HP Integrity iLO 2 Operations Guide

HP Part Number: 5992-1085
Published: November 2012
Edition: 14

Legal Notices

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel, Pentium, Intel Inside, Itanium, and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Acrobat is a trademark of Adobe Systems Incorporated.

Java is a US trademark of Sun Microsystems, Inc.

UNIX is a registered trademark of The Open Group.

Contents

About This Document

This document provides information and instructions on how to use the HP Integrated Lights-Out 2 (iLO 2) for HP Integrity for BL870c, BL860c, rx2660, rx3600, and rx6600 servers.

The document date and part number indicate the document's current edition. The date changes when a new edition is published. The document part number changes when extensive changes are made.

Document updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, subscribe to the appropriate product support service. See your HP sales representative for details.

This document is also a reference for the following HP Integrity servers with Integrity iLO 2:

- rx7640
- rx8640
- Superdome sx2000

The latest version of this document can be found on the HP website at http://www.hp.com.

Intended Audience

This document provides technical product and support information for authorized service providers, system administrators, and HP support personnel.

Publishing History

The publishing history below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, *as needed*, basis.

Table 1 Publishing History Details

Document Manufacturing Part Number	Operating Systems Supported	Supported Servers	Publication Date
5971-4292	HP-UX 11i v2 OpenVMS 8.3 Microsoft Windows Server 2003 Red Hat Linux and SuSE	rx3600 rx6600	September 2006
AB419-9006A	HP-UX 11i v2 OpenVMS 8.3 Microsoft Windows Server 2003 Red Hat Linux and SuSE	rx2660 rx3600 rx6600	December 2006
AD217-9001A	HP-UX 11i v2 OpenVMS 8.3 Microsoft Windows Server 2003 Red Hat Linux and SuSE	BL860c rx2660 rx3600 rx6600	February 2007
5991-5983	HP-UX 11i v2 OpenVMS 8.3 Microsoft Windows Server 2003 Red Hat Linux and SuSE	BL860c rx2660 rx3600 rx6600	June 2007
5991-5992	HP-UX 11i v2	BL860c	November 2007

Table 1 Publishing History Details *(continued)*

Document Manufacturing Part Number	Operating Systems Supported	Supported Servers	Publication Date
	OpenVMS 8.3 1H1 Microsoft Windows Server 2003 Red Hat Linux and SuSE	rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	
5991-6005	HP-UX 11i v2 OpenVMS 8.3 1H1 Microsoft Windows Server 2003 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	January 2008
5991-6024	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	August 2008
5991-8053	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	May 2009
5991-8053_ed9	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	August 2009
5991-8053_ed10	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600	December 2009

Table 1 Publishing History Details *(continued)*

Document Manufacturing Part Number	Operating Systems Supported	Supported Servers	Publication Date
		rx6600 rx7640* rx8640* Superdome sx2000*	
5991-8053_ed11	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	April 2010
5991-8053_ed12	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	May 2010
5991-8128	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	January 2011
5992-1085	HP-UX 11i v3 OpenVMS 8.3 1H1 Microsoft Windows Server 2008 Red Hat Linux and SuSE	BL870c BL860c rx2660 rx3600 rx6600 rx7640* rx8640* Superdome sx2000*	November 2012

* All of the iLO 2 functionality is not currently available on this server.

Document Organization

This document is divided into the following chapters.

Chapter 1 *Introduction* Use this chapter to learn about iLO 2 functionality.

Chapter 2 *Ports and LEDs* Use this chapter to learn about ports and LEDs.

Chapter 3 *Getting Connected to iLO 2* Use this chapter to connect to iLO 2.

Chapter 4 *Logging in to iLO 2* Use this chapter to log in to iLO 2.

Chapter 5 *Adding Advanced Features* Use this chapter to learn about the HP Lights-Out Advanced KVM card functionality and installation on the rx7640, rx8640, and Superdome sx2000 servers.

Chapter 6 *Accessing the Host Console* Use this chapter to learn how to access the host console of an HP Integrity server through iLO 2.

Chapter 7 *Configuring DHCP, DNS, LDAP, and Schema-Free LDAP* Use this chapter to configure DHCP, DNS, LDAP extended schema, and Schema-Free LDAP.

Chapter 8 *Using iLO 2* This chapter provides information on the different interfaces you can use to interact with iLO 2 such as text user interface, web GUI, and SMASH SM CLP.

Chapter 9 *Installing and Configuring Directory Services* Use this chapter to learn about installing and configuring directory services functions.

Glossary Use the glossary to learn iLO 2 terms and definitions.

Typographic Conventions

This document uses the following typographical conventions:

%, $, or # A percent sign represents the C shell system prompt. A dollar sign represents the system prompt for the Bourne, Korn, and POSIX shells. A number sign represents the superuser prompt.

`Command` A command name or qualified command phrase.

`Computer output` Text displayed by the computer.

Ctrl+x A key sequence. A sequence such as **Ctrl+x** indicates that you must hold down the key labeled **Ctrl** while you press another key or mouse button.

`ENVIRONMENT VARIABLE` The name of an environment variable, for example, `PATH`.

ERROR NAME The name of an error, usually returned in the `errno` variable.

Key The name of a keyboard key. **Return** and **Enter** both refer to the same key.

Term The defined use of an important word or phrase.

`User input` Commands and other text that you type.

`Variable` The name of a placeholder in a command, function, or other syntax display that you replace with an actual value.

[] The contents are optional in syntax. If the contents are a list separated by |, you must choose one of the items.

{} The contents are required in syntax. If the contents are a list separated by |, you must choose one of the items.

... The preceding element can be repeated an arbitrary number of times.

Three vertical periods Indicates the continuation of a code example.

| Separates items in a list of choices.

WARNING A warning calls attention to important information that if not understood or followed will result in personal injury or nonrecoverable system problems.

CAUTION	A caution calls attention to important information that if not understood or followed will result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task
NOTE	A note contains additional information to emphasize or supplement important points of the main text.

Related Information

You can find other information on HP server hardware management, Microsoft® Windows®, and diagnostic support tools in the following publications.

HP Technical Documentation Website

http://www.hp.com/go/Integrity_Servers-docs for HP Integrity servers

http://www.hp.com/go/Blades-docs for HP Integrity server blades

Windows Operating System Information

Find information about administration of the Microsoft Windows operating system on the following website:

http://www.microsoft.com/technet/

Diagnostics and Event Monitoring: Hardware Support Tools

Complete information about HP hardware support tools, including online and offline diagnostics and event monitoring tools, is on the HP website at:

http://www.hp.com/go/hpux-diagnostics-docs

Website for HP Technical Support

http://www.hp.com/hpsc/

Books About HP-UX Published by Prentice Hall

You can find the entire Prentice Hall Professional Series on HP at:

http://www.informit.com/imprint/series_detail.aspx?st=61305

HP Contact Information

For the name of the nearest HP authorized reseller:

- In the United States, see the HP US service locator webpage (http://welcome.hp.com/country/us/en/wwcontact.html.)
- In other locations, see the Contact HP worldwide (in English) webpage:

  http://welcome.hp.com/country/us/en/wwcontact.html.

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage: (http://welcome.hp.com/country/us/en/contact_us.html)

  To contact HP by phone:

  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, see the HP website at: (http://www.hp.com/go/carepack).
- In other locations, see the Contact HP worldwide (in English) webpage (http://welcome.hp.com/country/us/en/wwcontact.html).

Documentation Feedback

HP welcomes your feedback. To make comments and suggestions about product documentation, send a message to **docsfeedback@hp.com**.

Include the document title and manufacturing part number. All submissions become the property of HP.

1 Introduction to iLO 2

The Integrated Lights-Out Management Processor (iLO MP) for Integrity servers is an autonomous management subsystem embedded directly on the server. It is the foundation of the server's High Availability (HA) embedded server and fault management. It also provides system administrators secure remote management capabilities regardless of server status or location. iLO is available whenever the system is connected to a power source, even if the server main power switch is in the off position.

HP has used several different names to describe the management functionality embedded in servers, including "the management processor." In addition, HP uses the term "management processor" to refer to any embedded microprocessor that manages a system. Management processor is a descriptive term (such as "server"), and iLO is a brand name or label (such as "Integrity").

Remote access is the key to maximizing efficiency of administration and troubleshooting for enterprise servers. Integrity servers are designed so all administrative functions that can be performed locally, can also be performed remotely. iLO enables remote access to the operating system console, control over the server's power and hardware reset functionality, and works with the server to enable remote network booting through a variety of methods.

The iLO 2 is an Integrated Lights-Out 2 management processor with the latest advanced digital video redirection technology. This new feature gives you a higher performance graphics console redirection experience than with the previous iLO.

This documentation addresses HP Integrated Lights-Out 2 (iLO 2) for Integrity servers and server blades. For information on iLO for ProLiant servers and ProLiant BladeSystem server blades, see www.hp.com/go/iLO.

NOTE: Previously, this document used the name iLO 2 MP as a reference to a management processor. For the remainder of this document, we will simply refer to it as iLO 2 unless when referring to physical components such as MP ports, connectors, LEDs, and so on.

IMPORTANT: This guide addresses server-specific details that vary between server products. These details are frequently updated. For the latest server-specific product information, see the Integrity iLO 2 Quick Specs on the HP website at www.hp.com/go/integrityilo.

