>	Removes the IP address from the list of clients allowed to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
SET ALERTMAIL [MAILBOX | SENDERDOMAIN | SMTPSERVER]	Sets the e-mail address of the alert recipient, the domain name, and the mail server address.	Only enclosure administrators may execute this command.
SET NTP [PRIMARY | SECONDARY | POLL]	Sets the IP address of the primary and secondary NTP servers. Also sets the frequency of the updates.	Only enclosure administrators may execute this command.
SHOW NETWORK	Displays the DHCP state, Dynamic DNS state, IP address, subnet mask, gateway address, primary and secondary DNS addresses, MAC address, HTTP and HTTPS server status, SNMP status, Secure Shell status, Telnet status, NTP status, NTP primary and secondary server address, NTP poll interval, NTP last update time, IP security configuration, AlertMail status, AlertMail mailbox, SMTP server address and sender domain of the enclosure.	Only enclosure administrators may execute this command.
SET ENCLOSURE SERIAL {NUMBER} <serial number>	Allows modification of the serial number reported by the enclosure information.	Only enclosure administrators may execute this command.

6 Setting Up the System

This chapter explains the levels of user rights recognized by the Integrated Administrator and provides detailed procedures to configure the management functions provided by the Integrated Administrator.

- Customizing the enclosure settings
  - Changing the Administrator password
  - Modifying enclosure and rack names
  - Modifying the asset tag number
  - Modifying the date and time
- Setting up user accounts
  - Adding a group
  - Adding a user
- Enabling remote console sessions to blade PCs
- Setting up AlertMail
  - Adding mailbox address
  - Adding SMTP server address
  - Adding Sender Domain
  - Enabling AlertMail
  - Disabling AlertMail
- Setting up IP Security
  - Adding IP address
  - Enabling IP Security
  - Disabling IP Security
- Setting up Automatic Time Configuration (NTP)
  - Adding primary NTP server
  - Adding secondary NTP server
  - Setting the poll interval

- Enabling NTP
- Disabling NTP

- Configuring SNMP support
  - Entering a community string
  - Modifying the system location
  - Modifying the system contact information
  - Adding trap targets
  - Removing trap targets

For a detailed explanation of the command line conventions used in this document, see Command Line Conventions on page 118.

These procedures are supported by the Web-based user interface and the CLI unless otherwise noted.

NOTE: Most of these tasks are limited to a subset of users. For more information on who can perform each task, see the User Permissions on page 68 section and the section describing that task in this chapter.

User Permissions

The group-centered approach of Integrated Administrator to user permissions facilitates the maintenance of user groups and groups of blade PC bays. This approach operates according to the following principles:

- A blade PC bay is assigned exclusively to one group only.
- A group can be assigned many blade PC bays.
- A user can have various permission levels within any number of groups.
- Access to a blade PC by users or groups depends on the rights assigned to the blade PC bay in which the blade PC is installed.

Use the following table to distinguish the various permission levels available from the HP PC Blade Enclosure Integrated Administrator.

Table 6-1 HP PC Blade Enclosure Integrated Administrator Permissions Levels

Title	Account Type	Permissions	Description
Enclosure Administrator	Administrator	View/Modify for all groups in the enclosure	Enclosure administrators may maintain blade PC bay privileges, manage the enclosure, manage blade PC bays, and create and maintain groups. One special enclosure administrator account (named Administrator) cannot be deleted, disabled, or stripped of enclosure administrator permissions. No other enclosure administrator may change the password to this account. Enclosure administrators cannot disable or delete their own accounts.

Table 6-1 HP PC Blade Enclosure Integrated Administrator Permissions Levels (continued)

Group Administrator	User	View/Modify	Group administrators may manage blade PC bay data for groups in which they are administrators. Group administrators may view blade PC bay data for groups in which they are members. Group administrators may modify their profile (not their privileges) and view enclosure data.
Group member	User	View	Group members may view blade PC bay data for groups in which they are members. Group members may modify their profile (not their privileges) and view enclosure data.
Group member	User		Group member

Customizing the Enclosure Settings

NOTE: Only enclosure administrators may execute these commands.

To change the default Administrator password using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **User List** in the side panel.
3. Click the **Administrator** user name in the user list.
4. Click **View/Modify User**. The View/Modify User screen displays.
5. Click **Change Password**.
6. Type in the new Administrator password in the **Password** and **Confirm password** fields.
7. Click **OK**.

To change the default Administrator password using the CLI, type:

```
SET USER PASSWORD Administrator <new password>
```

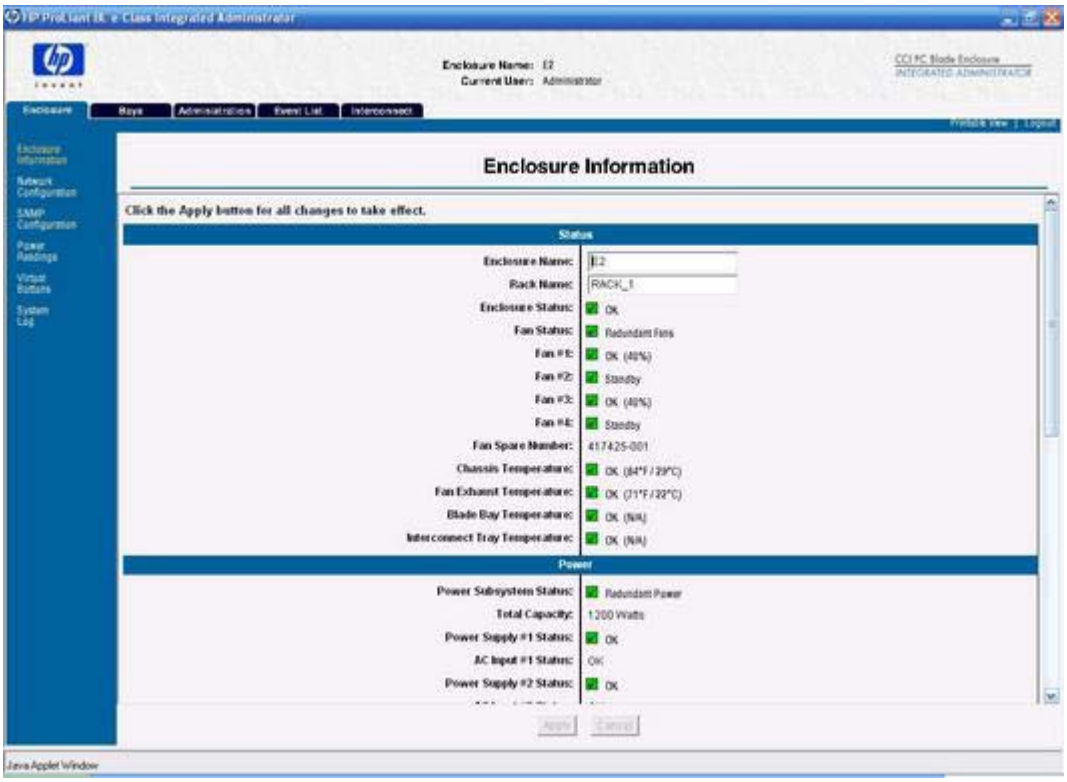
NOTE: The user name (Administrator) is case-sensitive. The <new password> must be 3-8 characters long and can include all printable characters.

Modifying Enclosure and Rack Names

To modify the enclosure name or rack name using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Click the **Enclosure Name** field of the **Status** area.
4. Type the enclosure name.
5. Click the **Rack Name** field of the **Status** area.

6. Type the rack name.



7. Click **Apply**.

To modify the enclosure name or rack name using the CLI, type the following commands sequentially:
`SET ENCLOSURE NAME <enclosure name>`

NOTE: The <enclosure name> must be 1-32 characters long and includes all alphanumeric, the dash, and the underscore characters.

The default enclosure name is IA-XXXXXXXXXXXX where XXXXXXXXXXXX is replaced with the actual MAC address: `SET RACK NAME <rack name>`

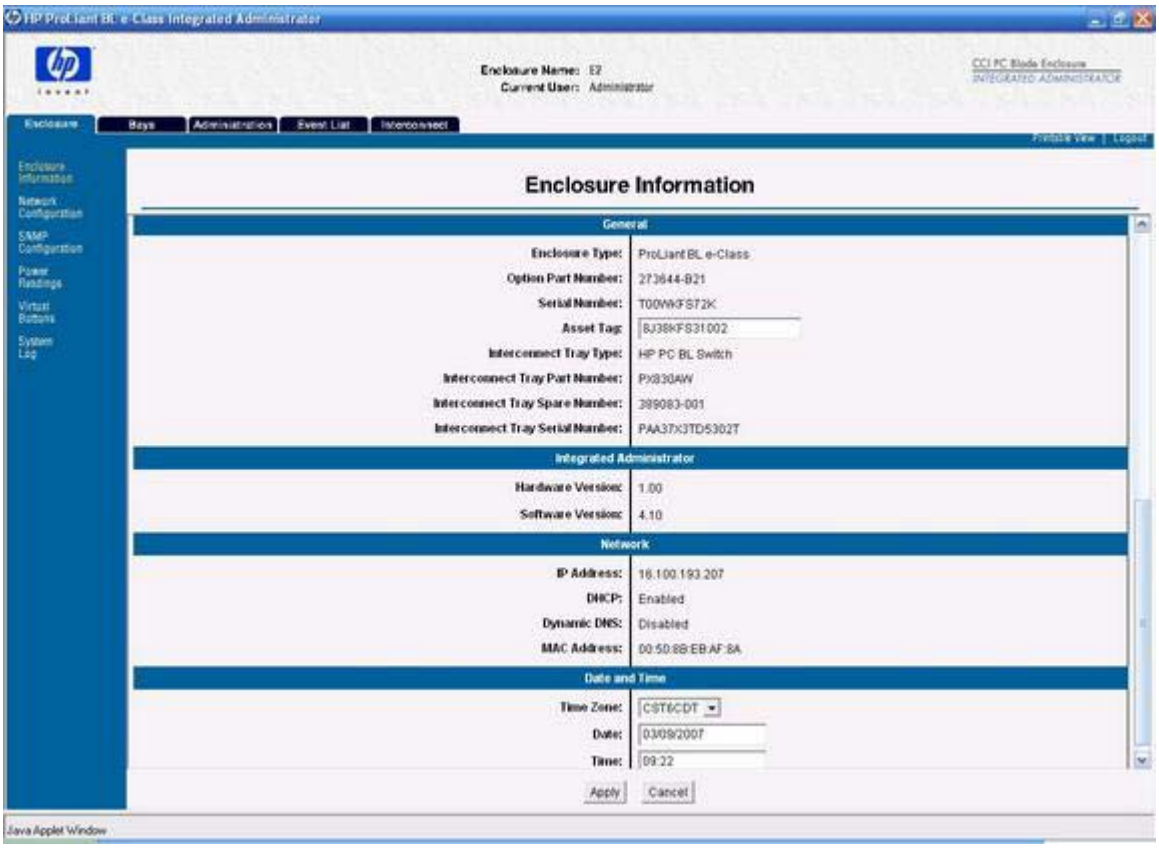
NOTE: The <rack name> must be a maximum of 32 characters long and includes all alphanumeric, dash, and underscore characters. The default rack name is **UnnamedRack**.

Modifying the Asset Tag Number

To modify the asset tag number using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Scroll down to the **General** area.
4. Click the **Asset Tag** field.

5. Type the asset tag number.



6. Click **Apply**.

To modify the asset tag number using the CLI, type:

```
SET ENCLOSURE ASSET {TAG} <asset tag>
```

NOTE: The <asset tag> must be 1-31 characters long and includes alphanumeric, dash, and underscore characters. The default enclosure asset tag is blank.

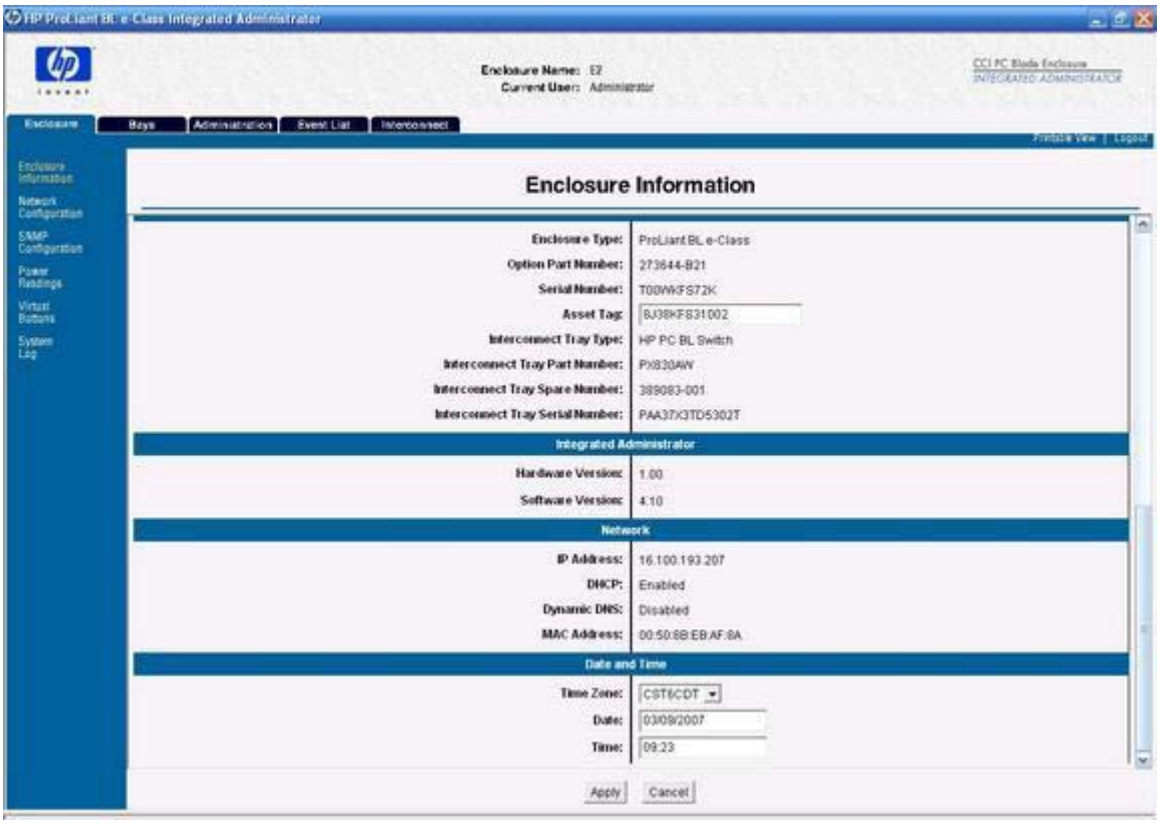
Modifying the Date and Time

To modify the date and time settings using the Web-based user interface:

NOTE: On a Linux system, this information can only be modified using the CLI.

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Scroll down to the **Date and Time** area.
4. Select the proper time zone from the pull-down list.
5. Click the **Date or Time** field.

6. Type the date or time.



7. Click **Apply**.

To modify the date and time settings using the CLI, type:

```
SET DATE MMDDhhmm{{CC}YY} {TZ}
```

where:

- MM: month
- DD: day
- hh: hour (24-hour time, an integer from 0-23)
- mm: minute
- CC: century
- YY: year
- TZ: timezone

NOTE: If the time zone is left blank, the current time zone is left in effect. For a list of supported time zones, see Time Zone Settings on page 130.

Setting Up User Accounts

NOTE: Only enclosure administrators may perform this task.

The Integrated Administrator enables you to manage blade PC bays and administer users by organizing those blade PC bays and users into groups.

This approach enables enclosure administrators, for example, to re-assign user permissions to groups of blade PCs en masse, instead of requiring enclosure administrators to modify permissions one user at a time.

Enclosure administrators assign users access rights to blade PC bays through the following tasks:

- Adding groups with access to specific blade PC bays in an enclosure
- Adding users with certain permissions within specific groups

Adding a Group

NOTE: Restricted default names of group and user accounts (Administrator, switcha, and switchb) are not case-sensitive. Nondefault group and user names are case-sensitive.