Features

Integrity iLO 2 functionality includes the following:

- Monitoring of server health and status
- Control of power, reset, and Transfer of Control (TOC) capabilities
- Console access
- Display and recording of system events
- Display of detailed information about the various internal subsystems and field replaceable units (FRUs)
- A virtual front panel to monitor system status and see the state of front panel LEDs

Integrity iLO 2 is completely independent of the host system and the operating system. It has its own microprocessor and runs its own firmware. The operating system cannot send packets out on the MP LAN, and packets on the MP LAN cannot go to the operating system. The MP LAN is exclusive to iLO 2 and is driven by an embedded realtime operating system (RTOS) running on iLO 2.

NOTE: The following ProLiant iLO 2 features are not available on Integrity iLO 2:

- Virtual Folder
- Shared LAN
- Graphics Console Replay

Integrity iLO 2 offers the following standard and advanced features.

Standard Features

Integrity iLO 2 standard features provide the following basic system board management functions, diagnostics, and essential Lights-Out functionality on iLO 2-supported HP servers.

Always-On Capability

Integrity iLO 2 is active and available through the MP LAN connection and the local serial port connection as long as the power cord is plugged in. In the event of a complete power failure, iLO 2 data is protected by an onboard battery backup.

Virtual Front Panel

The virtual front panel (VFP) presents a summary of the system front panel using direct console addressing.

Multiple Access Methods

The available methods to access iLO 2 are as follows:

IPMI/LAN	Through the iLO 2 MP MAC address
LAN	Using Telnet, web, or SSH to access the iLO 2 MP LAN
Local Serial Port	Using a terminal or laptop computer for direct connection
Web	Using a GUI

Security

Integrity iLO 2 provides security for remote management in IT environments, such as the following:

- User-defined TCP/IP ports
- User accounts and access management
- Lightweight Directory Access Protocol- (LDAP) based directory services authentication and authorization
- Encrypted communication using SSL and SSH

User Access Control

Integrity iLO 2 is restricted by user accounts. User accounts are password protected and are assigned access rights that define a specific level of access to the server and to the iLO 2 MP commands. iLO 2 supports both LDAP directory user authentication and locally stored iLO 2 user accounts. iLO 2 users can have any of the following access rights:

Console Access	Right to access the system console (the host operating system). This does not bypass host authentication requirements, if any.
Power Control Access	Right to power on, power off, or reset the server, and the right to configure the power restore policy.
Local User Administration Access	Right to configure locally stored user accounts.
MP Configuration Access	Right to configure all iLO 2 MP settings and some system settings, such as the power restore policy.

Virtual Media Access	Enables Advanced Pack license users the right to use the virtual media applet.

Multiple Users

Multiple users can interact with iLO 2. However, iLO 2 command mode and console mode are mirrored, allowing only one user at a time to have write access to the shared console. When a command is completed, write access is released and any user can initiate another command.

IMPORTANT: Although iLO 2 can support multiple simultaneous connections, to do so can impact performance. HP does not recommend running more than eight simultaneous connections.

Integrity iLO 2 supports the following connections simultaneously:

- Four web (each web connection can have a remote serial console connection as well and not be counted as part of the total number of connections allowed)
- Eight SSH
- One local console serial port (RS-232)
- Four IPMI over LAN
- Four Telnet
- One Integrated Remote Console
- One vMedia

IPMI over LAN

The Intelligent Platform Management Interface (IPMI) option provides direct access from the MP LAN port to the server Baseboard Management Controller (BMC) monitoring and controlling functions such as temperature, voltage, fans, and power supplies. IPMI defines a common interface for platform management hardware. With IPMI over LAN enabled, BMC functions are available to other management software applications. This enables you to write your own customizable management applications using IPMI v1.0. iLO 2 supports up to four simultaneous IPMI over LAN connections.

Currently, there is no capability to manage the IPMI user name or password in the iLO 2 command line or web interfaces. There is only the ability to enable or disable access with IPMI through the SA command.

To set a user name or password using the IPMI over LAN interface, you can use an IPMI tool. HP does not recommend any particular IPMI tools.

IMPORTANT: IPMI traffic is unencrypted, just like Telnet traffic is unencrypted. Also, at initial enablement, there is no password, and the IPMI over LAN port is insecure.

HP recommends that iLO 2 management traffic be on a separate dedicated management network and that only administrators be granted access to that network. Also, set firewalls or routers to accept only specific source and destination addresses. For example, you can allow inbound IPMI traffic into the host server only if it comes from one of the predetermined management workstations.

For more information on IPMI, see the Intel website at:

http://developer.intel.com/design/servers/ipmi

System Management Homepage

The HP Insight Management Agents support a web interface for access to runtime management data through the HP System Management Homepage. The HP System Management Homepage is a secure web-based interface that consolidates and simplifies the management of individual servers and operating systems. By aggregating data from HP Insight Management Agents and other management tools, the System Management Homepage provides an intuitive interface to review in-depth hardware configuration and status data, performance metrics, system thresholds, and software version control information.

Firmware Upgrades

Firmware upgrades enhance the functionality of iLO 2.

The MP firmware is packaged along with system, BMC, and FPGA/PSOC firmware. You can download and upgrade the firmware package from the HP website at http://www.hp.com/go/bizsupport.

Select **Download drivers and software**, select your server, and follow the instructions provided.

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

Internal Subsystem Information

Integrity iLO 2 displays information about the following internal subsystems:

- FRU information
- System power state and fan status
- Processor Status

DHCP and DNS Support

Integrity iLO 2 supports the Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS) configuration options for acquiring network information through the MP LAN port. When iLO 2 starts, it acquires the port configuration stored on a DHCP server to assign an IP address to the MP LAN port. If DNS is configured, this information is updated on the DNS server. The simplest method to initially connect to iLO 2 is with the default DNS name found on the iLO Network Information Tag on the server, for example, `mp0014c29c064f`.

Group Actions

Integrity iLO 2 integrates with HP SIM, HP OpenView, and third-party management tools.

Group Actions Using HP SIM

HP Systems Insight Manager (HP SIM) is a system-level management tool that supports executing commands from HP SIM using the SSH interface. HP SIM enables you to perform similar management activities across multiple iLO 2s (group actions) without requiring you to access each iLO 2 individually. Group actions are launched from the HP SIM GUI and are supported at all times, regardless of the server power state.

You can download HP SIM from the HP website. For more information about HP SIM, see the HP website at http://www.hp.com/go/hpsim.

For the user guide, see the Information Library.

SNMP

The SNMP is part of the TCP/IP protocol suit developed to manage servers on an IP network. SNMP enables you to manage network performance, find and solve network problems, and plan for network growth.

SMASH

Server Management Architecture for Server Hardware (SMASH) is an initiative by the Distributed Management Task Force (DMTF) that encompasses specifications (Server Management CLP, SM ME Addressing, SM Profiles) that address the interoperable manageability requirements of small to large scale heterogeneous computer environments.

SM CLP

The SM CLP specification defines a user friendly command-line protocol that provides command line interface (CLI) standards for interoperability.

Mirrored Console

The system console output stream is reflected to all connected console users, and any user can provide input.

Remote Power Control

Integrity iLO 2 enables remote power cycle, power on and power off, and TOC. It also provides options to reset the system, the BMC, or iLO 2.

Power Regulation

Although the 24-hour graph function of power regulation feature requires the iLO 2 Advanced Pack, you can obtain some power regulation information without the license:

- For both server blades and entry-rack servers, use the `SS` command from the MP CLI interface for an instantaneous power reading.
- For server blades, use the web GUI Server Status page to obtain current power usage and ambient temperature.

Event Logging

Integrity iLO 2 provides event logging, display, and keyword search of console history and system events.

Advanced Features

Integrity iLO 2 advanced features provide additional functionality such as the graphical integrated remote console and virtual media. In addition, the advanced features increase security by integrating iLO 2 user administration with the Active Directory or eDirectory.

iLO advanced features are enabled on Integrity servers in one of two ways. For Integrity entry class and blades, the advanced features are enabled with a license key. For Integrity cell-based servers, the advanced features are enabled with a PCI-X accessory card instead of a key.

IMPORTANT: On HP Integrity server blades, the Advanced Pack license is standard. Remember to save the Advanced Pack license key information that was provided by HP. If you ever need to replace your server blade under warranty, you will need to transfer the key by entering the code on the replacement server blade.

NOTE: A HP ProLiant iLO 2 Advanced Pack license key will not work on an HP Integrity server, and vice versa.

NOTE: Not all advanced features are supported on all systems. For the most current information on accessories, features, and supported products, see the HP website at http://www.hp.com/go/integrityilo and look for the Quick Specs.

Integrity iLO 2 advanced features include the iLO 2 standard features and the following features:

Virtual Media

Virtual Media (vMedia) enables connections of a CD/DVD physical device or image file from the local client system to the remote server. The virtual device or image file can be used to boot the server with an operating system that supports USB devices.

Virtual Media depends on a reliable network with good bandwidth. This is especially important when you are performing tasks such as large file transfers or OS installs.

NOTE: iLO vMedia is automatically disconnected if the iLO management processor is reset. HP does not recommend use of iLO vMedia with firmware update tools such as HPOFM which reset the management processor mid-way through the update process.

Integrated Remote Console

The Integrated Remote Console (IRC) provides a high-performance graphical remote console to HP Integrity-based Windows servers. IRC supports Windows clients running the Internet Explorer browser. IRC requires that the server have VGA. VGA is optional for some Integrity servers. VGA is included on the Lights-Out Advanced KVM card.

Directory-Based Secure Authorization Using LDAP

The directory-based authentication and authorization option enables iLO 2 user accounts to be defined in a centralized database on an LDAP server. iLO 2 users are authenticated when logging in to iLO 2 and authorization is given each time an iLO 2 command runs. This provides a centralized database (LDAP server) of all user accounts and avoids the overhead of creating users in each iLO 2.

Directory authentication occurs by enabling Extended Schema or Default Schema. When Extended Schema is used, the schema in the directory server must be extended. When Default Schema is selected, schema extension is not needed.

Schema-Free LDAP

Schema-Free LDAP enables you to use directory authentication to log in to iLO 2 without having to do any schema extension on the directory server or snap-in installation on the client. In addition to general directory integration benefits, iLO 2 schema-free integration provides the following:

- Minimal maintenance and administration
- Reliable security
- Complements two-factor authentication

Not extending the schema on the directory server means the directory server does not know anything about the iLO 2 object or privileges, and the only thing the iLO 2 queries from the directory server is to authenticate the user name and password.

Power Meter Readings

The power meter readings feature enables you to graphically view and monitor server power usage, temperature, and power regulator settings.

The Advanced Pack license enables you to see the Power Regulator graphs from the iLO 2 web GUI. The license key also enables iLO 2 to share information with Insight Power Manager.

NOTE: You can obtain an instant power reading without a license key through the CLI using the PS command.

HP Insight Power Manager

HP Insight Power Manager (HP IPM), a plug-in to HP Systems Insight Manager (HP SIM), is an integrated power monitoring and management application that provides centralized control of server power consumption and thermal output.

Leveraging HP power regulator technology, HP IPM makes policy-based power and thermal management possible by enabling you to view and modify the power efficiency regulator mode of the system. It expands the capacity of data centers by reducing the amount of power and cooling required for supported Integrity servers and the server blades.

Information on HP IPM is available on the HP website at http://www.hp.com/go/ipm.

Obtaining and Activating iLO 2 Advanced Pack Licensing

For Integrity entry class systems, an Integrity iLO 2 Advanced Pack license key can be purchased from your HP sales rep. To find the part number for the option for your system, see the HP website at http:/www.hp.com/go/integrityiLO. A free 30-day evaluation license is available for download on the HP website. The evaluation license activates and accesses iLO 2 Advanced Pack features. You can only install one evaluation license per iLO 2. After the evaluation period, an iLO 2 Advanced Pack license is required to continue using the advanced features. The iLO 2 Advanced Pack license features automatically deactivate when the evaluation license key expires.

Systems that do not have VGA support all other iLO 2 Advanced Pack license features.

For more information, see the HP website at http://h71028.www7.hp.com/enterprise/cache/279991-0-0-0-121.html.

Follow the factory-install or manual install instructions located on the *Integrated Lights-Out Advanced Pack for HP Integrity Servers; Certificate of License to Use; License Installation Card* to activate your license.

Lights-Out Advanced KVM Card

The HP Lights-Out Advanced KVM card is a PCI-X card that you install into a partition in any sx2000-based mid-range or high-end HP Integrity server such as rx7640, rx8640, and Superdome sx2000.

The Lights-Out Advanced KVM card extends the basic iLO 2 features built into your server by adding virtual media and integrated remote console features to an individual partition. You must add a card for each partition where vMedia or IRC is desired.

The Lights-Out Advanced KVM card is also a KVM card that offers physical video functionality for servers running Windows, and USB functionality for servers running HP-UX, Windows, and OpenVMS.

All Lights-Out Advanced features are fully enabled on the Lights-Out Advanced KVM card. There is no additional advanced pack license to purchase. At present, the IRC is only available for servers running Windows, and vMedia is available for servers running HP-UX, Windows, and OpenVMS.

Supported Systems and Required Components and Cables

Table 2 lists the systems on which iLO 2 is supported and the components and cables that are required to operate iLO 2.

Table 2 Supported Systems and Required Components Matrix

Supported Systems	Required Components	Required Cables[1]
BL860c	Front console serial port (RS-232)	SUV or DB-9 cable
	Rear OA/iLO network port	LAN cable
rx2660	iLO 2 hardware is integrated into the system board	LAN, serial, and VGA cables
rx3600, rx6600	Core I/O board without VGA; factory installed	LAN and serial cables
	Core I/O board with VGA (optional) (This is only supported on Windows Server OS.)	LAN, serial, and VGA cables
rx7640, rx8640, Superdome sx2000	iLO 2 hardware is integrated in the main system. Lights-Out Advanced KVM cards can be added per partition.	LAN, serial, and VGA cables

[1] Cables are not provided with the server.

Integrity iLO 2 Supported Browsers and Client Operating Systems

Integrity iLO 2's web GUI standard features are supported with Microsoft Internet Explorer 6.0 SP1 or Internet Explorer 7, Mozilla Firefox 2.0.0.10.02 or Firefox 3, and HP Secure Web Browser 1.7-13. iLO 2's advanced feature of Integrated Remote Console, a graphical remote console, is supported only with Internet Explorer browsers and requires DirectX control. All browsers support the iLO 2 Remote Serial Console and vMedia applets using the 32-bit Java Plug-in 1.6.0_01.

You can view the most current list of supported browsers and operating systems in the Quickspecs on the HP website at http://www.hp.com/go/integrityilo.

Related Links

- Java™ for HP-UX
  - http://www.hp.com/products1/unix/java/versions/index.html
  - http://www.hp.com/products1/unix/java/archives/index.html
- Java for OpenVMS
  - http://h18012.www1.hp.com/java/alpha
- Firefox for HP-UX
  - http://www.hp.com/products1/unix/java/firefox/index.html

    Note: 1.5.0.00 needs patch
  - http://www.hp.com/go/firefox
- Firefox for Linux®
  - http://linuxcoe.corp.hp.com
- Firefox for Windows and Linux
  - http://www.mozilla.com/firefox
- Browser Support 1.5.0
  - http://java.sun.com/j2se/1.5.0/system-configurations.html

Security

You must have strong security surrounding the iLO 2 device. HP security requirements for iLO 2 include the following:

Authentication
Integrity iLO 2 incorporates authentication techniques with the use of 128-bit Secure Socket Layer (SSL) encryption. It is password based for web and password- and key-based for secure shell (SSH).

Authorization
Using local accounts, iLO 2 enables you to define up to 19 separate users and to vary the server access rights of each user. The directory services capabilities of iLO 2 enables you to maintain network user accounts and security policies in a central, scalable database that supports thousands of users, devices, and management roles.

Integrity
Integrity iLO 2 incorporates a trusted Java applet for vMedia.

Privacy
Integrity iLO 2 uses SSL for web connections, RSL-RC4 encryption for IRC and remote serial console, and 3DES-CBC/AES128-CBD recommended encryption algorithms for SSH-based connections. You can enable or disable Telnet, IPMI over LAN, web, and SSH connectivity.

Login	After initial failed login attempts (default three), a delay of approximately one second is imposed on the serial connection and the login banner warnings are repeated. All other connection types are disconnected.

IMPORTANT: Ensure that physical access to the server is limited. Anyone can clear passwords by pressing the iLO MP reset button for longer than four seconds.

NOTE: For greater security, HP recommends that iLO 2 management traffic be on a separate dedicated management network that is configured to only allow limited access from selected secure systems by designated system administrators. This acts as the first line of defense against security attacks. A separate network enables you to physically and logically control which systems are allowed to connect to the network and the iLO 2 LAN port.

Protecting SNMP Traffic

Because SNMP uses passwords, known as community strings, that are sent across the network in clear text, you must enhance the network security when using SNMP traffic. To enhance network security, do the following:

- Reset the community strings (read only) with the same frequency and according to the same guidelines as the administrative passwords. For example, select alphanumeric strings with at least one uppercase letter, one numeral, and one symbol.
- Set firewalls or routers to accept only specific source and destination addresses. For example, you can allow inbound SNMP traffic into the host server only if it comes from one of the predetermined management workstations.

TIP: Telnet sends data without encryption and is not a secure connection. HP recommends using SSH instead of Telnet because SSH uses encryption.

To enable and disable Telnet access, use the SA command.

2 Ports and LEDs

All iLO 2 functions are available through the server MP LAN port and the local and remote serial ports. On HP Integrity server blades, all iLO 2 functions are available on the Onboard Administrator (OA). This chapter describes the available iLO 2 ports, connectors, and LEDs on the HP Integrity server blades, and the rx2660, rx3600, and rx6600 servers.

HP Integrity Server Blade Components

Onboard Administrator (OA) is the enclosure management processor, subsystem, and firmware base used to support the HP Integrity server blades and all the managed devices contained within the enclosure. The OA provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Using this hard-wired knowledge, the OA performs initial configuration steps for the enclosure, enables runtime management and configuration of the enclosure components, and informs you of problems within the enclosure through email, SNMP, or the Insight Display.