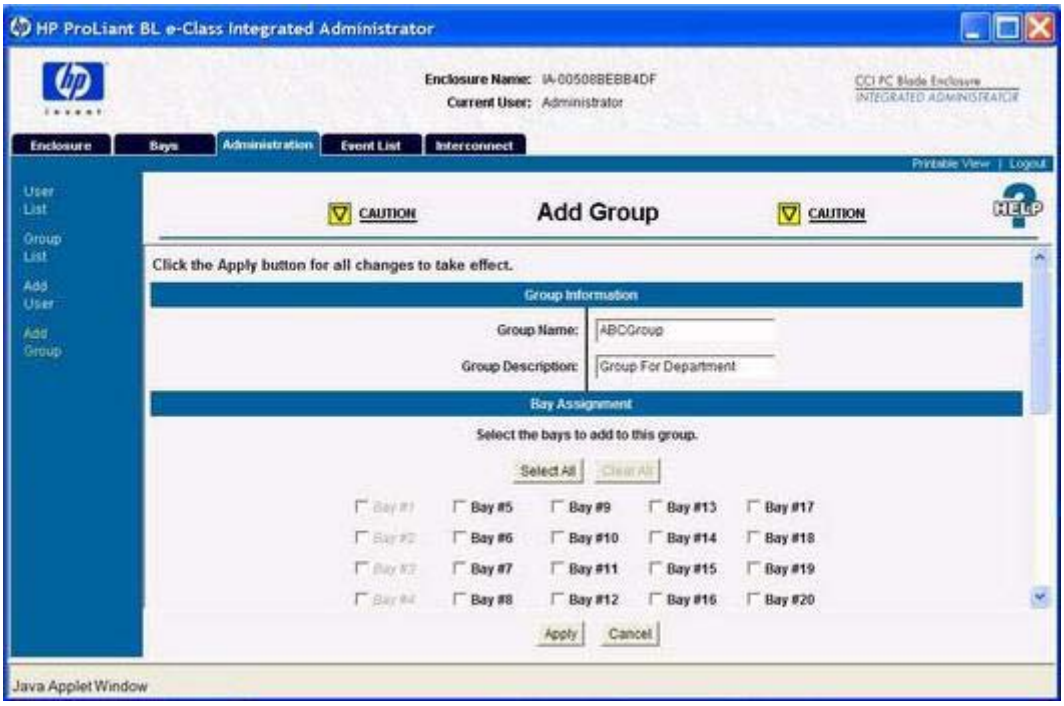
For more information on the Web-based user interface screens for this function, see Group List on page 39. For information on using the CLI, see User Account Commands on page 52.

To create a group using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Add Group** in the left panel.
3. Type the group name and description in the fields.

4. Select bays for the group by selecting the appropriate check boxes.

NOTE: If a blade PC bay is gray, that blade PC bay is inaccessible because it already belongs to another group.



5. To add existing users to this group:

   a. Select users in the **User Names** area.

   b. Click **Add User [View] or Add User [View/Modify]**. For more information on permission levels, see the User Permissions on page 68 section in this chapter.

6. Click **Apply**.

To create a group using the CLI, type the following commands sequentially:

```
ADD GROUP <group name>
```

NOTE: The <group name> must be unique to all other group names and user names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric characters, the dash, and the underscore.

```
SET GROUP {DESCRIPTION} <group name><description>
```

NOTE: The <description> must be 1-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

ASSIGN BAY [ALL | <bay number> {[, | -]<bay number>}] <group name>

ASSIGN USER <user name> <group name> {[VIEW | MODIFY]}

NOTE: The <use name> and <group name> are case-sensitive. The Administrator account cannot be added to a group. The default setting is **View**.

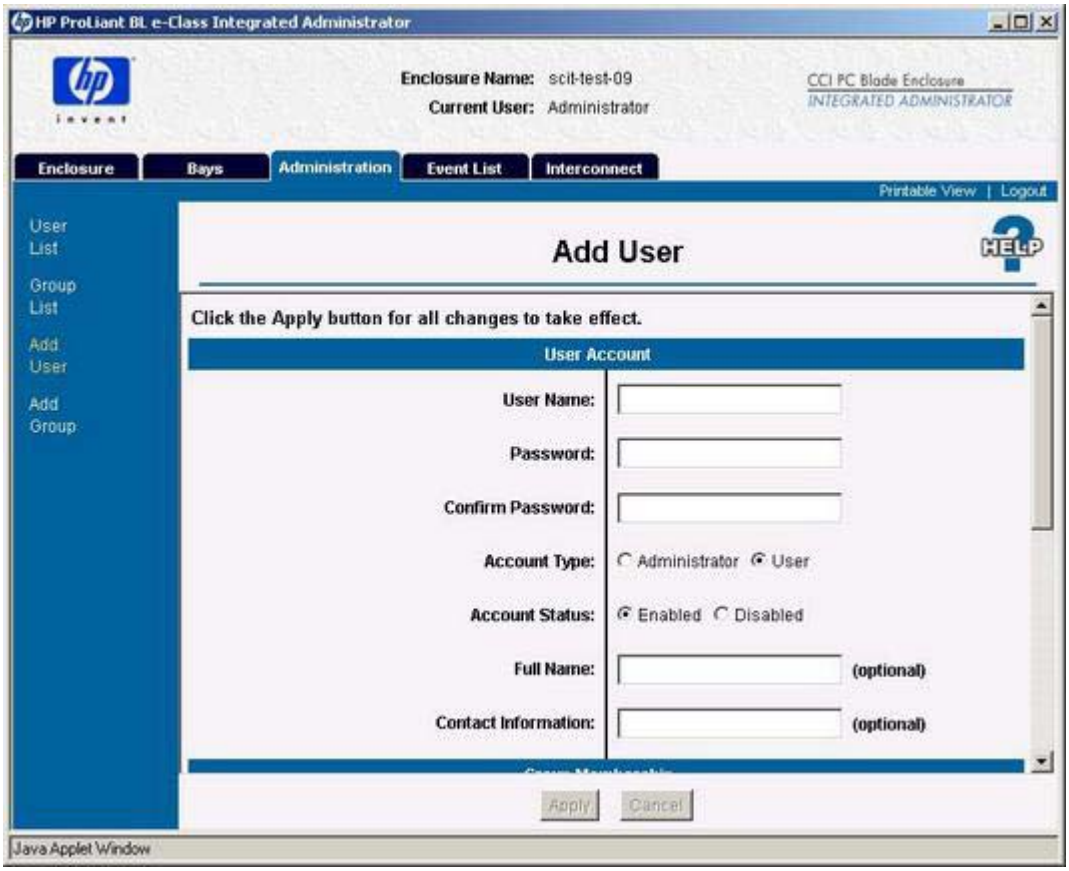
Adding a User

NOTE: Restricted default names of group and user accounts are not case-sensitive. Nondefault group and user names are case-sensitive.

For information on permission levels, see the User Permissions on page 68 section in this chapter.

To create a user using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Add User** in the left panel.
3. Type the user information in the appropriate field. For information on “Account Type,” see the User Permissions on page 68 section in this chapter.



NOTE: The **Account Type** setting determines whether the account holder has management permissions. The optional **Full Name** and **Contact Information** fields provide the account holder’s name and a readily accessible means of contact in case of emergency.

4. To assign the user to an existing group:

   a. Select groups in the **Group Names** area.

   b. Click **Add User [View] or Add User [View/Modify]**. For more information on permission levels, see the User Permissions on page 68 section in this chapter.

5. 5. Click **Apply**.

To add a user using the CLI, type the following commands sequentially:

```
ADD USER <user name> {<password>}
```

NOTE: The <user name> must be unique to all other user names and group names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric characters, the dash, and the underscore. The <password> must be 3-8 characters long and includes all printable characters.

```
ASSIGN ADMINISTRATOR {RIGHTS} <user name>

SET USER FULLNAME {<user name>} <full name>
```

NOTE: The <full name> must be 1-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

```
SET USER CONTACT {<user name>} <contact info>
```

NOTE: The <contact info> must be 1-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

```
ASSIGN USER <user name> <group name> {[VIEW | MODIFY]}
```

Enabling Remote Console Sessions to Blade PCs

The remote console feature of the Integrated Administrator enables a user to connect to the console (serial) connector of the blade PC in order to access the ROM-Based Setup Utility (RBSU). Accessing the RBSU of the blade PC requires nothing more than connecting to the blade PC.

Setting Up AlertMail

AlertMail enables users to receive system events by e-mail instead of using SNMP traps. AlertMail is completely independent from SNMP and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with an SMTP capable mail server.

Table 6-2 AlertMail Commands

Function	Command
Add an e-mail address using command line interface	SET ALERTMAIL MAILBOX <email address>
Add an SNMP server address	SET ALERTMAIL SMTPSERVER <ip address>
Set the sender domain	SET ALERTMAIL SENDERDOMAIN <domain name>
Enable Alertmail	ENABLE ALERTMAIL
Disable Alertmail	DISABLE ALERTMAIL

* For security reasons, some SMTP servers will only forward mail if the sender's domain is set properly. You may need to set this parameter to match the network domain.

E-mail Alerts

AlertMail, if enabled, will send out alerts by e-mail for the following events:

- Enclosure boot message
- IA reboot message
- Fan status change
- Fan inserted
- Fan removed
- Enclosure thermal status change
- Power supply status change
- Power supply inserted
- Power supply removed
- Power subsystem redundancy change
- Blade inserted
- Blade removed
- Blade status change

- Blade thermal change
- Blade fault

NOTE: If the enclosure has a switch installed, it can take up to 60 seconds before the system will send out an AlertMail after a system boot up. Events generated within this period of time will be sent out when the switch has come online.

All e-mails have the following header:

```
Subject: HP AlertMail-SEQ: <SEVERITY> SUBJECT

Date: Date in standard format

From: Enclosure ENCLOSURE-NAME <enclosure-name@domain>

To: RECEIVER MAILBOX
```

Where SEVERITY is one of the following:

- Highest
- # CRITICAL
- # WARNING
- # NOTICE
- # INFO
- Lowest

Example e-mail:

----SAMPLE START----

```
Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2003 15:02:22 +0200

From: Enclosure IA-00508BEBA571 <IA-00508BEBA571@hp.com>

To: user@userdomain

X-OS: HP Integrated Administrator

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed

Enclosure, IA-00508BEBA571, has detected that a power supply in bay 1 has
changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You
can ensure that the center wall assembly is operating correctly by swapping
the two power supplies. Make sure that there are no bent pins on the power
supply connectors before reinserting and that each power supply is fully
seated.
```

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power event has occurred. A blinking LED on the power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL: <https://16.181.75.213/>

- PLEASE DO NOT REPLY TO THIS EMAIL -

----SAMPLE END----

Setting Up IP Security

IP security allows an administrator to define a set of IP addresses that are the only ones allowed to connect to the services provided (SSH, HTTP, TELNET, SNMP). This means that an administrator can make sure only a certain set of machines have access to Integrated Administrator. You can enter a maximum of five IP addresses.

Table 6-3 IP Security Commands

Function	Command
Add an IP address	ADD IPMANAGER <ipaddress>
Remove an IP address	REMOVE IPMANAGER <ip address>
Enable IP security	ENABLE IPSECURITY
Disable IP security	DISABLE IPSECURITY

Setting Up Automatic Time Configuration (NTP)

Automatic time configuration allows the Integrated Administrator to synchronize its date and time with a blade PC supporting the Network Time Protocol (NTP).

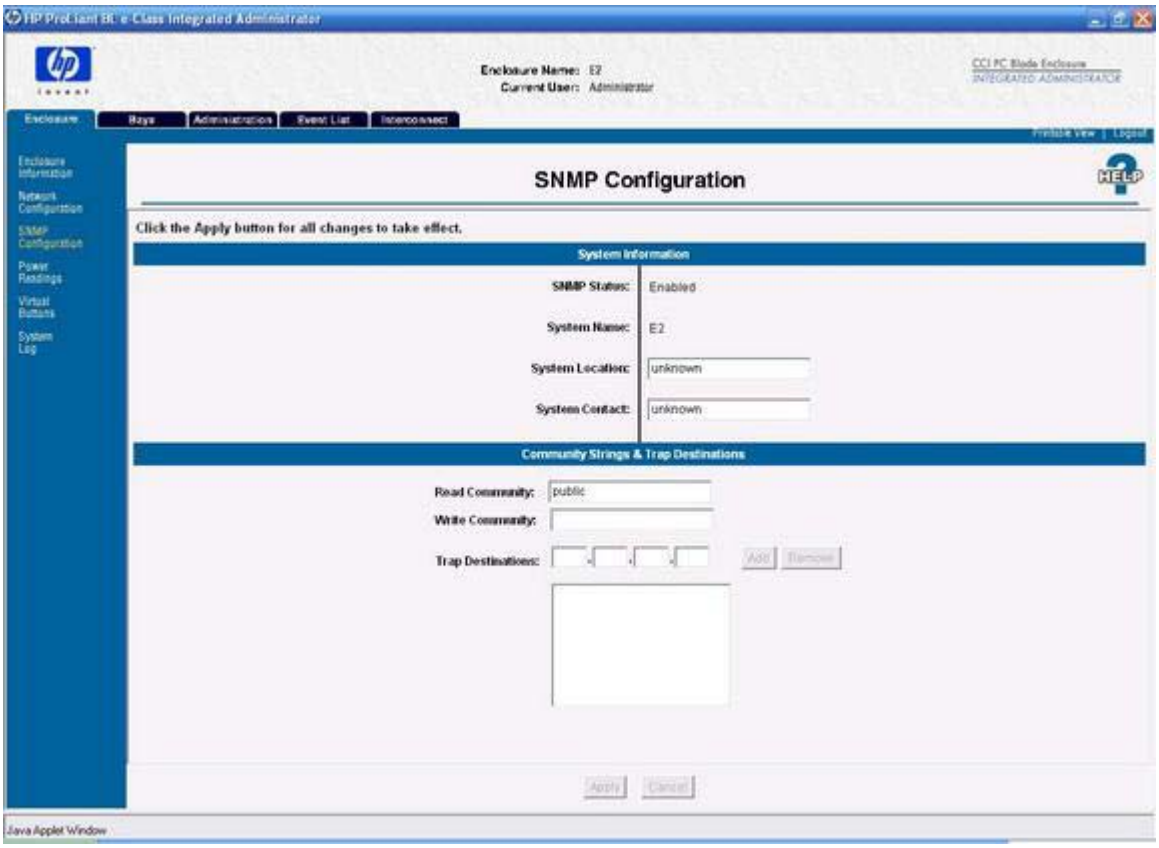
Table 6-4 Automatic Time Configuration Commands

Function	Command
Set the NTPpoll interval*	SET NTP POLL <seconds>
Set the primary NTP server	SET NTP PRIMARY <ip address>
Set the secondary NTP server	SET NTP SECONDARY <ip address>
Disable the secondary NTP server	SET NTP SECONDARY NONE
Enable NTP	ENABLE NTP
Disable NTP	DISABLE NTP

* If an NTP poll interval is not set, it will default to 720 seconds. The minimum time is 60 seconds and the maximum time is 9999 seconds.

Configuring SNMP Support

NOTE: Only enclosure administrators may execute these tasks.



Entering a Community String

To enter a read community or write community string using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Click the **Read Community** or **Write Community** field.
4. Type the string.

NOTE: Entering a blank string into the Read Community field sets the Read Community to "public." Entering a blank string into the Write Community field disables the SNMP set commands.

5. 5. Click **Apply**.

To enter a read community or write community string using the CLI, type:

```
SET SNMP COMMUNITY [READ | WRITE] <community name>
```

The write <community name> must be 1-20 characters long and the read <community name> must be 1-20 characters long. Both community names support all alphanumeric characters, the underscore, and the dash characters.

The default read community name is “public,” and the default write community name is blank.

Modifying the System Location

NOTE: The SNMP protocol can be disabled in the Network Configuration area of the Web-based user interface.

To modify the system location information using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Set the cursor in the **System Location** field and type the appropriate information.
4. Click **Apply**.

To modify the system location information using the CLI, type:

```
SET SNMP LOCATION <location>
```

The <location> field must be 1-20 characters long and supports all the alphanumeric characters, the underscore, the dash, and spaces with quotes.

Modifying the System Contact Information

To modify the system contact information using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Set the cursor in the System Contact field and type the appropriate information.
4. Click **Apply**.

To modify the system contact information using the CLI, type:

```
SET SNMP CONTACT <contact>
```

The <contact> field must be 1-20 characters long and supports all the alphanumeric characters, the underscore, the dash, and spaces with quotes.

Adding Trap Targets

To add a trap target using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Type the IP address in the appropriate field of the SNMP area.
4. Click **Add**.
5. Click **Apply**.