Before setting up the HP BladeSystem OA, HP recommends that you read the *HP BladeSystem Onboard Administrator User Guide* on the HP website at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00705292/c00705292.pdf

Reading this guide ensures that you understand the HP BladeSystem OA and that you properly complete the initial setup to facilitate its proper functioning.

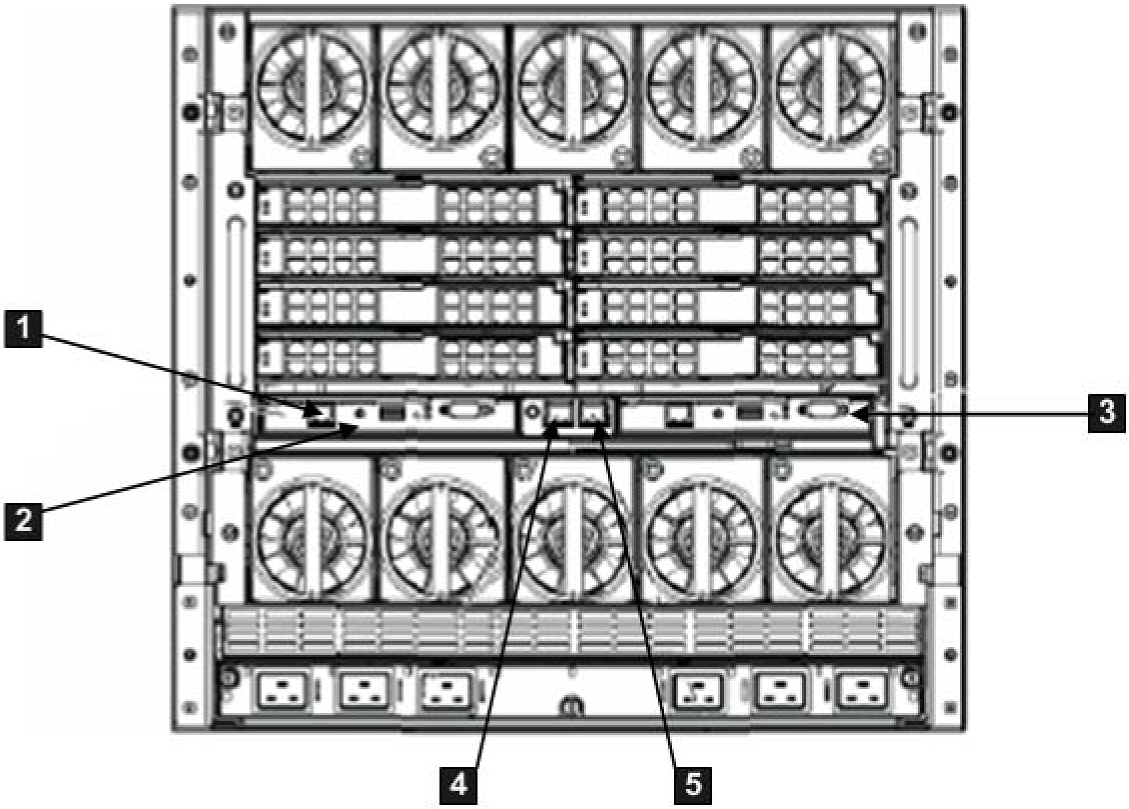
You can find other OA docs on the HP website at:

HP BladeSystem c-Class Onboard Administrator

Onboard Administrator

Figure 1 shows the OA/iLO network port and components.

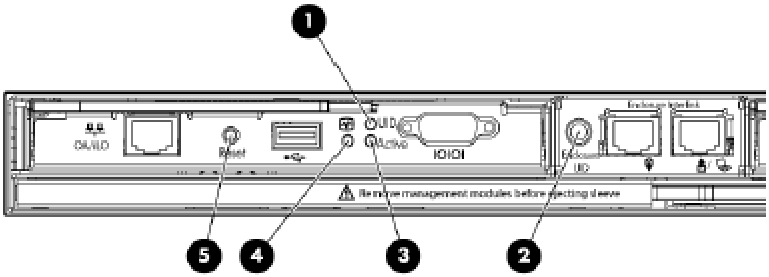
Figure 1 OA/iLO Network Port and Components



1 OA/iLO Network Port
2 OA Bay 1
3 OA Bay 2 (redundant if used)
4 Enclosure Link-Up Port
5 Enclosure Link-Down Port

Figure 2 shows the OA LEDs and buttons.

Figure 2 Onboard Administrator LEDs and Buttons



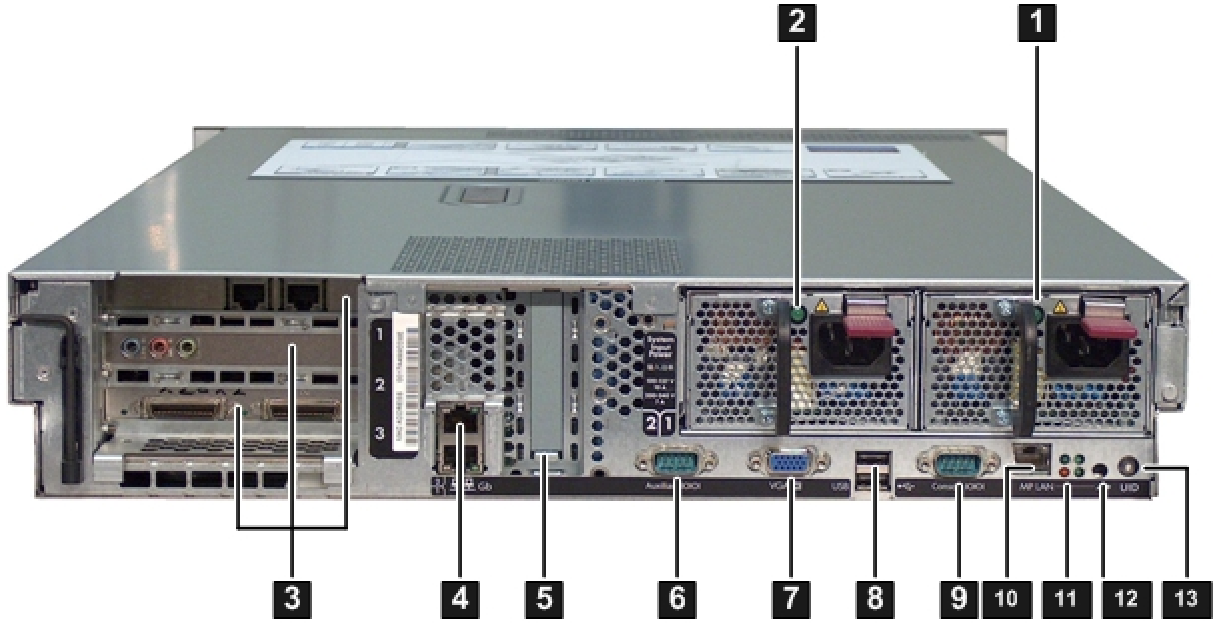
1 OA UID LED
2 Enclosure UID LED
3 OA Active LED
4 OA Health LED
5 OA Reset Button

HP Integrity rx2660 Server Components

Figure 3 shows the rear view of the HP Integrity rx2660 server.

The system LAN functionality is integrated into the system board.

Figure 3 HP Integrity rx2660 Server Rear View



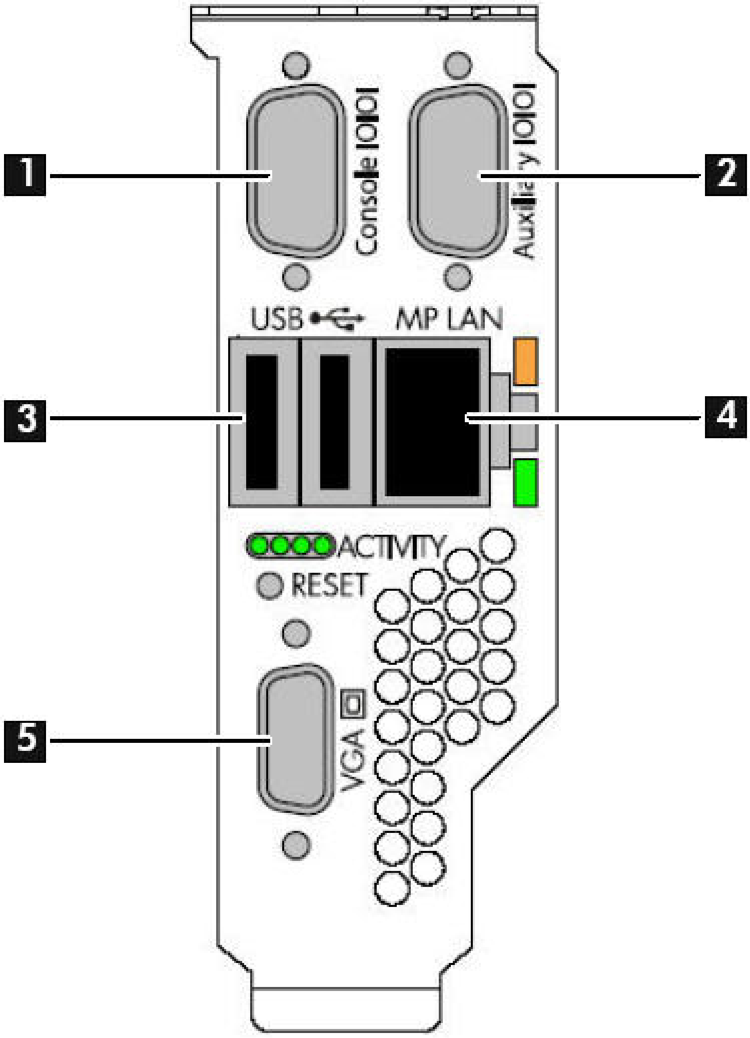
1 Power Supply 1 and LED
2 Power Supply 2 and LED
3 PCI-x/PCIe Slots
4 Core LAN Ports
5 Smart Array P400 Controller Slot
6 Auxiliary Serial Port
7 VGA Port
8 USB Ports
9 Console Serial Port (RS-232)
10 MP LAN Port
11 iLO 2 MP Status LEDs
12 iLO 2 MP Reset Button
13 UID Button/LED

HP Integrity rx3600 and rx6600 Server Components

Figure 4 shows the controls, ports, and LEDs on the rear of the HP Integrity rx3600 and rx6600 servers.

NOTE: This figure is oriented vertically to match the orientation of the core I/O board.

Figure 4 HP Integrity rx3600 and rx6600 Server Rear Ports and LEDs



1 iLO 2 MP Serial Console Port (RS-232) (DB-9F to DB-9F cable) connected to emulation terminal device (PC, laptop, or ASCII terminal)

2 General Use Serial Port (Printers, etc.)

3 USB 2.0 Ports (any USB device)

4 MP LAN Port (10/100 LAN)

5 VGA Port (No iLO 2 access; EFI only)

iLO 2 MP Status LEDs

Table 3 lists the state of the iLO 2 MP status LEDs during normal operation.

Table 3 iLO 2 MP Status LEDs

iLO 2 MP Status LED	LED State
Standby Power	Solid green.
iLO 2 MP Self Test	Off. The LED is solid amber when AC power is first applied. It remains solid amber for a few seconds until the MP completes its self test; then the LED turns off.
iLO 2 MP Heartbeat	Flashing green.
BMC Heartbeat	Flashing green.

iLO 2 MP Reset Button

The iLO 2 MP Reset button enables you to reset iLO 2 and reset the user-specific values to factory default values. A momentary press causes a soft reset of iLO 2 when the button is released. A greater than four second press causes a soft reset of iLO 2 upon release and resets local user accounts and passwords to factory default values.

Resetting Local User Accounts and Passwords to Default Values

If iLO 2 user passwords are lost, or iLO 2 local user accounts are disabled and logging in through LDAP directory server is unsuccessful because the directory server is down or directory settings have not been configured properly in LDAP command, you can reset local user accounts and passwords to their default values.

To reset local user accounts and passwords to default values:

1. Connect a serial terminal (or serial-cabled laptop with serial emulation) to the console serial port.
2. Press and hold the iLO 2 MP Reset button for more than four seconds. iLO 2 reboots to factory default settings automatically.
3. Respond to the prompt to reset local user accounts and passwords to default values.

Console Serial Port and Auxiliary Serial Port

Figure 5 shows the console serial port connector with numbered labels for each pin on each port.

Figure 5 Console Serial Port (RS-232) Connector

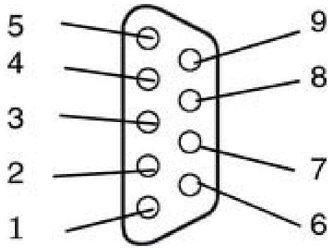


Table 4 maps the console serial port connector pin number to its signal description on each port.

Table 4 Console Serial Port Pinouts

Pin Number	Signal Description
1	Not used
2	Receives data
3	Transmits data
4	Not used
5	Ground

Table 4 Console Serial Port Pinouts *(continued)*

Pin Number	Signal Description
6	Not used
7	Requests to send
8	Clears to send
9	Not used

MP LAN Port

Figure 6 shows the MP LAN port connector pins and LEDs.

Figure 6 MP LAN Port

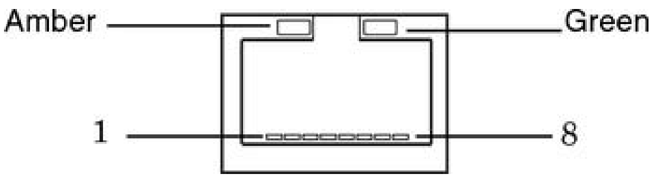


Table 5 maps the MP LAN port connector pin numbers to their signal descriptions.

Table 5 MP LAN Port Pinouts

Pin Number	Signal Description
1	TXP
2	TXN
3	RXP
4	Not used
5	Not used
6	RXN
7	Not used
8	Not used

MP LAN LEDs

Table 6 lists the MP LAN link status LEDs and states.

Table 6 MP LAN Link Status LEDs

Link State	LED State
Activity	Blinking green
Link with no activity	Solid green
No link	Off

Table 7 lists the MP LAN link speed LEDs and states.

Table 7 MP LAN Link Speed LEDs

Link Speed	LED State
100 Mb/s	Solid amber
10 Mb/s	Off

3 Getting Connected to iLO 2

This chapter provides information on getting connected to iLO 2 through a rackmount server or a server blade.

Setup Checklist

Table 8 Setup Checklist

Step		Action	X
Standard			
• For rackmount servers, perform all of the following steps. • For server blades, see "Server Blade Connection" (page 39) first and then continue with steps 3-8 below.			
1	Prepare	**1.** Determine the access method to select and connect cables. **2.** Determine the LAN configuration method and assign an IP address if necessary. **NOTE:** When accessing iLO 2 via LAN, HP recommends that iLO 2 management traffic be on a separate dedicated management network and that only administrators be granted access to that network. **3.** Find and remove the iLO Network Information Tag. This tag contains the default DNS name and iLO 2 login information. Removing the tag ensures ventilation holes are kept clear for proper server cooling.	
2	Configure the MP LAN	Choose a method to configure the LAN for iLO 2 access: • DHCP with DNS (Use the default DNS name supplied on your iLO Network Information Tag.) • ARP Ping (This feature is supported on certain Integrity servers to assign a static IP number to the MP LAN.) • Console serial port (RS-232) (You can perform all iLO 2 text commands from a serial console, or you can use this interface to assign a static IP number, disconnect the serial port, and resume from a web browser.)	
3	Log in to iLO 2	Log in to iLO 2 from • a supported web browser if using DNS or static IP • the TUI if using the console serial port Use the default user name and password (Admin, Admin) as found on your removable iLO Network Information Tag.	
4	Change default user name and password	Change the default user name and password on the administrator account to your predefined selections.	
5	Set up user accounts	Set up the user accounts if you are using the local accounts feature.	
6	Set up security access	Set up the security access settings.	
7	Access the host console	Access the host console using your method of choice.	