To add a trap target using the CLI, type:

```
ADD SNMP TRAPRECEIVER <IP address>
```

The <IP address> must be in the form ###.###.###.###, where ### ranges from 0 to 255.

The Integrated Administrator only supports v1 traps and directs the traps to SNMP port 162 by default. You can add a maximum of eight IP addresses to receive SNMP traps.

Removing Trap Targets

To remove a trap target list using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Type the list name in the appropriate field of the **SNMP** area.
4. Click **Remove**.
5. Click **Apply**.

To add or remove a trap target list using the CLI, type:

```
REMOVE SNMP TRAPRECEIVER <IP address>
```

The <IP address> must be in the form ###.###.###.###, where ### ranges from 0 to 255.

7 Performing Common Administrative Tasks

This chapter explains the following Integrated Administrator management functionalities:

- Managing blade PC bays
  - Opening a remote console session to a blade PC
  - Accessing ROM-Based Setup Utility for a blade PC
  - Reviewing the activity for a blade PC
  - Powering off the blade PC

    △ **CAUTION:** Without the blade PC health driver, the Integrated Administrator cannot gracefully shutdown a blade PC.
  - Identifying a blade PC using the Unit Identification LED
- Managing the enclosure
  - Reviewing the activity for the enclosure
  - Identifying the enclosure using the Unit Identification LED
  - Generating an enclosure summary
  - Identifying problem components
- Managing users
  - Modifying a user's rights to blade PC bays
  - Disabling and deleting user accounts

Managing Blade PC Bays

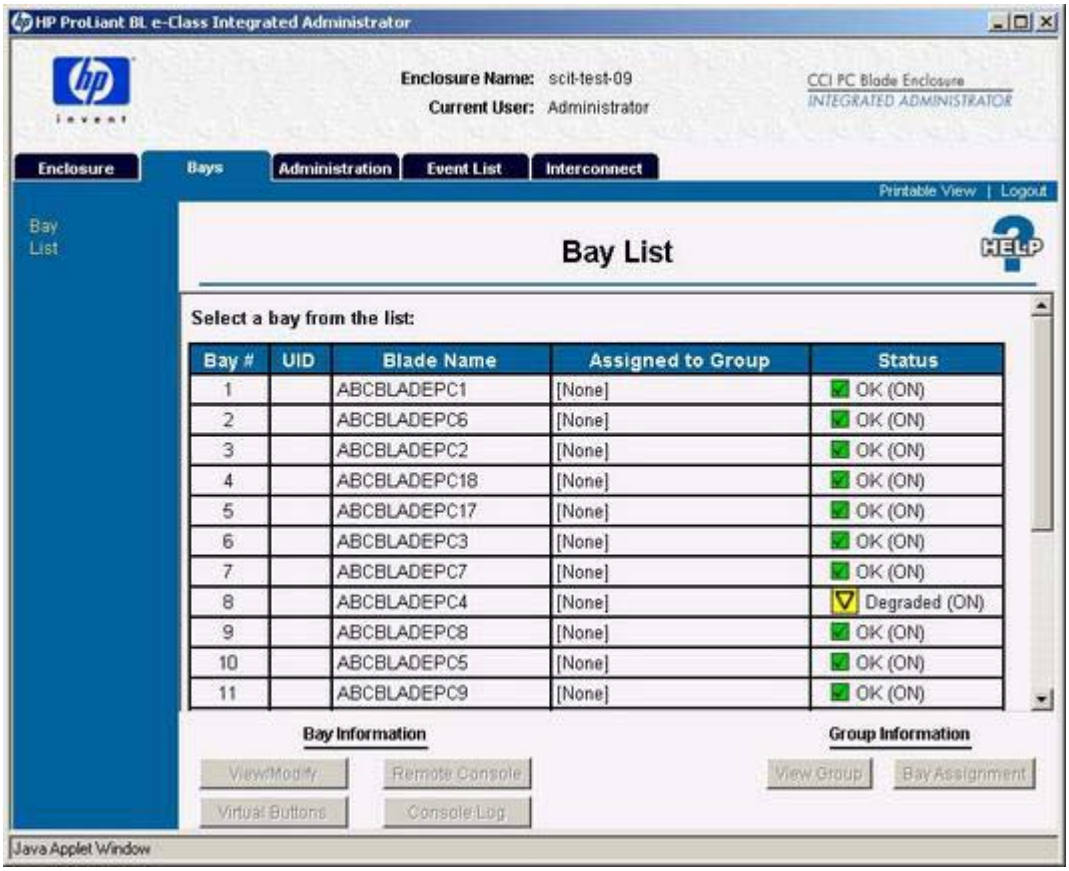
Opening a Remote Console Session to a Blade PC

NOTE: :Enclosure administrators and group administrators with access to the bay can click the Remote Console button to open a remote text-based console to the blade PC in the bay.

To access the remote console using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Select the blade PC from the blade list.

NOTE: The blade PC name is listed in the column titled **Blade Name**. When a blade PC is highlighted, the Bay Information buttons become active.



4. Click **Remote Console**. The Remote Console screen displays.
5. Click **Remote Console** to open a new window that enables you to connect to the blade PC terminal interface.

To access the remote console using the CLI, type:

```
CONNECT BAY <bay number>
```

NOTE: A blade PC can only support one remote console session at a time.

Accessing the ROM-Based Setup Utility for a blade PC

NOTE: Enclosure administrators and group administrators with access to the bay can select the Remote Console button to open a remote text-based console to the blade PC in the bay.

To access the ROM-Based Setup Utility (RBSU) for a blade PC using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Select the bay from the bay list.
4. Click **Remote Console** at the bottom of the screen.
5. Click **Remote Console** from the Remote Console screen.
6. If the blade PC is running the Windows 2000 operating system:
   a. Return to the Web-based user interface and click **Virtual Buttons** in the left panel.

   △ **CAUTION:** Without the blade PC health driver, the Integrated Administrator cannot reboot a blade PC.

   b. If the blade PC is off, select **Power On** at the bottom of the screen; otherwise, select **Reboot** at the bottom of the screen.
   c. Click **Apply** and return to the remote console session.
7. When prompted, press F10 for ROM-Based Setup Utility:
   a. Press Esc.
   b. Press the 0 key.
8. To exit RBSU:
   a. Press Esc.
   b. When prompted, press F10, press the Esc key and the 0 key to confirm.
9. To close the remote console session:
   a. Press the Ctrl+Shift+_ keys.
   b. Press the D key.

To access the RBSU for a blade PC using the command line interface:

△ **CAUTION:** Without the blade PC health driver, the Integrated Administrator cannot reboot a blade PC.

1. If the blade PC is running the Windows 2000 operating system, reboot the blade PC by entering the following commands sequentially:

   ```
   REBOOT BAY <bay number>

   Yes
   ```

2. Connect to the blade PC by observing its bay number and typing:

   ```
   CONNECT BAY <bay number>
   ```

3. When prompted, press the F10 key for ROM-Based Setup Utility for Blade PCs:
   a. Press Esc.
   b. Press the 0 key.

4. To exit RBSU:

   a. Press Esc.

   b. When prompted, press F10, press the Esc key and the 0 key to confirm.

5. To close the remote console session:

   a. Press the Ctrl+Shift+_ keys.

   b. Press the D key.

Reviewing Activity for a Blade PC

NOTE: This task can only be performed for a given blade PC bay by enclosure administrators, group administrators, and group members with access rights to the blade PC bay.

To access the console log for a blade PC using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Choose the bay from the Bay list.
4. Click **Console Log** under **Bay Information**.

To view the system log for a blade PC using the CLI, type:

```
SHOW SYSLOG BAY <bay number>
```

NOTE: Typing `q` quits the command. Typing any other key shows the next screen if more information is available to display. The system log of the blade PC is not stored between reboots, so the information only includes what has taken place since the last power-on of the Integrated Administrator.

Powering Off the Blade PC

CAUTION: Without the blade PC health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shutdown a blade PC. This condition may result in the permanent loss of critical data.

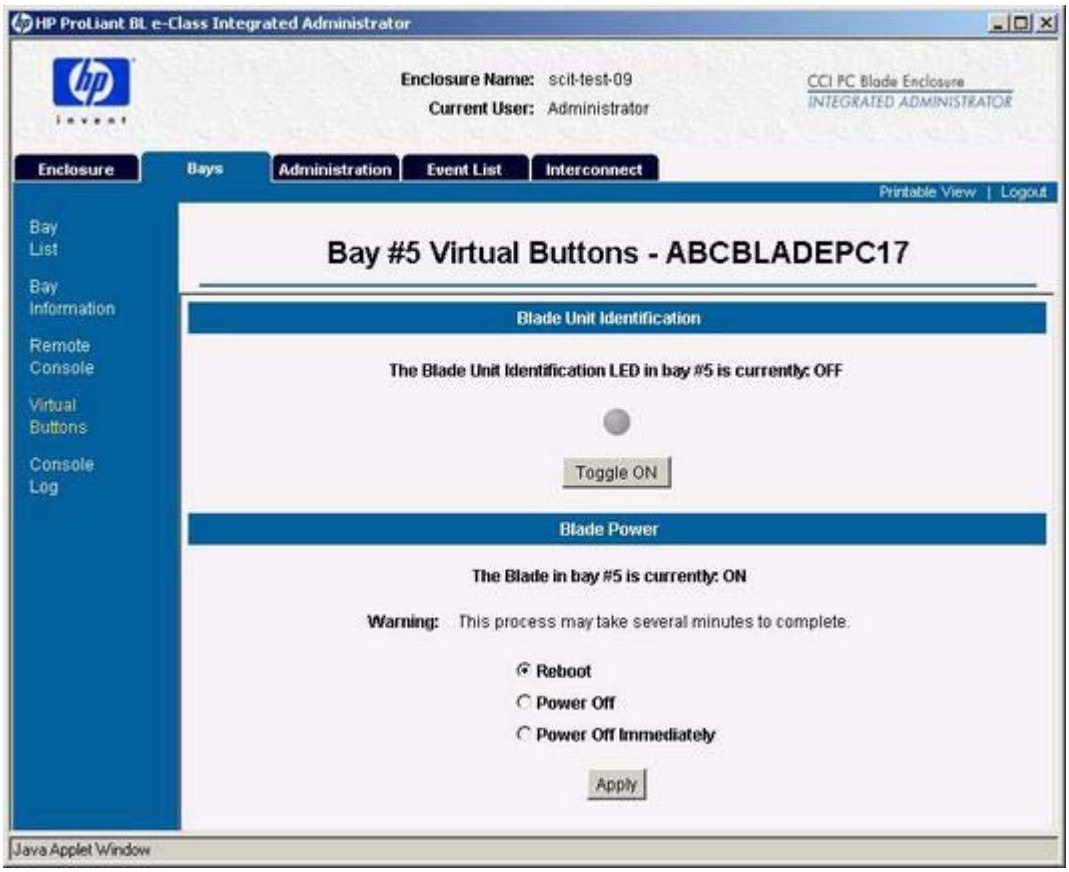
CAUTION: Rebooting or powering off the blade PC removes all power from the blade PC and ends all open sessions.

NOTE: This task can only be performed for a given blade PC bay by enclosure administrators and group administrators with access rights to the blade PC bay.

To reboot or power off the blade PC using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Click the blade PC whose power state to modify.
4. Click **Virtual Buttons** at the bottom of the screen.

5. Click **Reboot**, **Power Off** or **Power Off Immediately**.



6. Click **Apply**.

When the blade PC power is off, the Power Off button text becomes Power On.

To reboot the blade PC using the CLI, type:

```
REBOOT BAY <bay number> {[ , | - ] <bay number>} {FORCE} {[PXE | HDD | RBSU]}
```

NOTE: This command sends a request to the blade PC in a given bay to perform a graceful shutdown and then reboots the blade PC.

To power off the blade PC (immediately or otherwise) using the CLI, type:

```
POWEROFF BAY <bay number> {[ , | - ] <bay number>} {FORCE}
```

NOTE: If the FORCE argument is invoked, the blade PC powers down immediately and could lose data or become unstable.

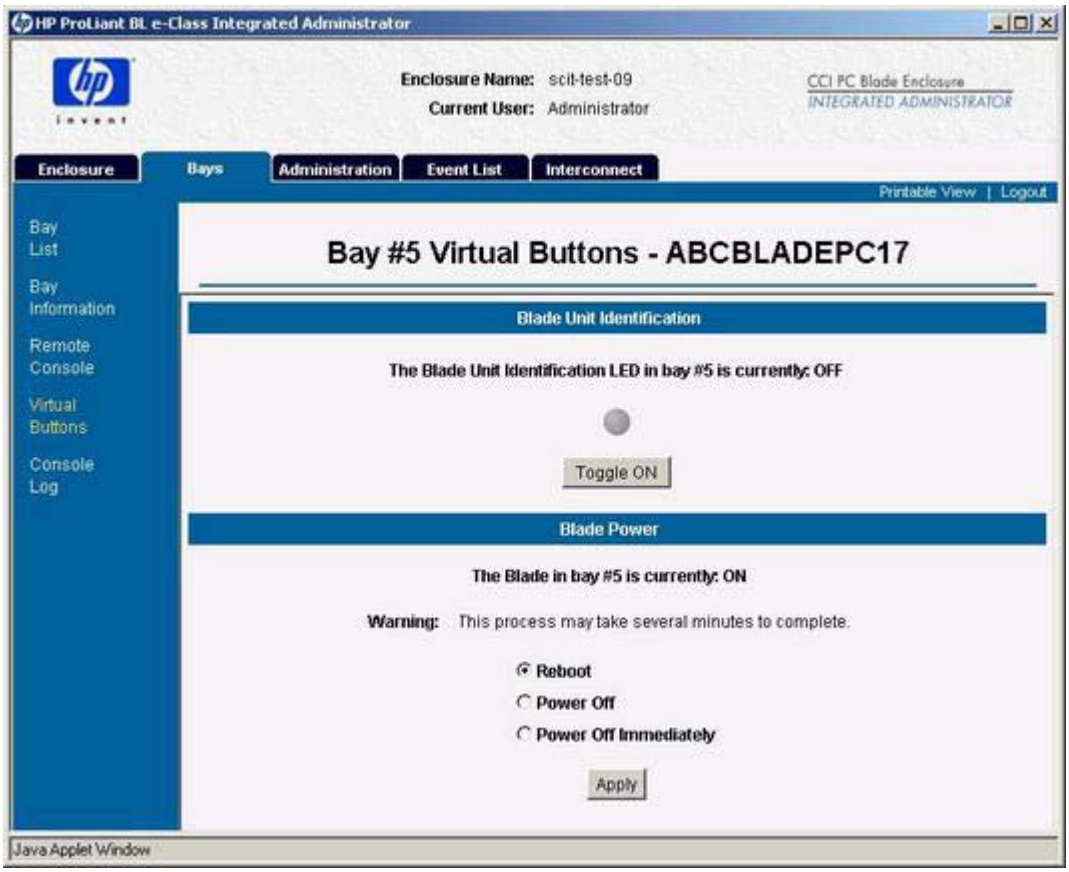
Identifying a Blade PC Using the Unit Identification LED

NOTE: You can perform this task only for a given blade PC bay by enclosure administrators and group administrators with access rights to the blade PC bay.

The virtual button for the Unit Identification LED of the blade PC physically changes the state of the Unit Identification LED on the front panel of the blade PC from off to on, or vice-versa. The Unit Identification LED illuminates bright blue and is designed to help a technician quickly identify a specific blade PC in the data center.

To change the state of a Unit Identification LED of for a blade PC using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Click the blade PC whose Unit Identification LED you wish to toggle.
4. Click **Virtual Buttons** at the bottom of the screen.
5. Click **Toggle ON** or **Toggle OFF** depending on the current state of the Unit Identification LED for the blade PC.