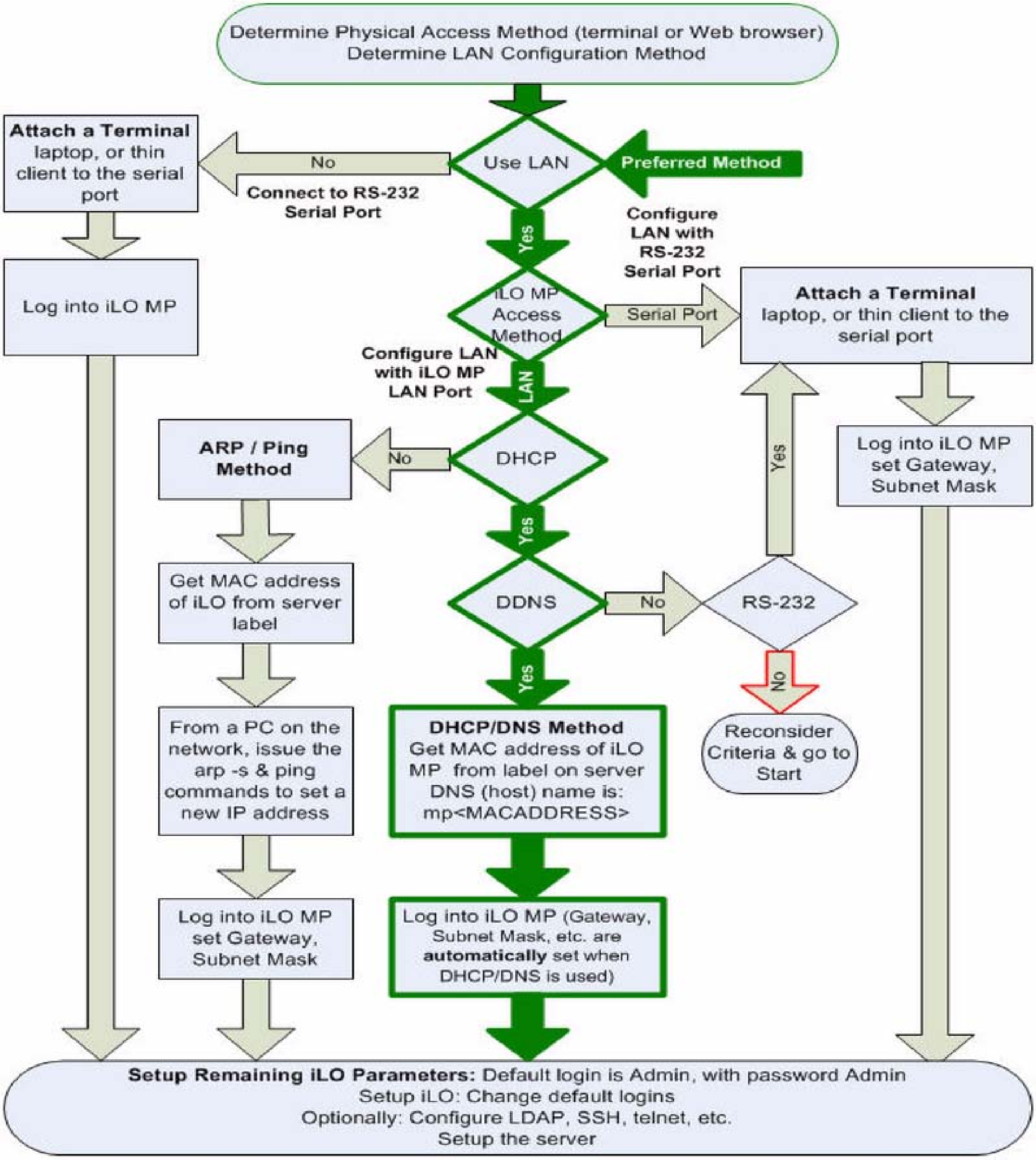
Table 8 Setup Checklist *(continued)*

Step		Action	X
Advanced			
8	Activate advanced features	• Integrity entry class ○ Activate advanced features by entering your HP Integrity Advanced Pack license key. • Integrity server blades ○ Ships with Advanced Pack license key factory installed. • Integrity mid range and Superdome ○ Advanced features are enabled per hard partition with installation of Lights-Out Advanced KVM cards. No Advance Pack license key required.	

Setup Flowchart

Use this console setup flowchart as a guide to help set up the Integrity iLO 2.

Figure 7 Setup Flowchart



Determine Physical Access Method (terminal or Web browser)
Determine LAN Configuration Method
Use LAN
Preferred Method
No
Connect to RS-232 Serial Port
Attach a Terminal laptop, or thin client to the serial port
Log into iLO MP
Yes
Configure LAN with RS-232 Serial Port
iLO MP Access Method
Serial Port
Attach a Terminal laptop, or thin client to the serial port
Configure LAN with iLO MP LAN Port
LAN
Log into iLO MP set Gateway, Subnet Mask
DHCP
No
ARP / Ping Method
Yes
Get MAC address of iLO from server label
DDNS
No
RS-232
Yes
No
Reconsider Criteria & go to Start
From a PC on the network, issue the arp -s & ping commands to set a new IP address
DHCP/DNS Method
Get MAC address of iLO MP from label on server
DNS (host) name is: mp<MACADDRESS>
Log into iLO MP set Gateway, Subnet Mask
Log into iLO MP (Gateway, Subnet Mask, etc. are automatically set when DHCP/DNS is used)
Setup Remaining iLO Parameters: Default login is Admin, with password Admin
Setup iLO: Change default logins
Optionally: Configure LDAP, SSH, telnet, etc.
Setup the server

There are differences in how you connect to iLO 2 depending on if you have a rackmount server or a server blade.

Rackmount Server Connection

For a rackmount server, you can connect directly through the serial console or you can connect using the MP LAN.

To set up the console:

1. Determine the physical access method to connect cables. There are two physical connections to iLO 2 :
   - Console serial port (RS-232)
   - MP LAN port
2. Assign an IP address to the iLO 2 MP LAN using one of the following methods:
   - DHCP and DDNS. Though there are several methods to configuring the LAN, HP recommends DHCP with DNS. DHCP with DNS comes preconfigured with default factory settings, including a default user account and password. Use the DNS name on the iLO Network Information Tag on the server.

     To assign a static IP address instead of using DHCP, use one of the following methods:
   - ARP Ping. This method can be used for Integrity entry class only.
   - Console serial port (RS-232)

Preparing to Set Up iLO 2

Perform the following tasks before you configure the iLO 2 MP LAN:

- Determine the physical access method to select and connect cables.
- Determine the iLO 2 MP LAN configuration method and assign an IP address if necessary.

NOTE: Server blade iLO 2s are assigned an IP address by the blade chassis OA.

Determining the Physical iLO 2 Access Method

Before you can access iLO 2, you must determine the correct physical connection method.

There are several ways you can physically connect to iLO 2. Table 9 lists the appropriate connection method, required connection components, and connectors to the host console.

Table 9 Physical Connection Matrix

Connection Method	Required Connection Components
Console serial port (RS-232)	• Host console • Console serial port (RS-232) DB-9F to DB-9F cable (modem eliminator cable) • Emulation terminal device (for example, a PC, laptop, or ASCII terminal) These connection methods directly attach to the iLO 2 MP through the console serial port. This is an RS-232 connection from a workstation to the server's iLO 2 MP console serial port. Serial cable concentrators are used to provide switched access from one workstation to multiple servers. Typically, the console serial port method is used by an administrator in the data center.
LAN port	10/100 LAN cable Remote access to the iLO 2 is a more convenient method. This remote access is through the MP LAN port. Depending on your LAN administration, this can be restricted to the datacenter, or extended outside the data center to your company's intranet. For greater security, HP recommends restricting LAN access to well known, trusted and secured networks. The iLO 2 has a separate LAN port from the system LAN port. It requires a separate LAN drop, IP address, and networking information from that of the operating system LAN port. See Figure 3 and Figure 4 (page 28) and use Table 9 to determine your physical connection method.

Determining the iLO 2 MP LAN Configuration Method

To access iLO 2 through the MP LAN, iLO 2 must acquire an IP address. The way iLO 2 acquires an IP address is dependent upon whether DHCP is enabled or disabled on the server, and if DHCP and DNS services are available to the server (see Table 10).

Once you have determined the iLO 2 access method, you must determine how you will configure the MP LAN in order to acquire an IP address using the following methods:

- DHCP/DNS through the management LAN (dynamically assigns an IP address): use the DNS name on the iLO Network Information Tag on the server.
- Setting up a static IP address using a laptop with DHCP services and the management LAN.
- ARP Ping to set a static IP using a laptop and the management LAN (assigns a static IP address to Integrity entry class only)
- Local RS-232 serial port and a serial console (assigns a static IP address).

Table 10 provides all the possible IP address acquisition scenarios. Use this table to help you select the appropriate LAN configuration method to obtain an IP address.

Table 10 LAN Configuration Methods

DHCP	DNS	Console Serial Port (RS-232)	LAN Configuration Method
Yes	Yes	No	DHCP
Yes	Yes	Yes	DHCP or console serial port
No	No	No	ARP Ping (entry class only)
No	Yes	No	ARP Ping (entry class only)
No	Yes	Yes	ARP Ping (entry class only); or console serial port
Yes	No	Yes	Console serial port
No	No	Yes	Console serial port or ARP Ping (entry class only)
Yes	No	No	Cannot set up the LAN; reconsider your criteria

Configuring the iLO 2 MP LAN Using DHCP and DNS

DHCP automatically configures all DHCP-enabled servers with IP addresses, subnet masks, and gateway addresses. All HP Integrity entry class servers with iLO 2 are shipped from the factory with DHCP enabled.

HP recommends using the DHCP and DNS method to simplify access to iLO 2.

NOTE: You can use ARP Ping on entry class servers regardless of the status of DHCP unless an IP address has ever been acquired using DHCP. Once an IP address is assigned using DHCP, ARP Ping is permanently disabled.

When you use DHCP and DNS, you can connect to iLO 2 by entering the DNS name in your browser rather than an IP address **only** if the following applies:

- DHCP must be enabled (DHCP is enabled by default).
- You are using a DHCP server that provides the domain name.
- The primary DNS server accepts dynamic DNS (DDNS) updates.
- The primary DNS server IP address was configured through the DHCP server.

IMPORTANT: You must know the DNS domain name, which is served out by the DHCP server, unless its domain is local or the same domain.

To configure iLO 2 using DHCP and DNS:

1. Obtain the factory-set DNS name from the iLO Network Information Tag on the server. The DNS name is 14 characters long. It consists of the letters `MP` followed by the 12 characters of the MAC address. For example:

   ```
   mp0014c29c064f
   ```

   This address is assigned to the iLO 2 MP system board. The system board has a unique MAC address that identifies the hardware on the network.
2. Connect the MP LAN cable from the server to an active network port.
3. Apply AC power to the server.
4. Open a browser, Telnet, or SSH client and enter the fully-qualified DNS name (the full path name ending in the DNS name). The iLO 2 Log In window appears.
5. Log in using the default user name and password (Admin/Admin).

△ **CAUTION:** When DHCP is enabled, the system is vulnerable to security risks because anyone can access iLO 2 until you change the default user name and password.

HP strongly recommends you assign user groups and rights before proceeding.