To change the state of the Unit Identification LED for a blade PC using the CLI, type:

```
SET BAY UID <bay number> {[ , | - ] <bay number>} [ON | OFF]
```

Managing the Enclosure

Reviewing the Activity of the Enclosure

The system log of the Integrated Administrator is a chronology of system activities, such as user logins, enclosure shutdowns, and system failures. The system log also displays warnings and errors that occur in the HP PC Blade Enclosure, including:

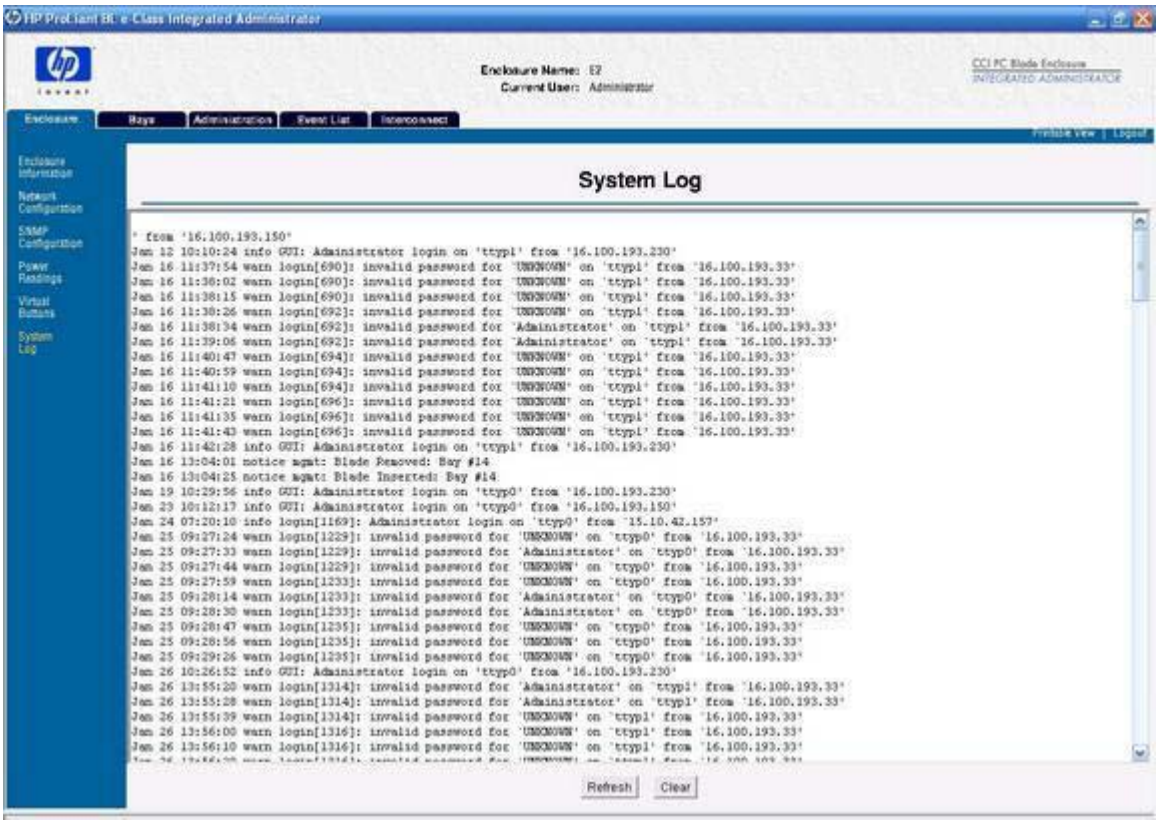
- User account modifications
- Group modifications
- Bay assignment modifications
- Valid and invalid login attempts
- System failures
- System status changes
- Blade insertion and removals
- DHCP, Dynamic DNS, and WINS messages
- Updates to the Integrated Administrator's firmware

Enclosure administrators can view events in the enclosure by accessing the System Log. In contrast to the Event List, no other users can access the System Log. For more information on how the Event List differs from the System Log, see the Identifying Problem Components on page 98 section in this chapter.

To view the System Log using the Web-based user interface:

1. Click the **Enclosure** tab.

2. Click **System Log** in the left panel.



3. To update the System Log, click **Refresh**.

4. To clear the System Log, click **Clear Log**. The Integrated Administrator prompts you to confirm this decision.

To view the System Log of the enclosure using the CLI, type:

```
SHOW SYSLOG ENCLOSURE
```

Only enclosure administrators can execute this command.

Identifying the Enclosure Using the Unit Identification LED

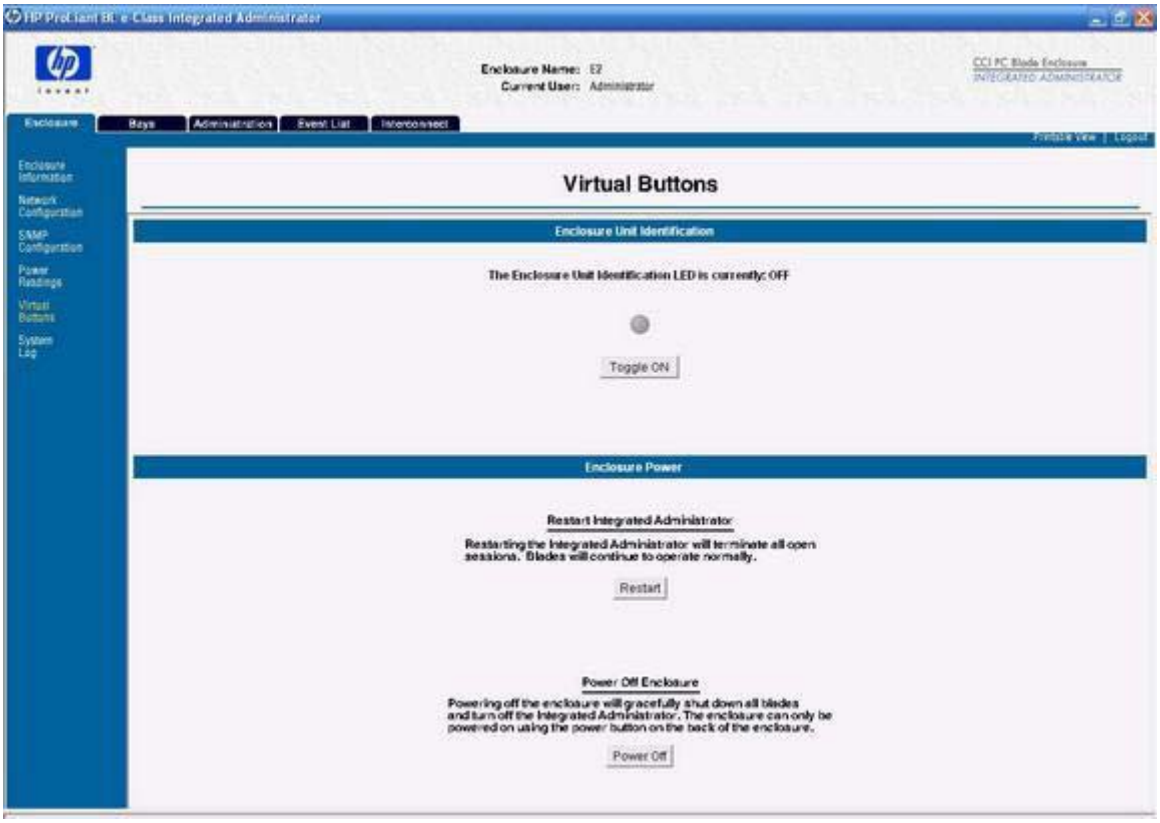
The virtual button for the Unit Identification LED of an enclosure physically changes the state of the Unit Identification LED on the rear panel of the enclosure from Off to On, or vice versa. The Unit Identification LED illuminates bright blue and is designed to help a technician quickly identify a specific enclosure in the data center.

To change the state of the Unit Identification LED of the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.

2. Click **Virtual Buttons** in the left panel.

3. Click **Toggle ON** or **Toggle OFF** depending on the current state of the Unit Identification LED for the enclosure.



To change the state of the Unit Identification LED for the enclosure using the CLI, type:

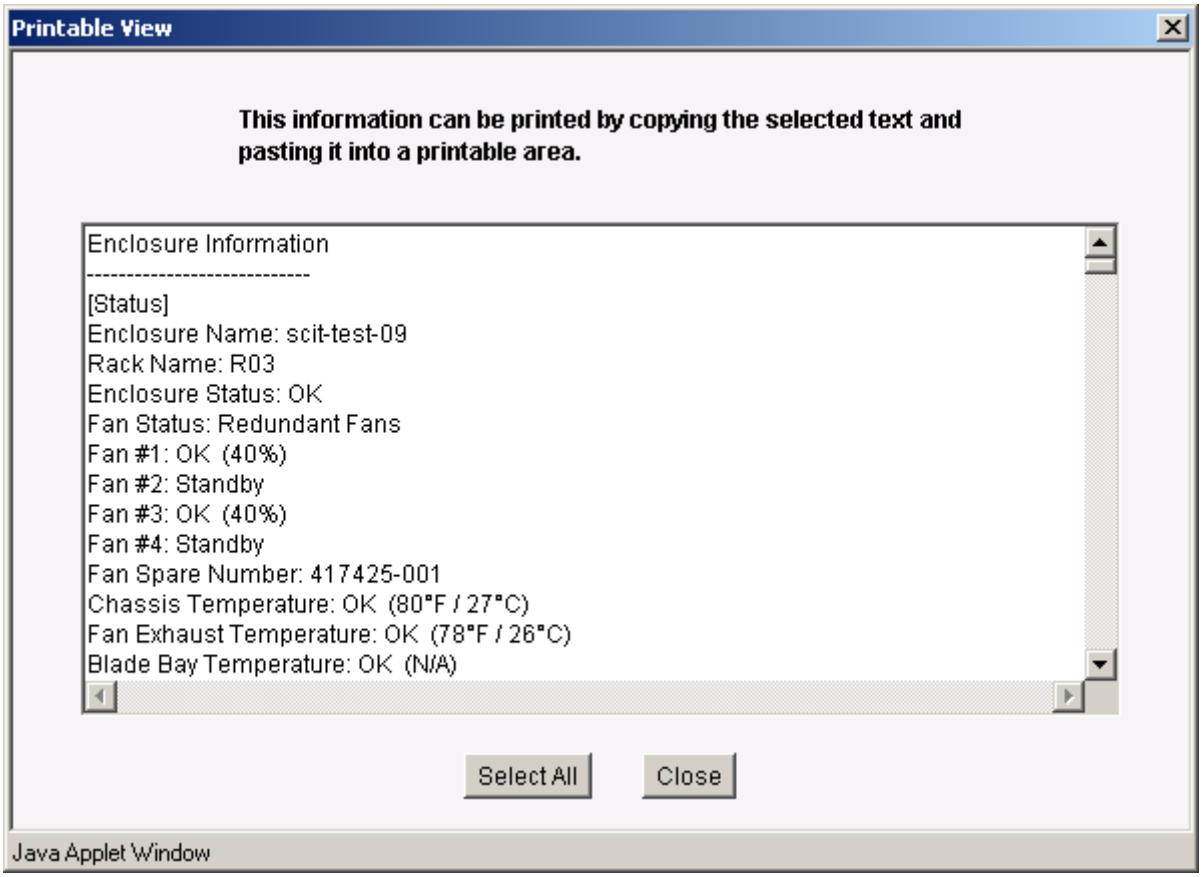
```
SET ENCLOSURE UID [ON | OFF]
```

Only enclosure administrators may execute this command.

Generating an Enclosure Summary

You can generate a printable synopsis of all the data for the enclosure including the enclosure name and type; the part, serial, and asset tag numbers of the enclosure; the software and hardware versions of the Integrated Administrator; the MAC address of the Integrated Administrator; and the type, part number, and serial number of the interconnect tray.

To generate a printable synopsis of all the data for the enclosure using the Web-based user interface, click Printable View in the top panel. The Web-based user interface opens a new window that shows all enclosure information, which you can copy and paste into a printable file.



To obtain the enclosure information using the CLI, enter the following commands as needed:

```
SHOW ENCLOSURE FAN [<fan number> | ALL]
```

This command displays the status, redundancy, partner, speed, and part number for one or all fans in the enclosure.

```
SHOW ENCLOSURE INFO
```

This command displays the enclosure name and enclosure type; the software and hardware version of the Integrated Administrator; the part number, serial number, and asset tag number of the enclosure; the MAC address of the Integrated Administrator; and the type, part number, and serial number of the interconnect tray.

```
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]
```

This command displays the status, AC input status, capacity, input voltage range #1 (Volts), input voltage range #2 (Volts), input frequency range (Hz), part number, serial number, and hardware revision for one or all power supplies in the enclosure.

```
SHOW ENCLOSURE STATUS
```

This command displays the status of enclosure health, Integrated Administrator health, and the Unit Identification LED under the heading “enclosure status,” and displays the status and capacity of the power supplies of the enclosure under the heading “power status.”

```
SHOW ENCLOSURE TEMP
```

This command displays the location, status (OK, warm, degraded, or failed), and temperature (degrees Fahrenheit and Celsius) for all the temperature sensors of the enclosure.

Identifying Problem Components

The Integrated Administrator alerts you to problem conditions or failed components in the enclosure, such as:

- A fan
- A power supply
- A blade PC
- Over-temperature conditions

If the enclosure enters a degraded state at any time, the Web-based user interface of the Integrated Administrator alerts the user with icons along the top of the deck panel.

Identify the degraded components in the enclosure and their respective part numbers in the following ways:

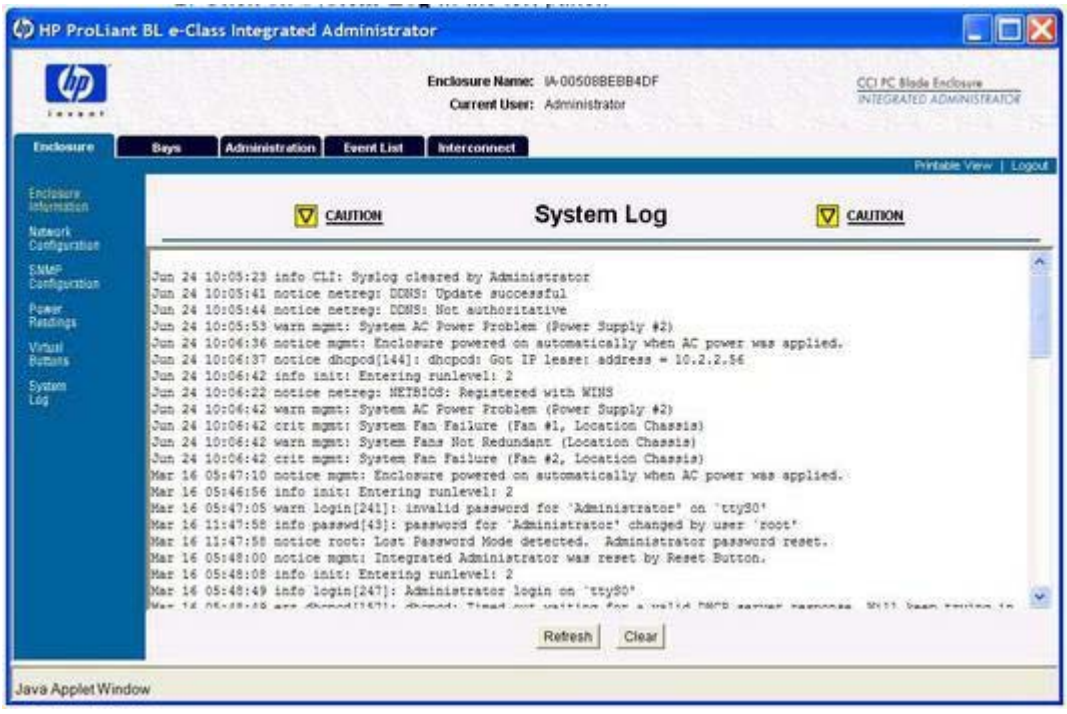
- Opening the enclosure system log
- Opening the event list - the event list differs from the system log in the following ways:
  - Any user can view the event list. Only enclosure administrators can access the system log.
  - The messages in the event list are limited to cautions and critical failures. Refer to the enclosure system log for information on fixes.
  - The event list only displays messages received since the user logged into the Integrated Administrator. The system log displays every message generated by the enclosure diagnostics.
- Clicking on the **Caution** or **Critical** icon along the top of the deck panel

This action opens the event list. By highlighting an item in the event list and clicking **View Event Details**, you can access the area within the Integrated Administrator that provides detailed information about that degraded component.

NOTE: As soon as you click the **Caution** or **Critical** icon, that icon disappears whether the degraded conditions are corrected or not.