For greater security, HP recommends that iLO 2 management traffic be on a separate dedicated management network that is configured to only allow limited access from selected secure systems by designated system administrators.

Configuring the iLO 2 MP LAN Using ARP Ping

This method can only be used for entry class.

NOTE: You can use ARP Ping regardless of the status of DHCP unless an IP address has ever been acquired using DHCP. Once an IP address is assigned using DHCP, ARP Ping is permanently disabled. Some DHCP server options can cause the apparent issuance of ARP Ping to iLO 2, which negates the DHCP over DNS method.

The Address Resolution Protocol (ARP) and Packet Internet Grouper (Ping) utility uses ARP packets to ping (discover) a device on the local network segment. The IP address you assign to the server must use the same network segment (subnet) as the system assigning the address. ARP does not work across routed or switched networks.

Use the ARP Ping utility to assign a static IP address when you do not have access to the console serial port (RS-232) or when DHCP is not available.

ARP Ping has the following operational issues:

- The PC and the server must be on the same physical subnet.
- When a new server is first booted, DHCP is automatically available (factory-set default), but ARP Ping does not start until three minutes after iLO 2 is booted. This applies to every subsequent boot of iLO 2 until an IP address is obtained by DHCP or is assigned using the `LC` command.
- Upon successfully assigning an IP address using ARP Ping, DHCP is automatically disabled.

Select one of the following methods to use the ARP Ping utility:

1. Connect a PC to the network that is on the same physical subnet as the server and run the ARP Ping commands from the PC.
2. Locate an existing server on the network and log in to it.
3. Run the ARP Ping commands from the server.

Table 11 lists the ARP Ping commands.

Table 11 ARP Ping Commands

ARP Command	Description
`arp -s`	Assigns the IP address to the iLO 2 MP MAC address. This ARP table entry maps the MAC address of the iLO 2 MP LAN interface to the static IP address designated for that interface.
`ping`	Tests network connections and verifies that the MP LAN port is configured with the appropriate IP address.

NOTE: The following procedure explains how to use the ARP Ping utility using a PC that is connected to the network that is on the same physical subnet as the server.

To configure a static IP address using the ARP Ping utility:

1. Obtain the iLO 2 MP MAC address. To set the IP address using ARP, you must know the MAC address of the iLO 2 MP LAN. You can find the MAC address of the iLO 2 MP LAN on a label on the server.

   IMPORTANT: Make sure you obtain the MAC address to the iLO 2 MP LAN and not the MAC address to the server core LAN.

2. Verify that an active LAN cable on the local subnet is connected to the MP LAN port on the server.
3. Access a PC on the same physical subnet as the server.
4. Open a DOS window on the PC.
5. At the DOS command prompt (`C: >`) , enter **`arp -s`** to assign the IP address to the iLO MAC address.

   The syntax is as follows:

   `arp -s` *`<IP address you want to assign to the iLO MAC address>`* *`<iLO 2 MAC address>`*

   Example from Windows

   ```
   arp -s 255.255.255.0 00-00-0c-07-ac-00
   ```

6. At the DOS command prompt, enter **`ping`** followed by the IP address to verify that the MP LAN port is configured with the appropriate IP address. The destination address is the IP address that is mapped to the iLO MAC address. Perform this task from the PC that has the ARP table entry.

   The syntax is as follows:

   `ping` *`<IP address just assigned to the iLO MAC address>`*

   Example from Windows

   ```
   ping 192.0.2.1
   ```

7. Use this IP address to connect to the iLO 2 MP LAN.
8. Use web or Telnet access to connect to iLO 2 from a host on the local subnet and configure the rest of the LAN parameters (gateway, subnet).

Configuring the iLO 2 MP LAN Using the Console Serial Port

The terminal emulation device runs software that interfaces with the server. The software emulates console output as it would appear on an ASCII terminal screen and displays it on a console device screen.

To configure the iLO 2 MP LAN using the console serial port (RS-232):

IMPORTANT: Do not configure duplicate IP addresses on different servers within the same network. The duplicate server IP addresses conflict and the servers cannot connect to the network.

The LC command enables you to configure a static IP address, host name, subnet mask, and gateway address.

IMPORTANT: Ensure you have a console connection through the console serial port (RS-232) or a network connection through the LAN to access the iLO 2 MP CLI and use the LC command.

1. Ensure the emulation software is correctly configured:
   a. Verify that the communication settings are configured as follows:
      - 8/none (parity)
      - 9600 baud
      - None (receive)
      - None (transmit)
   b. Verify that the terminal type is configured appropriately. The following are supported terminal types:
      - hpterm
      - vt100
      - vt100+
      - vt-utf8

   IMPORTANT: Do not mix hpterm and vt100 terminal types at the same time. If there are two users collaborating and viewing console output with different emulation modes set, their clients will see garbled results if the output from the system is terminal specific.

   Consult the help section of the emulation software application for instructions on how to configure the software options.
2. Use Table 9 to determine the required connection components and the ports used to connect the server to the console device.
3. Connect the cables.
4. Start the emulation software on the console device.
5. Log in to iLO 2. See "Logging In to iLO 2 Using the Command Line Interface" (page 47).
6. At the MP Main Menu, enter **CM** and press **Enter** to select command mode.
7. At the command mode prompt, enter **LS** and press **Enter**. The screen displays the default LAN configuration values. Write down the default values or log the information to a file.
8. To disable DHCP, enter the LC command.
   a. From the LC command menu, enter **D** and press **Enter**.
   b. Follow the instructions on the screen to change the DHCP status from enabled to disabled.
   c. Enter **XD -R** to reset iLO 2 (this is only necessary if you are connected through a serial port).
9. Use the LC command to enter information for the IP address, host, subnet mask, gateway parameters, and so on.
10. Enter **XD -R -NC** to reset iLO 2.
11. After iLO 2 resets, log in to iLO 2 again and enter **CM** at the MP> prompt.
12. To confirm that DHCP is disabled and display a list of updated LAN configuration settings, enter the **LS** command.

NOTE: HP ProLiant servers allow you to assign a static IP address at boot time to iLO 2 using a VGA monitor, keyboard, and mouse and HP ProLiant BIOS commands. This feature is not available on HP Integrity servers.

Server Blade Connection

For a server blade, you can connect directly through the SUV cable to the serial console or you can connect using the MP LAN internal connection in the blade enclosure.

NOTE: You do not cable up a separate MP LAN cable to each server blade.

In most circumstances, it is not necessary to physically connect to the iLO 2 on a Server Blade. The iLO 2 on server blades typically use the MP LAN connection in the blade enclosure, and typically get their LAN IP addresses assigned using the OA. In the rare cases where a physical connection directly to a server blade iLO 2 is necessary, use one of the following methods:

- Connect to iLO 2 with DHCP enabled. Use the OA/iLO network port on the rear of the enclosure. If the OA/iLO network port on the enclosure is connected to the local network that has a DHCP server, your iLO 2 MP IP address is automatically generated by the DHCP server. The server blade is factory set with DHCP enabled.
- Connect to iLO 2 with no network connection. Use the console serial port on the SUV cable. If the enclosure is not connected to any network, you must configure your server through the console serial port (RS-232) on the SUV cable.

NOTE: The local video port can be used to access the console at EFI or potentially the OS, but is not a connection to iLO 2. The USB provides keyboard and mouse to the operating system on HP Integrity server blades. Also, server blades do not support directly connecting a modem to the MP (called the remote RS-232 port on servers), so there is no remote RS-232 connection on the server blade. In addition, there is no LAN connection on the front of the server blade.

Connecting to a Server Blade iLO 2 Using the Console Serial Port

If the enclosure is not connected to any network, you must configure your server through the console serial port (RS-232) on the SUV cable. Use this procedure to configure the console serial port to enable iLO 2 access. To perform this procedure, you need a terminal emulator (for example, a laptop using hyperterm) to connect to the server blade.

NOTE: On the HP Integrity server blades, you have access to two serial ports through the RS-232 connector. The default setting is for the iLO 2 interface, the other is for an AUX UART directly connected to the host operating system and can be used for any serial device (terminal, debug port, and so on). HP recommends using the AUX UART for server blade setup and debug purposes only.

You can use a command to toggle between the two ports. However, if access to the iLO 2 MP TUI CLI is not possible through Telnet and if the port mode of operation is set to the AUX UART, perform a hard reset of iLO 2 to set it to the default shipping settings. To perform a hard reset, push the recessed MP Reset button.

TIP: It is not necessary to physically connect to iLO 2 through the console serial port to perform management tasks. Use the OA/iLO 2 LAN port to communicate with any iLO 2 in the enclosure and the OA. You can use the LCD panel and the OA to configure and determine the iLO 2 MP LAN address.

Connecting the SUV Cable to the Server Blade

This section describes how to connect your server blade to a terminal device using the SUV port.

△ **CAUTION:** Disconnect the SUV cable from the port when it is not in use. The port and connector are not intended to provide a permanent connection as it may block proper air flow if left attached for extended periods.