To identify a degraded component using the System Log from the Web-based user interface:

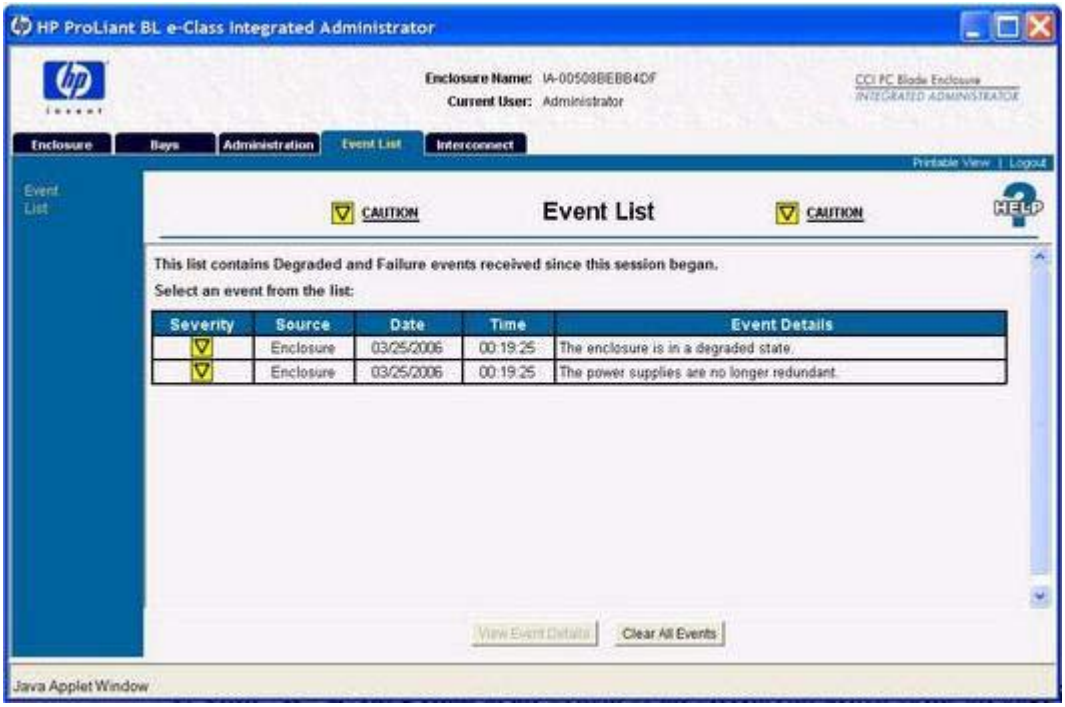
1. Click on the **Enclosure** tab.
2. Click on **System Log** in the left panel.



3. Go to the appropriate area in the Integrated Administrator for the spare number of the degraded component.

To identify a degraded component using the event list from the Web-based user interface:

1. Click the **Event List** tab.

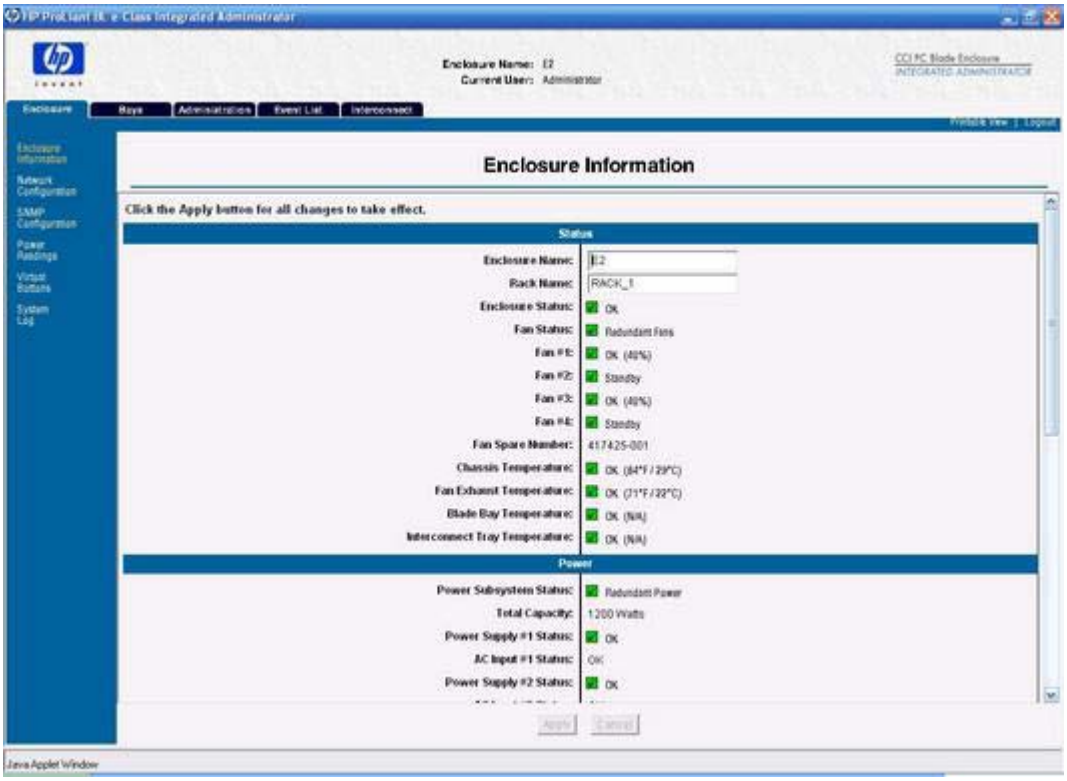


2. Click the degraded item in the event list.

3. Click **View Event Details** at the bottom of the screen. This action opens the page in the Integrated Administrator that displays information about the degraded component.

To identify a degraded component using the **Caution** or **Critical** icons along the top of the deck panel from the Web-based user interface, click an icon. This action opens the event list.

By highlighting an item in the event list and clicking **View Event Details**, you can access the area within the Integrated Administrator that provides detailed information about that degraded component.



To identify a degraded component using the CLI:

1. Type: `SET DISPLAY EVENTS [ON | OFF]`

2. Type the appropriate commands:

   `SHOW ENCLOSURE FAN [<fan number> | ALL]`

   This command displays the status, redundancy, partner, speed, and part number for one or all fans in the enclosure.

   `SHOW ENCLOSURE INFO`

   This command displays the enclosure name, type, part number, serial number, and asset tag number; the Integrated Administrator software and hardware version; the MAC address of the Integrated Administrator, and the interconnect tray type, part number, and serial number.

   `SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]`

   This command displays the status, AC input status, capacity, input voltage range #1 (Volts), input voltage range #2 (Volts), input frequency range (Hz), part number, serial number, and hardware revision for one or both power supplies in the enclosure.

   `SHOW ENCLOSURE STATUS`

   This command displays the status of enclosure health, Integrated Administrator health, and the Unit Identification LED under the heading “enclosure status,” and displays the status and capacity of the power supplies of the enclosure under the heading “power status.”

   `SHOW ENCLOSURE TEMP`

This command displays the location, status (OK, warm, degraded, or failed), and temperature (degrees Fahrenheit or Celsius) for all the temperature sensors of the enclosure.

Managing Users

NOTE: Only enclosure administrators may perform these tasks.

NOTE: Restricted default names of group and user accounts (Administrator, switcha, and switchb) are not case-sensitive. Nondefault group and user names are case-sensitive.

Modifying a User's Rights to Blade PC Bays

You can only modify a user's rights to blade PC bays by modifying their group rights, specifically by choosing one of the following methods:

- Creating a new group for the user with the updated access rights to the blade PC bays
- Modifying the rights to blade PC bays for a group to which the user has membership

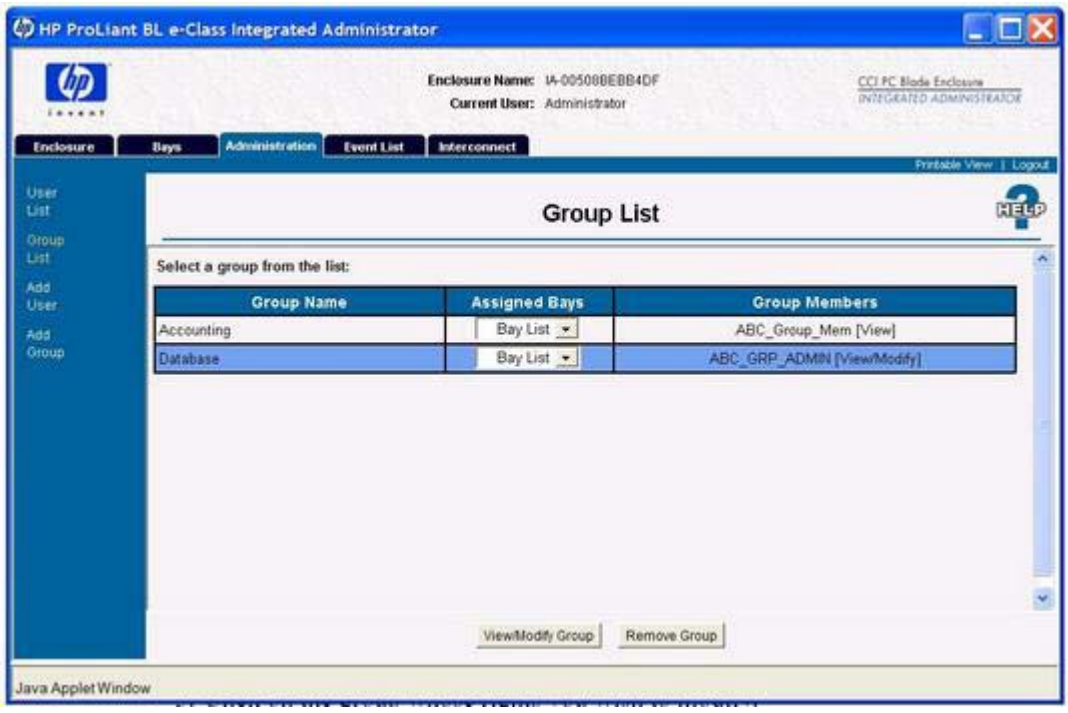
Creating a New Group with the Updated Access Rights

To create a new group with the updated blade PC access profile you wish to assign your user, see Adding a Group on page 73.

Modifying Group Rights to Blade PC Bays

To modify group rights to blade PC bays using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Group List** in the left panel.



3. Click on the group whose rights you wish to modify.

4. Click **View/Modify Group**.

5. Select the appropriate check boxes for the available blade PC bays that reflects the updated rights you wish to give the group.

6. Click **Apply**.

To modify rights to blade PC bays for an existing group using the CLI, choose from among the following commands:

NOTE: Only enclosure administrators may execute these commands.

- To expand the number of blade PCs assigned to a group, type:

```
ASSIGN BAY [ALL | <bay number> {[ , | - ]<bay number>}] <group name>
```

  If a blade PC bay is currently assigned to a group, this command re-assigns the bay from its current group to the new group.

- To remove access rights to blade PC bays for any group, type:

```
UNASSIGN BAY [ALL | <bay number> {[ , | - ] <bay number>}]
```

Disabling and Deleting User Accounts

NOTE: Only enclosure administrators may execute this command. Group accounts can be deleted, but cannot be disabled.

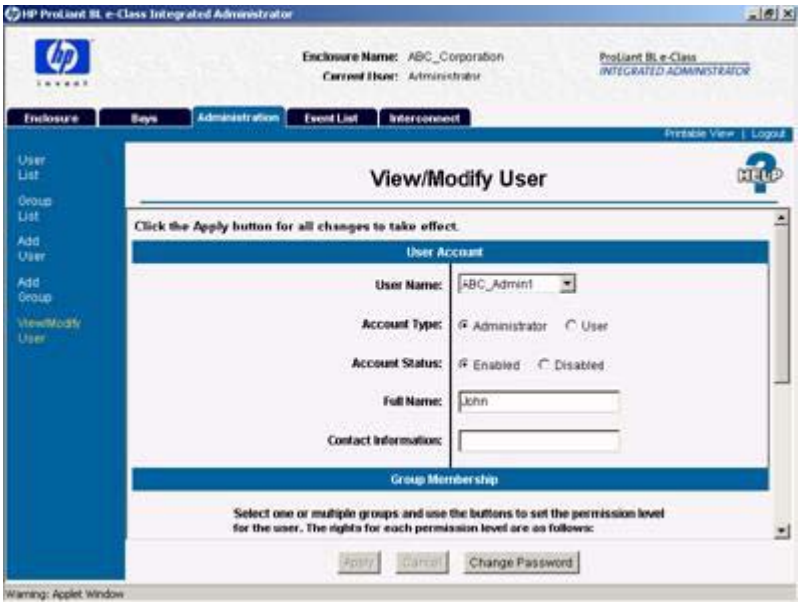
To disable a user account using the Web-based user interface:

1. Click the **Administration** tab.

2. Click on **User List** in the left panel.

3. Select the user whose account you wish to disable from the user list.

4. Click **View/Modify User**.



5. Set the account status to **Disabled**.
6. Click **Apply**.

To disable a user account using the CLI, type:

```
DISABLE USER <user name>
```

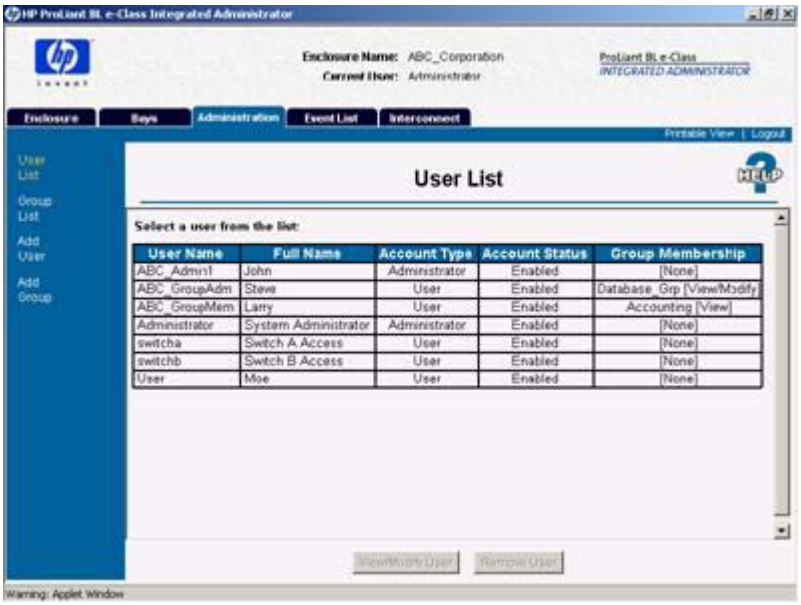
When this command is executed, the user is immediately logged out of the system and prevented from logging in until the account is enabled.

Deleting a User Account

To delete a user account using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **User List** in the left panel.

3. Select the user account you wish to delete from the user list.



4. Click **Remove User**.

To delete a user account using the CLI, type:

```
REMOVE USER [ALL | <user name>]
```

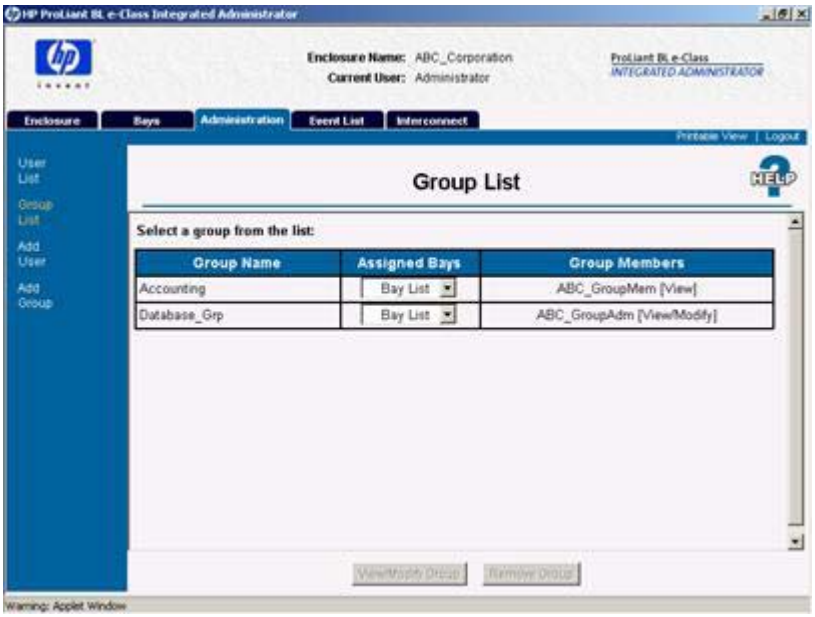
If **ALL** is specified, the command deletes all the user accounts except the Administrator account. The Administrator account cannot be removed.

Deleting Group Accounts

To delete a group account using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Group List** in the left panel.

3. Select the group from the group list.



4. Click **Remove Group**.

To delete a group account using the CLI, type:

```
REMOVE GROUP [ALL | <group name>]
```

If **ALL** is specified, the command deletes all the group accounts.

8 Performing Advanced Functions

This chapter provides an explanation of the following advanced tasks you can perform using the Integrated Administrator. These procedures are supported by the Web-based user interface and the CLI unless otherwise noted:

- Replicating the configuration of the Integrated Administrator
- Administering security certificates
  - Creating a security certificate
  - Downloading a security certificate
- Key-Based SSH Authentication
- Configuring a Blade PC Boot Order
- Powering off the enclosure
- Disabling network protocols to the Integrated Administrator
- Upgrading the firmware of the Integrated Administrator
- Recovering a lost Administrator password
- Launching flash disaster recovery

NOTE: Only enclosure administrators may perform the tasks in this chapter.

Replicating the Configuration of the Integrated Administrator

NOTE: The Integrated Administrator does not support this task using the Web-based user interface.

To set up several enclosures with the same configuration, configure one enclosure (such as add all user accounts, add all groups, and assign bays) and then replicate that configuration on the other enclosures.

To replicate the configuration of the Integrated Administrator using the CLI:

1. Login as Administrator on the first enclosure.
2. Type: `UPLOAD CONFIG <url>`. This command uploads the current runtime configuration to the specified TFTP or FTP server. If your FTP server does not allow anonymous uploading, specify an FTP username and password using the syntax:

   `ftp://username:password@ftpserver/filename`
3. Edit the uploaded configuration file using a text editor to customize the configuration (such as user names, passwords, and network settings) for the other enclosures.

   NOTE: Step 4 only applies if the other enclosures have been configured previously.

   NOTE: For security reasons, passwords are never replicated in the configuration file.
4. Restore the factory defaults on each of the other enclosures to clear any previous configuration:
   a. Login as Administrator on an enclosure to which you intend to replicate the configuration.
   b. Type: `SET FACTORY`. This command sets the Integrated Administrator back to its factory default settings, although the password of the Administrator account does not change. The Integrated Administrator is restarted after all the changes are implemented. IMPORTANT: Only the Administrator account may execute this command.
5. Download the configuration to each of the other enclosures:
   a. Log in as Administrator on an enclosure to which you intend to replicate the configuration.
   b. Type: `DOWNLOAD CONFIG <url>`. The Integrated Administrator does not check the configuration file for errors, but auto-executes the file in script mode. The file is not allowed to change the password of the Administrator account. Supported protocols are http, ftp, and tftp. Format the URL as `protocol://host/path/file`. If your ftp server does not support anonymous connections, specify a user name and password by replacing the host part in the above format with `username:password@host`.

      NOTE: Step c applies only if you did not set user account passwords in the configuration file.

   c. Set the password for each user account. For commands, see Chapter 5, in section “User Account Commands.”

Administering Security Certificates

NOTE: The Integrated Administrator does not support these tasks using the Web-based user interface.

Creating a Certificate Request

To create a security certificate using the CLI, type: `GENERATE CERTIFICATE REQUEST`

This command generates a PKCS#10 certificate request. This certificate request can be sent to your certification authority (CA) to obtain a PKCS#7 certificate file to use below.

To create a self-signed security certificate using the CLI, type: `GENERATE CERTIFICATE SELFSIGNED`

This command generates a self-signed PKCS#7 certificate to replace the existing SSL certificate. This certificate is signed with the current name of the enclosure and will be valid for 10 years. Users who do not have a certificate authority (CA) may use this certificate as a replacement.

Downloading a Security Certificate

To download a security certificate using the CLI, type:

`DOWNLOAD CERTIFICATE <url>`

This command downloads a CA supplied PKCS#7 file to replace the current security certificate on the system.

Supported protocols are http, ftp, and tftp. Format the URL as: protocol://host/path/file

If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format: `username:password@host`

Key-Based SSH Authentication

Users may install their own public SSH keys for password-less logins to the Integrated Administrators. Only enclosure administrators can use key-based authentication. The CLI features four commands to install and manage the authorized SSH keys.

- To view any current installed authorized SSH keys, type: `SHOW SSHKEY`

  This command shows any keys currently installed on the Integrated Administrator that are authorized to log in using an enclosure administrator account.

- To view the fingerprint of the Integrated Administrator host key, type: `SHOW SSHFINGERPRINT`

  This command shows the fingerprint of the host key for the Integrated Administrators. Users may compare this fingerprint with the fingerprint displayed by their SSH client when connecting to the Integrated Administrators to guarantee the authenticity of the Integrated Administrator connection. Users who need guaranteed authenticity will want to use the Integrated Administrator serial console to obtain the SSH fingerprint for the first time.

- To clear any currently installed authorized SSH keys, type: `CLEAR SSHKEY`

  This command clears any authorized keys currently installed on the Integrated Administrator that are authorized to log in. After this command has been issued, all users have to enter a valid password in order to log in.

- To download and install one or more SSH keys, type: `DOWNLOAD SSHKEY <url>`

This command downloads and install a file containing one or more SSH keys which are authorized to log into the Integrated Administrator. The new file will replace any existing keys.

Supported protocols are http, ftp and tftp. Format the URL as: `protocol://host/path/file`.

If your ftp server does not support anonymous logins, you can specify a username and password by replacing the host part (in previous format) with: username:password@host.

The Integrated Administrator supports multiple SSH keys in one downloaded file. Max file size for SSH keys is 16K.

Key-based SSH logins has an advantage for use with scripting as well. Remote commands can be sent to any Integrated Administrator after installing the appropriate authorized key without having to enter a password between each command. Using the OpenSSH package, the user can send commands using the following syntax: `ssh user@host command`

You can group together commands to perform a series of actions. To view the health status of the enclosure and all blades with a single command, type:

```
ssh user@host "SHOW ENCLOSURE STATUS; SHOW STATUS BAY ALL"
```

By having an authorized key file installed on the Integrated Administrator, the user can combine these without having to enter a password between each command sent to the Integrated Administrator.

Configuring Blade PC Boot Order

Enclosure and group administrators may change the boot order, sometimes referred to as Initial Program Load (IPL), of their blade PCs by using the CLI of the Integrated Administrator. The change can be made permanently or only for the next reboot. Several commands are available in the CLI to control the blades in this manner. This feature requires version 1.20 or higher of the Integrated Administrator firmware and a blade ROM dated 06/15/02 or newer to be controlled in this manner.

To set a blade PC boot order, type:

```
SET BAY BOOT FIRST [HDD | PXE] [ALL | <bay number> {[,|-] <bay number>}]
```

During the next reboot, this will set the specified blade PC boot order to use the given boot device first. This has the same effect as changing the Standard Boot Order (IPL) setting in the RBSU on the blade PC.

To set a blade PC boot order for the next boot only, type:

```
SET BAY BOOT [ONCE | ALWAYS] [HDD | PXE | RBSU] [ALL | <bay number> {[,|-]
<bay number>}]
```

This will force the specified blade PC to boot to the specified media on the next boot only. The RBSU setting will make the blade PC(s) boot into the RBSU which can be viewed with the Remote Console functionality. The HDD setting forces the blade PC to boot from the hard drive first, and the PXE setting forces it to boot from the integrated NIC first.

To reset blade boot order settings which have not yet taken effect, type:

```
CLEAR BAY BOOT [FIRST | ONCE | ALWAYS] [ALL | <bay number> {[,|-] <bay
number>}]
```

This will clear changes to the specified blade PC boot order that were made with the SET BAY BOOT command. It only affects pending changes so if the blade PC has been rebooted since the SET BAY BOOT command, this command will have no effect.

The POWERON BAY and REBOOT BAY commands have been extended to allow an argument which sets blade PC boot order for that boot only. These settings are the same as the SET BAY BOOT ONCE command.

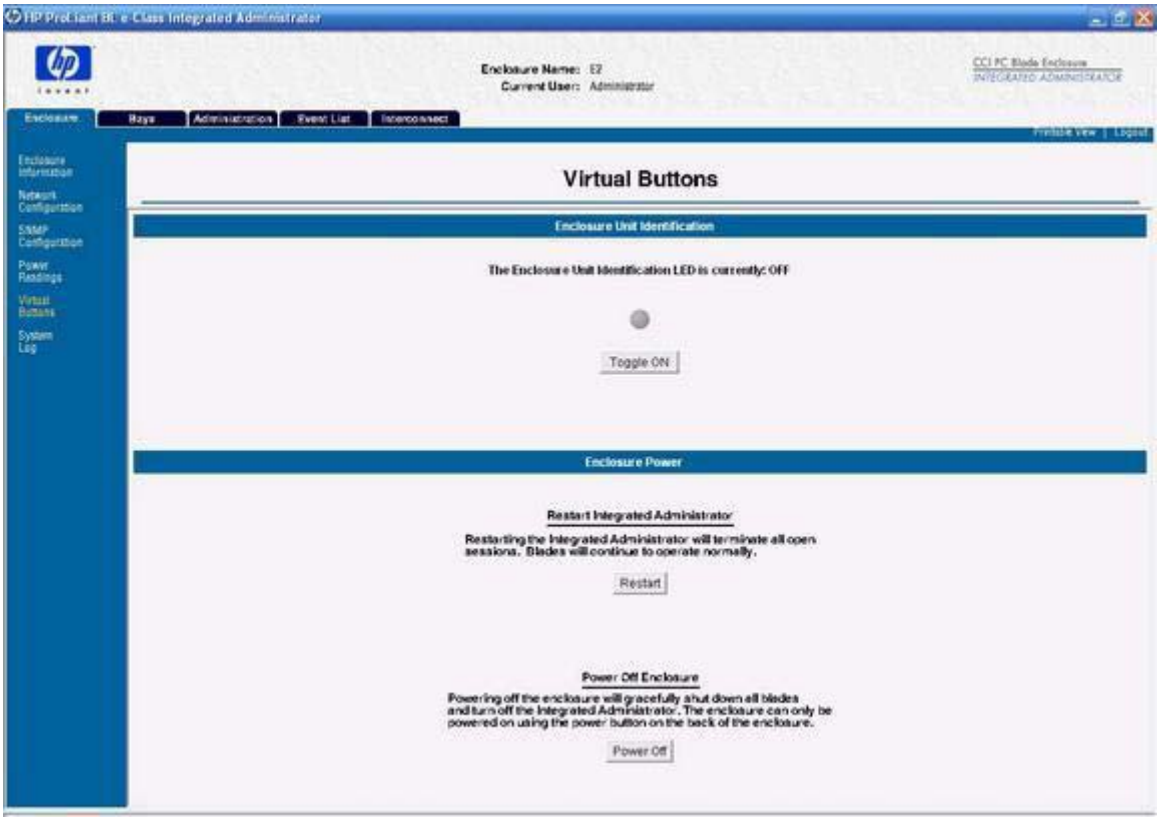
To determine if any boot order changes are pending for a specific blade, use the SHOW BAY INFO command. The “Pending Boot Order:” status line will show any pending changes to the boot order, either one-time or permanent.

Powering Off the Enclosure

△ **CAUTION:** Powering off the enclosure removes all power from the blade PCs and ends all open sessions. After powering off the enclosure, you can only power on the enclosure if you have physical access to the enclosure.

To power off the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Virtual Buttons**.
3. Click **Power Off**.



4. Click **Apply**.

To power off the enclosure using the CLI, type: `POWEROFF ENCLOSURE`

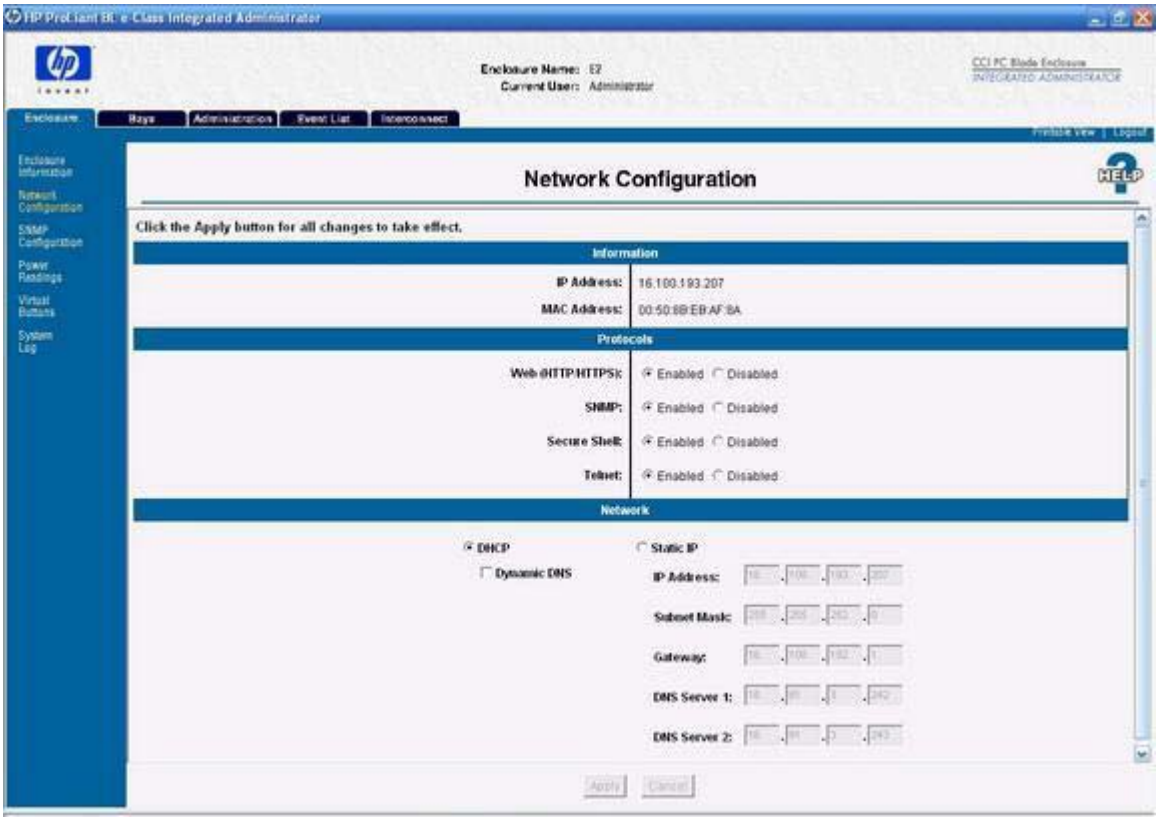
This command attempts to perform a graceful shutdown of the enclosure by powering off each blade PC and then powering off the enclosure. After 5 minutes, the command powers down all components of the system immediately if they are not already powered off.

△ **CAUTION:** Without the blade PC health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shutdown a blade PC. This condition may result in the permanent loss of critical data.

Disabling Network Protocols

To modify the supported communications protocols of the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Network Configuration** in the left panel.



3. Select the appropriate radio buttons in the **Protocols** area.
4. Click **Apply**.

To modify the supported communications protocols of the enclosure using the CLI, choose from among the following commands:

- To disable http/https communication, type: `DISABLE WEB`

  Disabling http/https causes the users to lose access to the Web-based user interface.

- To disable automatic time updates, type: `DISABLE NTP`
- To disable SNMP communication, type: `DISABLE SNMP`
- To disable Secure Shell communication, type: `DISABLE SECURESH`

Disabling Secure Shell causes the users to lose access to the Web-based user interface.

- To disable telnet communication, type: `DISABLE TELNET`

Upgrading the Integrated Administrator Firmware

The firmware associated with the Integrated Administrator can be upgraded remotely using the CLI using the management (10/100 Ethernet) connector located on the rear panel of the enclosure.

```
UPDATE IMAGE <url>
```

The <url> can be any of the following:

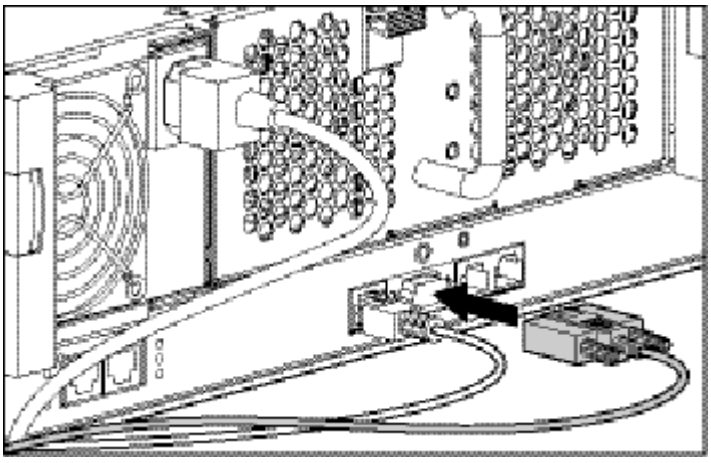
- http://host/path
- tftp://host/path
- ftp://username:password@host/path
- ftp://host/path

...where “host” is a fully qualified domain name or an IP address and path is the pathname of the flash image to download. Refer to the documentation associated with the firmware upgrade for detailed information.

Recovering a Lost Administrator Password

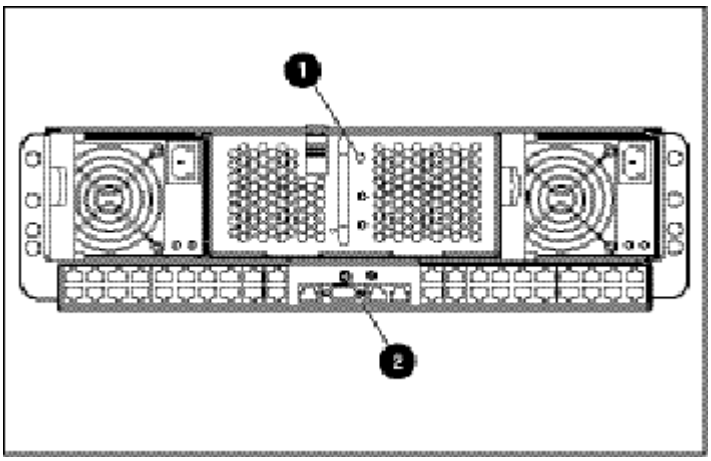
To recover a lost Administrator password:

1. Be sure the local client device is properly configured for local access to the Integrated Administrator. See Chapter 3, in section Requirements for Local Client Devices on page 11.
2. Connect a local client device to the Integrated Administrator (serial) console connector using the nullmodem serial cable (provided with the enclosure).



3. Open a terminal emulation application.

4. Press and hold the enclosure Unit Identification button (1) and press the Integrated Administrator Reset button (2) simultaneously on the rear panel of the blade PC to place the enclosure in Lost Password/Flash Disaster Recovery mode.



5. When the serial console prompt appears, press the L key.

This command boots the system in Lost Password mode, which resets the Administrator password to the factory default and displays it on the console.

Launching Flash Disaster Recovery

Flash Recovery mode requires the following items:

- DHCP server
- TFTP server
- A connection to the Integrated Administrator serial console
- Integrated Administrator ROM image file on the TFTP server

NOTE: The filename of the ROM image of the Integrated Administrator can be any valid ASCII filename. The ROM image of the Integrated Administrator can be any valid image that supports the “update image" facility in the operating system.

The Integrated Administrator will automatically enter Flash Recovery mode when a corrupted image is detected. Flash Recovery mode can also be manually initiated.

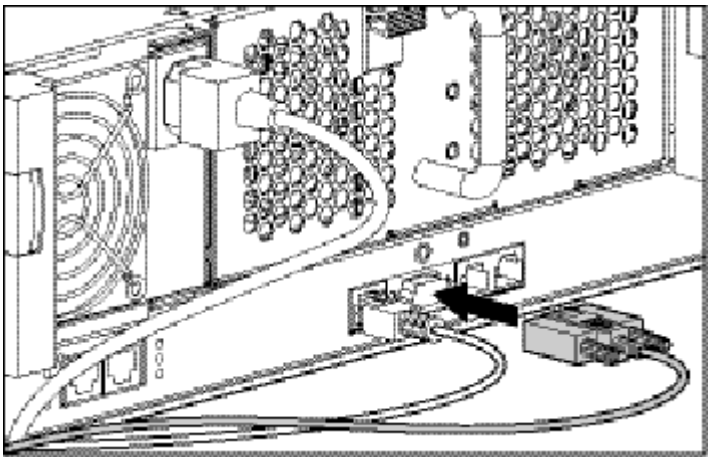
NOTE: No timeout exists for obtaining a DHCP address.

The Flash Recovery process should only be initiated when the Integrated Administrator fails to boot properly because an operating system image is corrupted by some unforeseen problem, such as a power/catastrophic failure during the standard “update image” flash procedure.

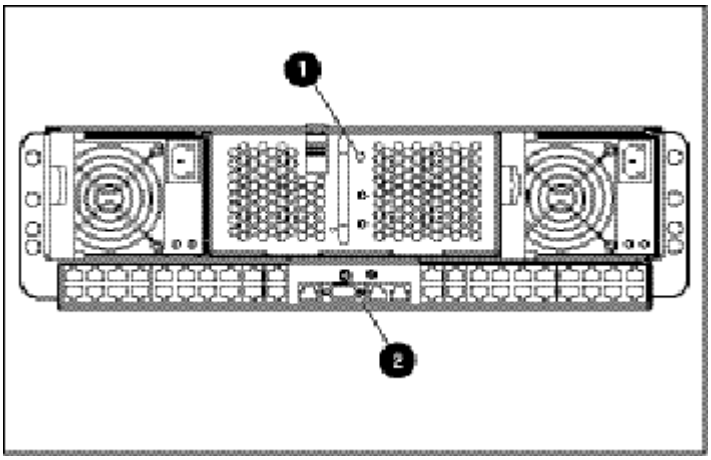
Flash Recovery mode makes every attempt to successfully flash the operating system image of the Integrated Administrator. The only way to leave Flash Recovery mode without successfully updating the image is to reset the Integrated Administrator.

You can manually place the Integrated Administrator in Flash Recovery mode:

1. Connect a local client device to the Integrated Administrator (serial) console connector using the nullmodem serial cable (provided with the enclosure). See Requirements for Local Client Devices on page 11.



2. Press and hold the enclosure Unit Identification button (1) and press the Integrated Administrator Reset button (2) simultaneously on the rear panel of the blade PC to place the enclosure in Lost Password/Flash Disaster Recovery mode.



3. When the serial console prompt appears, press the F key.

NOTE: This command is case-insensitive.

Pressing the L key launches Lost Password recovery mode. Pressing any other key exits Lost Password/ Flash Disaster Recovery mode and reboots the system.

This command boots the system in Flash Disaster Recovery mode, prints a message, and resets the enclosure.

Upon entering Flash Disaster Recovery mode, the Integrated Administrator attempts to acquire a DHCP address. If successful, the Integrated Administrator prompts the user for:

- IP address of the TFTP server
- Filename of the ROM on the TFTP server

The Integrated Administrator then downloads and verifies the ROM and updates the flash memory.

NOTE: No timeout exists for obtaining a DHCP address.

NOTE: If the ROM does not download properly or if the verification step fails, Flash Disaster Recovery mode restarts with another attempt to acquire a DHCP address.

The Integrated Administrator reboots.

A Command Line Conventions

The following table lists the conventions used by the Command Line Interface (CLI).

Table A-1 CLI Conventions

Symbol	Description
<lower case>	Devotes input to be keyed in
UPPER CASE	Denotes input to be keyed in as shown
[]	Denotes choices to be made where a choice is mandatory
{}	Denotes choices to be made where a choice is optional
|	Separates input options
“”	Used to enclose arguments that contain spaces

For example, the following command requires the user to input whether the Integrated Administrator is operating in a “DHCP” or “Static” network environment.

SET IPCONFIG [DHCP {DYNAMICDNS} | STATIC <IP address> <netmask>

Specifying “Dynamic DNS” is optional for executing this command for the DHCP environment, but specifying the IP address and netmask are required for executing this command for the static environment.

B Error Messages

The messages provided in this appendix are divided into the following categories:

- Warning messages
- Error messages

Warning Messages

This section provides a comprehensive list of warning messages specific to the major components of the Integrated Administrator. These warning messages advise you that you have implemented a configuration change or prompt you to confirm whether you wish to proceed with your requested action.

Enclosure Warning Messages

Table B-1 Enclosure Warning Messages

Warning Message	Cause
Are you sure you want to disable the Web protocol? Disabling this protocol will prevent access to the Web-based user interface until a terminal session re-enables the Web protocol.	Attempting to disable the Web (HTTP / HTTPS) protocol
Are you sure you want to disable the Secure Shell protocol? Disabling this protocol will prevent access to the Web-based user interface and Secure Shell terminal interface until a terminal session re-enables the Secure Shell protocol.	Attempting to disable the Secure Shell protocol
The SNMP protocol is currently disabled. The new settings will not take effect until this protocol is enabled on the Network Configuration screen.	Changing an SNMP value with the SNMP protocol disabled
The Read Community field is empty. The Read Community will be set to “public”. The SNMP protocol may be disabled on the Network Configuration screen.	Attempting to set a blank Read Community string
Are you sure that you want to power off the enclosure?	Attempting to power off the enclosure
Are you sure that you want to restart the Integrated Administrator? This process will take several minutes.	Attempting to restart the Integrated Administrator
Are you sure that you want to clear the system log?	Attempting to clear the system log
Enabling IP Security may disconnect this session. Are you sure you still want to perform this action?	Attempting to enable IP Security

Blade PC Warning Messages

Table B-2 Blade PC Warning Messages

Warning Message	Cause

Table B-2 Blade PC Warning Messages (continued)

This blade has been removed from the enclosure.	The blade that is being viewed has been removed from the enclosure.
This blade has been powered off. All open sessions will be closed.	The current blade has been powered off.
Are you sure that you want to power off the blade immediately? This process may result in the loss of any unsaved data on the blade.	Attempting to immediately power off a blade.

Administration Warning Messages

Table B-3 Administration Warning Messages

Warning Message	Cause
Are you sure you want to permanently remove <user name>? All data for this account will be removed from the system.	Attempting to delete a user
Are you sure you want to permanently remove <group name>? All bays in this group will be unassigned and the data for this group will be permanently removed from the system.	Attempting to delete a group

Error Messages

Enclosure Error Messages

Table B-4 Enclosure Error Messages

Error Message	Cause	Valid Input
The maximum number (8) of trap destinations has been reached.	Attempting to add a 9th trap destination	N/A
The trap destination of ###.###.###.### is already on the list. Enter a new value.	Attempting to add a duplicate trap destination	N/A
An error occurred while clearing the system log. Please try again.	Attempting to clear the system log	N/A

Blade PC Bay Error Messages

Table B-5 Blade PC Bay Error Messages

Error Message	Cause	Valid Input
You no longer have permissions to view this bay.	User permission change	N/A

Administration Error Messages

Table B-6 Administration Error Messages

Error Message	Cause	Valid Input
The user name field is empty. Please enter a user name.	Attempting to create a user with a blank user name	1-13 characters including alphanumeric, dash, and underscore characters. The user name must begin with a letter.
This user name already exists. Please select a different user name.	Attempting to create a user without a unique user name	1-13 characters including alphanumeric, dash, and underscore characters. The user name must begin with a letter.
The Password fields are empty. Please enter a value in each password field.	Attempting to create a user with a blank password	3-8 characters including all printable characters
The Password field is empty. Please enter a password.	Attempting to create a user with a blank Password field	3-8 characters including all printable characters
The Confirm Password field is empty. Please enter a password.	Attempting to create a user with a blank Confirm Password field	3-8 characters including all printable characters
The password must be at least 3 characters in length. Please enter a new password.	Attempting to create a user with a password that is less than 3 characters long	3-8 characters including all printable characters
The passwords do not match. Please try again.	Different strings in the Password and Confirm Password fields	3-8 characters including all printable characters
The maximum number (25) of users exists on the system.	Attempting to create a 26th user	N/A

Table B-6 Administration Error Messages (continued)

The group name is blank. Please enter a valid name.	Attempting to create a group with a blank group name	N/A
The maximum number (20) of groups exists on the system.	Attempting to create a 21st group	N/A
The Password fields are empty. Please enter a value in each password field.	Attempting to create a user with a blank password	3-8 characters including all printable characters
The Password field is empty. Please enter a password.	Attempting to create a user with a blank Password field	3-8 characters including all printable characters
The Confirm Password field is empty. Please enter a password.	Attempting to create a user with a blank Confirm Password field	3-8 characters including all printable characters
The password must be at least 3 characters in length. Please enter a new password.	Attempting to create a user with a password that is less that 3 characters long	3-8 characters including all printable characters
The passwords do not match. Please try again.	Different strings in the Password and Confirm Password fields	3-8 characters including all printable characters
NTP Poll-Interval has to be between 60 and 9999 seconds.	Attempting to set an NTP poll interval that is not between 60 and 9999 seconds.	60-9999
Invalid NTP address supplied. IP address should be in ###.###.###.### format where ### is between 0 and 255.	Attempting to enter an IP address that is not in the correct format.	###.###.###.### where ### is between 0 and 255
###.###.###.### is not a valid NTP server.	Attempting to set an NTP server address, but the address entered is not an NTP server.	N/A
Please set at least the Primary NTP server before enabling NTP.	Attempting to enable the NTP server before enabling the primary NTP server set.	N/A
<IP address> is already set as secondary NTP server.	Attempting to set the primary NTP server to <IP address> when the <IP address> is already set as secondary.	N/A
<IP address> is already set as primary NTP server.	Attempting to set the secondary NTP server to <IP address> when the <IP address> is already set as primary.	N/A
Primary NTP server is already cleared.	Attempting to clear the primary NTP server that has previously been cleared or never set.	N/A
The secondary NTP server is already cleared.	Attempting to clear the secondary NTP server that has previously been cleared or never set.	N/A
Please set the primary NTP server first.	Attempting to set the secondary NTP server without first setting the primary NTP server.	N/A
Invalid IP address supplied. IP address should be in ###.###.###.### or ###.###.###.###/## format where ### is between 0 and 255 and ## is between 0 and 32.	Attempting to set an IP address that is not in the correct format.	###.###.###.### where ### is between 0 and 255 and ## is between 0 and 32.

Table B-6 Administration Error Messages (continued)

Invalid e-mail address supplied. Address should be in user@domain.tld format.	Attempting to enter an e-mail address that is not in the correct format.	E-mail addresses formatted “user@domain.tld” and containing a maximum of 64 characters.
E-mail address is too long. Length must be less than 65 characters.	Attempting to enter an e-mail address containing more than 64 characters.	E-mail addresses formatted “user@domain.tld” and containing a maximum of 64 characters.

C Troubleshooting

This appendix provides troubleshooting information for the Integrated Administrator that ships as part of the HP PC Blade Enclosure. Use it to find details about solving performance problems that may arise when viewing or managing enclosure, blade PC, or user information using the Integrated Administrator.

For information on LEDS, switches, and troubleshooting information for the HP PC Blade Enclosure, refer to the HP PC Blade Enclosure Setup and Installation Guide.

Table C-1 Integrated Administrator Troubleshooting

Problem	Possible Solution
My Web browser flickers when I view the Integrated Administrator applet.	Be sure the client browser has at least 16-bit color depth.
My Web browser is not supported by the Integrated Administrator.	Be sure to use a supported Web browser. For the most up-to-date information on supported Web browsers, please view the customer advisories located at: www.hp.com/go/cci
I am having general browser problems.	For the most recent tips regarding the Integrated Administrator, refer to the customer advisories on the following Web site: www.hp.com/go/cci
My Web browser seems unstable when I access the Integrated Administrator.	Your Java Virtual Machine (JVM) must be build 3802 or newer. Netscape users are advised to use Netscape 6.2 or later to include this JVM and Internet Explorer users can download the latest JVM from the Microsoft Web site: www.microsoft.com/java/ This update is mandatory for Windows 95 and Windows 98 users and is available in Service Pack 2 for Windows 2000 users.
The Integrated Administrator does not show the most up-to-date blade information. The blade PC information is unknown.	The blade PC configuration information is exchanged with the Integrated Administrator during the blade PC Power-On Self Test (POST). If the Integrated Administrator is restarted after the blade PCs have booted, the Integrated Administrator does not display the blade PC configuration information until the blade PCs are rebooted. Also, the blade PC BIOS obtains part of the information of the blade PC from the health driver; so after installing the health driver, you may need to cycle the blade PC power to enable the Integrated Administrator to see new information.
I just got logged out of the GUI. Why? What should I do?	Your rights may have changed. If so, log in again to use your new rights. If the problem continues, contact the enclosure administrator.
When I ran “upload config,” garbage printed to the screen and then a statement printed saying the command completed successfully.	No error occurred in this command. Everything ran as expected.

Table C-1 Integrated Administrator Troubleshooting (continued)

Did an error occur?	
My fans periodically increase speed and then return to their normal speed.	Fans perform a self-test for 60 seconds every 24 hours.
Although my username and my password are valid, I am unable to log into the Integrated Administrator.	The Integrated Administrator supports up to 48 concurrent sessions. Be sure the number of sessions has not reached this threshold and check with an enclosure administrator to be sure your account is not disabled.
The Event List does not report event repairs.	The Event list only displays negative events that happen during the user's login session. Although repairs are not listed here, the user may highlight the event and click on View/Modify to see the present event status. The user can also view the System Log of the enclosure.

D Event Icons and Details

The Integrated Administrator provides real-time event notifications for an enclosure according to two categories: caution and critical. When an event occurs, the Integrated Administrator notifies the user by generating an icon that the user can click to view more details:

Table D-1 Event Notification Icons

Icon	Description
	Caution—An event that does not prevent the enclosure from operating, maintaining power, or serving its user community When a Caution event occurs, a reasonable guarantee that operability can persist no longer exists.
	Critical—An event that prevents the continued operation of the enclosure When a Critical event occurs, the inoperability of the enclosure is imminent.

The following table provides a comprehensive list of event messages in a format that reflects the display of the Integrated Administrator.

Table D-2 Event Details

Severity	Source	Date	Time	Event Details
	Enclosure	<date>	<time>	The enclosure has experienced a failure.
	Enclosure	<date>	<time>	Fan # has experienced a failure.
	Enclosure	<date>	<time>	Power supply # has experienced a failure.
	Enclosure	<date>	<time>	The enclosure temperature has exceeded the critical threshold.
	Blade in bay #	<date>	<time>	Blade # has experienced a failure.
	Blade in bay #	<date>	<time>	The temperature on blade # has exceeded the critical threshold.
	Enclosure	<date>	<time>	The enclosure is in a degraded state.
	Enclosure	<date>	<time>	Fan # is in a degraded state.
	Enclosure	<date>	<time>	The redundancy of the power supplies is in an unknown state.
	Enclosure	<date>	<time>	The power supplies are no longer redundant.
	Enclosure	<date>	<time>	Power supply # is in a degraded state.

Table D-2 Event Details (continued)

	Enclosure	<date>	<time>	The enclosure temperature has exceeded the caution threshold.
	Blade in bay #	<date>	<time>	Blade # is in a degraded state.
	Blade in bay #	<date>	<time>	The temperature on blade # has exceeded the caution threshold.

E Factory Default Settings

This appendix provides the factory default settings for the following components of the HP PC Blade Enclosure Integrated Administrator.

- Enclosure
- Users
- Groups
- Network
- Protocol

Enclosure

The following table provides the default values in the Integrated Administrator for fields related to the blade PC enclosure.

Table E-1 Default Enclosure Values

Field	Default Value
Name	IA-XXXXXXXXXXXX where XXXXXXXXXXXX is the MAC address of the Integrated Administrator
Rack Name	UnnamedRack
Asset Tag	Blank
Time Zone	CST6CDT

Users

The Integrated Administrator provides the following default users:

- Administrator
- switcha
- switchb

NOTE: The “switcha” and “switchb” accounts are used when accessing the optionally installed interconnect switch console.

Groups

No default groups are in the Integrated Administrator.

Network

The Integrated Administrator ships with the following default values assigned:

Table E-2 Default Enclosure Values

Field	Default Value
DHCP	Enabled
Dynamic DNS	Enabled

Protocol

The following table provides the default values in the Integrated Administrator for fields related to network interface protocols:

Table E-3 Default Network Values

Field	Default Value
HTTP	On
SSH	On
TELNET	On
SNMP	On
SNMP location	(blank)
SNMP contact	(blank)
READ community	Public
WRITE community	(blank)
NTP	Disabled
IP Security	Disabled
AlertMail	Disabled

F Time Zone Settings

This appendix provides a comprehensive list of time zones supported by the HP PC Blade Enclosure Integrated Administrator. These time zones are organized into the following categories:

- Universal
- Africa
- Asia
- Europe
- Oceania
- Polar
- The Americas

Universal

The following table provides the Universal time zone settings supported by the Integrated Administrator.

△ **CAUTION:** For the Integrated Administrator to recognize GMT time zones, the “Etc.” string must precede them.

Table F-1 Universal Time Zone Values

CET	Etc:GMT+5	Etc:GMT-4	HST
CST6CDT	Etc:GMT+6	Etc:GMT-5	MET
EET	Etc:GMT+7	Etc:GMT-6	MST
EST	Etc:GMT+8	Etc:GMT-7	MST7MDT
EST6EDT+1	Etc:GMT+9	Etc:GMT-8	Navajo
Etc:GMT	Etc:GMT+10	Etc:GMT-9	PST8PDT
Etc:GMT0	Etc:GMT+11	Etc:GMT-10	UCT
Etc:GMT+0	Etc:GMT+12	Etc:GMT-11	Universal
Etc:GMT+1	Etc:GMT-0	Etc:GMT-12	UTC
Etc:GMT+2	Etc:GMT-1	Etc:GMT-13	WET
Etc:GMT+3	Etc:GMT-2	Etc:GMT-14	W-SU
Etc:GMT+4	Etc:GMT-3	Greenwich	Zulu

Africa

The following table provides the African time zone settings supported by the Integrated Administrator.

Table F-2 African Time Zone Values

Africa:Abidjan	Africa:Ceuta	Africa:Lagos	Africa:Niamey
Africa:Accra	Africa:Conakry	Africa:Libreville	Africa:Nouakchott
Africa:Addis Ababa	Africa:Dakar	Africa:Lome	Africa:Ouagadougou
Africa:Algiers	Africa:Dar_es_Salaam	Africa:Luanda	Africa:Porto-Novo
Africa:Asmera	Africa:Djibouti	Africa:Lubumbashi	Africa:Sao_Tome
Africa:Bamako	Africa:Douala	Africa:Lusaka	Africa:Timbuktu
Africa:Bangui	Africa:El_Aaiun	Africa:Malabo	Africa:Tripoli
Africa:Banjul	Africa:Freetown	Africa:Maputo	Africa:Tunis
Africa:Bissau	Africa:Gaborone	AfricaMaseru:	Africa:Windhoek
Africa:Blantyre	Africa:Harare	Africa:Mbabane	Egypt
Africa:Brazzaville	Africa:Johannesburg	Africa:Mogadishu	Libya
Africa:Brazzaville	Africa:Kampala	Africa:Monrovia	—
Africa:Cairo	Africa:Kigali	Africa:Nairobi	—
Africa:Casablanca	Africa:Kinshasa	Africa:Ndjamena	

Asia

The following table provides the Asian time zone settings supported by the Integrated Administrator.

Table F-3 Asian Time Zone Values

Asia:Aden	Asia:Dushanbe	Asia:Nicosia	Asia:Tokyo
Asia:Almaty	Asia:Gaza	Asia:Novosibirsk	Asia:Ujung_Pandang
Asia:Amman	Asia:Harbin	Asia:Omsk	Asia:Ulaanbaatar
Asia:Anadyr	Asia:Hong_Kong	Asia:Phnom_Penh	Asia:Ulan_Bator
Asia:Aqtau	Asia:Hovd	Asia:Pyongyang	Asia:Urumqi
Asia:AqtobeAqtobe	Asia:Irkutsk	Asia:Qatar	Asia:Vientiane
Asia:Ashgabat	Asia:Istanbul	Asia:Rangoon	Asia:Vladivostok
Asia:Ashkhabad	Asia:Jakarta	Asia:Riyadh	Asia:Yakutsk
Asia:Baghdad	Asia:Jayapura	Asia:Riyadh87	Asia:Yekaterinburg
Asia:Bahrain	Asia:Jerusalem	Asia:Riyadh88	Asia:Yerevan
Asia:Baku	Asia:Kabul	Asia:Riyadh89	Hongkong
Asia:Bangkok	Asia:Kamchatka	Asia:Saigon	Iran
Asia:Beirut	Asia:Karachi	Asia:Samarkand	Israel

Table F-3 Asian Time Zone Values (continued)

Asia:Bishkek	Asia:Kashgar	Asia:Seoul	Japan
Asia:Brunei	Asia:Katmandu	Asia:Shanghai	Mideast:Riyadh87
Asia:Calcutta	Asia:Krasnoyarsk	Asia:Singapore	Mideast:Riyadh88
Asia:Chungking	Asia:Kuala_Lumpur	Asia:Taipei	Mideast:Riyadh89
Asia:Colombo	Asia:Kuching	Asia:Tashkent	PRC
Asia:Dacca	Asia:Kuwait	AsiaTbilisi:	ROC
Asia:Damascus	Asia:Macao	Asia:Tehran	ROK
Asia:Dhaka	Asia:Magadan	Asia:Tel_Aviv	Singapore
Asia:Dili	Asia:Manila	Asia:Thimbu	Turkey
Asia:Dubai	Asia:Muscat	Asia:Thimphu	

Europe

The following table provides the European time zone settings supported by the Integrated Administrator.

Table F-4 European Time Zone Values

Eire	Europe:Lisbon	Europe:Skopje
Europe:Amsterdam	Europe:Ljubljana	Europe:Sofia
Europe:Andorra	Europe:London	Europe:Stockholm
Europe:Athens	Europe:Luxembourg	Europe:Tallinn
Europe:Belfast	Europe:Madrid	Europe:Tirane
Europe:Belgrade	Europe:Malta	Europe:Tiraspol
Europe:Berlin	Europe:Minsk	Europe:Uzhgorod
Europe:Bratislava	Europe:Monaco	Europe:Vaduz
Europe:Brussels	Europe:Moscow	Europe:Vatican
Europe:Bucharest	Europe:Nicosia	Europe:Vienna
Europe:Budapest	Europe:Oslo	Europe:Vilnius
Europe:Chisinau	Europe:Paris	Europe:Warsaw
Europe:Copenhagen	Europe:Prague	Europe:Zagreb
Europe:Dublin	Europe:Riga	Europe:Zaporozhye
Europe:Gibraltar	Europe:Rome	Europe:Zurich
Europe:Helsinki	Europe:Samara	GB
Europe:Istanbul	Europe:San_Marino	GB-Eire
Europe:Kaliningrad	Europe:Sarejevo	Poland
Europe:Kiev	Europe:Simferopol	Portugal

Oceania

The following table provides the Oceanic time zone settings supported by the Integrated Administrator.

Table F-5 Oceanic Time Zone Values

Atlantic:Azores	Australia:North	Kwajalein
Atlantic:Bermuda	Australia:NSW	NZ
Atlantic:Canary	Australia:Perth	NZ-CHAT
Atlantic:Cape_Verde	Australia:Queensland	Pacific:Apia
Atlantic:Faeroe	Australia:South	Pacific:Auckland
Atlantic:Jan_Mayen	Australia:Sydney	Pacific:Chatham
Atlantic:Madeira	Australia:Tasmania	Pacific:Easter
Atlantic:Reykjavik	Australia:Victoria	Pacific:Efate
Atlantic:South_Georgia	Australia:West	Pacific:Enderbury
Atlantic:St_Helena	Australia:Yancowinna	Pacific:Fakaofo
Atlantic:Stanley	Iceland	Pacific:Fiji
Australia:ACT	Indian:Antananarivo	Pacific:Funafuti
Australia:Adelaide	Indian:Chagos	Pacific:Galapagos
Australia:Brisbane	Indian:Christmas	Pacific:Gambier
Australia:Broken_Hill	Indian:Cocos	Pacific:Guadalcanal
Australia:Canberra	Indian:Comoro	Pacific:Guam
Australia:Darwin	Indian:Kerguelen	Pacific:Honolulu
Australia:Hobart	Indian:Mahe	Pacific:Johnston
Australia:LHI	Indian:Maldives	Pacific:Kiritimati
Australia:Lindeman	Indian:Mauritius	Pacific:Kosrae
Australia:Lord_Howe	Indian:Mayotte	Pacific:Kwajalein
Australia:Melbourne	Indian:Reunion	Pacific:Majuro
Pacific:Marquesas	Pacific:Pitcairn	Pacific:Tongatapu
Pacific:Midway	Pacific:Ponape	Pacific:Truk
Pacific:Nauru	Pacific:Port_Moresby	Pacific:Wake
Pacific:Niue	Pacific:Rarotonga	Pacific:Wallis
Pacific:Norfolk	Pacific:Saipan	Pacific:Yap
Pacific:Noumea	Pacific:Samoa	US:Hawaii
Pacific:Pago_Pago	Pacific:Tahiti	US:Samoa
Pacific:Palau	Pacific:Tarawa	—

Polar

The following table provides the polar time zone settings supported by the Integrated Administrator.

Table F-6 Polar Time Zone Values

Antarctica:Casey	Antarctica:McMurdo	Antarctica:Vostok
Antarctica:Davis	Antarctica:Palmer	Antarctica:Longyearbyen
Antarctica:DumontDUrville	Antarctica:South_Pole	Antarctica:
Antarctica:Mawson	Antarctica:Syowa	

Americas

The following table provides the American time zone settings supported by the Integrated Administrator.

Table F-7 American Time Zone Values

America:Adak	America:Chihuahua	America:Guatemala
America:Anchorage	America:Cordoba	America:Guayaquil
America:Anguilla	America:Costa_Rica	America:Guyana
America:Antigua	America:Cuiaba	AmericaHalifax
America:Araguaina	America:Curacao	America:Havana
America:Aruba	America:Dawson	America:Hermosillo
America:Asuncion	America:Dawson_Creek	America:Indiana:Indianapolis
America:Atka	America:Denver	America:Indiana:Knox
America:Barbados	America:Detroit	America:Indiana:Marengo
America:Belem	America:Dominica	America:Indiana:Vevay
America:Belize	America:Edmonton	America:Indianapolis
America:Boa_Vista	America:Eirunepe	America:Inuvik
America:Bogota	America:El_Salvador	America:Iqaluit
AmericaBoise:	America:Ensenada	America:Jamaica
America:Buenos_Aires	America:Fort_Wayne	America:Jujuy
America:Cambridge_Bay	America:Fortaleza	America:Juneau
America:Cancun	America:Glace_Bay	America:Kentucky:Louisville
America:Caracas	America:Godthab	America:Kentucky:Monticello
America:Catamarca	America:Goose_Bay	America:Knox_IN
America:Cayenne	America:Grand_Turk	America:La_Paz
America:Chicago	America:Guadeloupe	America:Los_Angeles
America:Louisville	America:Rainy_River	Brazil:DeNoronha
America:Maceio	America:Rankin_Inlet	Brazil:East

Table F-7 American Time Zone Values (continued)

America:Managua	America:Recife	Canada:Central
America:Manaus	America:Regina	Canada:Eastern
America:Martinique	America:Rio_Branco	Canada:East-Saskatchewan
America:Mazatlan	America:Rosario	Canada:Mountain
America:Mendoza	America:Santiago	Canada:Newfoundland
America:Menominee	America:Santo_Domingo	Canada:Pacific
America:Merida	America:Sao_Paulo	Canada:Saskatchewan
America:Mexico_City	America:Scoresbysund	Canada:Yukon
America:Miquelon	America:Shiprock	Chile:Continental
America:Monterrey	America:St_Johns	Chile:EasterIsland
America:Montevideo	America:St_Kitts	Cuba
America:Montreal	America:St_Lucia	Jamaica
America:Montserrat	America:St_Thomas	Mexico:BajaNorte
America:Nassau	America:St_Vincent	Mexico:BajaSur
America:New_York	America:Swift_Current	Mexico:General
America:Nipigon	America:Tegucigalpa	US:Alaska
America:Nome	America:Thule	US:Aleutian
America:Noronha	America:Thunder_Bay	US:Arizona
America:Panama	America:Tijuana	US:Central
America:Pangnirtung	America:Tortola	US:Eastern
America:Paramaribo	America:Vancouver	US:East-Indiana
America:Phoenix	America:Virgin	US:Indiana-Starke
America:Port_of_Spain	America:Whitehorse	US:Michigan
America:Prince	America:Winnipeg	US:Mountain
America:Porto_Acre	America:Yakutat	US:Pacific
America:Porto_Velho	America:Yellowknife	-
America:Puerto_Rico	Brazil:Acre	-

G Open Source Availability

The Integrated Administrator is based on embedded Linux and contains numerous Open Source components. In compliance with Open Source licensing, HP has made the source code of all Open Source components used available at the following URL:

opensource.hp.com

To locate the Integrated Administrator project, consult the list of all projects.

Index