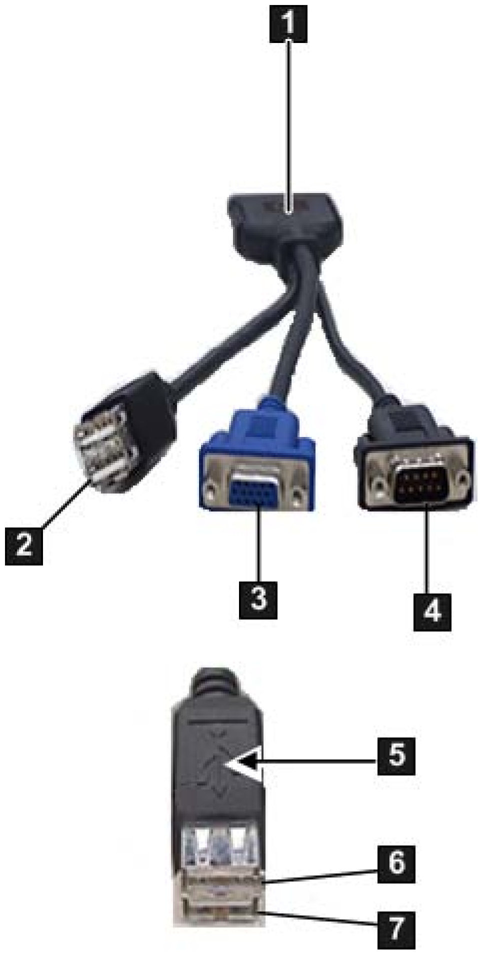
On the SUV cable, locking buttons are located on the sides of the server blade connector. Always squeeze the locking buttons on the SUV cable connector before disconnecting the SUV cable from the SUV cable port. Failure to do so can result in damage to the port.

Use caution when walking near the server blade when the SUV cable is installed. Hitting or bumping the cable can cause the port on the server blade to break. This can damage the system board, requiring it to be replaced.

To establish a connection from the server blade to the terminal emulator:

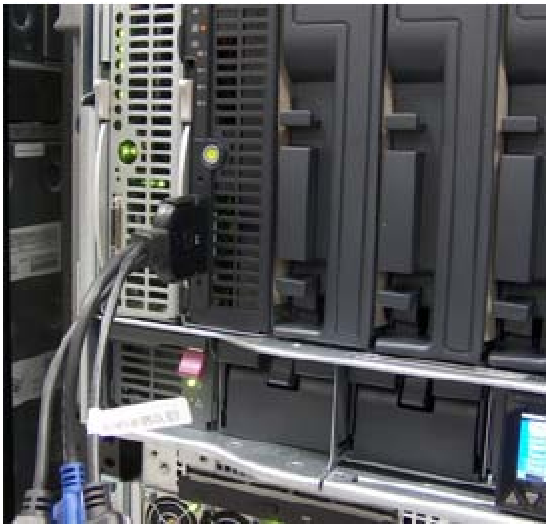
1. Insert the SUV cable into the SUV port on the rear of the server blade. See Figure 8 and Figure 9.
2. Connect a standard DB-9F to DB-9F modem eliminator cable to the RS-232 port on the SUV cable.
3. Connect the other end of the DB-9F to DB-9F modem eliminator cable to the terminal emulator.
4. Verify the parameters for serial console port communication are set to the following values on your terminal or emulator device:
   - VT 100 protocol
   - 8/none (parity)
   - 9600 baud
   - None (receive)
   - None (transmit)
5. To set the parameters, click **OK**.
6. If running an emulator, launch it now.

Figure 8 SUV Cable



1 Server Blade Connector
2 2-Port USB
3 VGA (no access to iLO 2)
4 9-Pin Console Serial Port (RS-232)
5 USB Label
6 USB-1
7 USB-0

Figure 9 Connecting the SUV Cable To the Server Blade



Connecting the Server Blade To iLO 2 Using the Onboard Administrator

If the OA/iLO network port on the enclosure is connected to the local network that has a DHCP server, your iLO 2 MP IP address is automatically generated by the DHCP server. The server blade is factory set with DHCP enabled.

For complete OA information, the following guides can be found on the HP website:

- For CLI, see the *HP BladeSystem Onboard Administrator Command Line Interface User Guide*.
- For web GUI, see the *HP BladeSystem Onboard Administrator User Guide*.

To connect to iLO 2 using the OA:

1. Connect a standard LAN cable to the OA/iLO network port on the rear of the server blade.
2. Connect the LAN cable to a local network that has a DHCP server. The LCD display panel on the front of the enclosure displays the Main Menu.
3. Select **Blade or Port Info** from the options and click **OK**.
4. Select the appropriate server blade from the options on the screen and click **OK**. The screen displays the iLO 2 MP IP address.
5. Write down the iLO 2 MP IP address.
6. Access iLO 2 through Telnet, SSH, or the web using the assigned DHCP iLO 2 MP IP address.

NOTE: For the HP Integrity server blades, you can use the OA to set the IP addresses for all iLO 2s. You can also find the iLO 2 MP address so you can log in.

ⓘ **IMPORTANT:** Integrity iLO 2 must have a reachable IP address as the default gateway address. Since the OA is always reachable, HP recommends using the OA IP address as the gateway address for Integrity iLO 2. If you use the Enclosure IP mode, this solution works during a failover. In the Enclosure IP mode, a static IP address is assigned to the active OA, and during a failover, the same IP address follows the active OA. If the OA IP address is assigned using DHCP, the solution does not work. In such instances, HP recommends manually changing the iLO 2 gateway address.

Auto Login

Auto login provides direct access to iLO 2 from the OA for users who already logged in to the OA. A user who has authenticated their connection to the OA can follow a link to a server blade in the enclosure without an additional login step. Auto login features and usage are as follows:

- A user who has authenticated a connection to the OA is able to establish a connection with iLO 2 without providing the user login and password to iLO 2.
- The OA provides the following auto login connection methods to iLO 2 links to users to launch these connections to iLO 2:

  iLO CLI SSH Connection

  If you logged in to the OA CLI through SSH, enter **`connect server <bay number>`** to establish an SSH/Telnet connection with iLO 2.

  iLO Web GUI Connection

  If you logged in to the OA web GUI, click on the link to launch the iLO web GUI.

- Auto login is implemented using IPMI commands over I2C between the OA and iLO 2 to create and delete user commands.
- Supports a maximum of four simultaneous OA user accounts. The OA keeps track of these users locally. The information maintained for each user is the user name, password, and privilege levels.
- User accounts for the auto login feature are created in the MP database when an auto login session is established. These accounts are deleted when the auto login session is terminated.
- If a maximum number of user accounts has already been reached, and the OA creates another account on iLO 2. The OA sends a request to iLO 2 to delete one of the previously created accounts, before attempting to create a new one.
- If iLO 2 is rebooted or power-cycled, it checks if there are any previously created OA user accounts in the iLO 2 user database when it boots up. If there are any previously-created OA user accounts, it deletes those accounts.
- View and manage user accounts created in iLO 2 by the OA like any other local user account on iLO 2. To view and manage user accounts, use the TUI `WHO, UC` commands; or use the User Administration Page in the web GUI.
- View and disconnect user connections established through the auto login feature just like other connections to iLO 2. To view and disconnect user connections, use the TUI `WHO, DI` commands, or use the User Administration Page in the web GUI.
- The OA supports three types of users: administrators, operators, and users. These user types map to the following iLO 2 capabilities:

  Administrators

  Can perform any function including iLO 2 MP configuration. This level equates to an iLO 2 user with all privilege levels such as, Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO MP settings. It allows access to all aspects of the OA including configuration, firmware updates, user management, and resetting default settings.

  Operators

  Provided access to the host system IRC, serial console, and vMedia. This level equates to an iLO 2 user with Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO settings. It allows access to all but configuration changes and user management. This account is used for individuals who might be required to periodically change configuration settings.

  Users

  Provided read-only login access to iLO 2. This account is used for individuals who need to see the configuration of the OA but do not need the ability to change settings. This level equates to an iLO 2 user with no privileges set.

NOTE: For information on how to set user roles and privilege levels in the OA, see the *HP BladeSystem Onboard Administrator User Guide*.

Initiating an Auto Login Session

The auto login session is initiated as follows:

1. The OA finds the first available auto login user by finding the first user entry with a time-created value of 0.(OAtmp1...OAtmp4).
2. If there are no available users, the oldest user is deleted.

   NOTE: This could terminate a currently active session.

   a. The OA sends a request to iLO 2 to delete that user.
3. The OA sends a command to create an OA user.
4. The OA launches an SSH or web GUI connection to iLO 2 and logs in with created user's credentials.

Terminating an Auto Login Session

When the auto login CLI or web GUI session is terminated, the following user clean up is performed:

- For auto login sessions, the temporary Auto Login iLO 2 account is deleted when the session with the iLO 2 is terminated.

User Account Cleanup During IPF Blade Initialization

During an IPF blade initialization, the OA and iLO 2 perform the following:

- When a server blade is inserted, or iLO 2 or the OA is reboot or reset, both the OA and iLO 2 perform cleanup of the accounts that could have been created for auto login before the reset.
- When iLO 2 initializes, the OA marks all four user slots as unused.
- Integrity iLO 2 scans its local user accounts. If there are any OA created user accounts, they are deleted from the iLO 2 user database.

Auto Login Troubleshooting

There may be times when auto login fails. The following information provides possible reasons for the failure

User Creation

When the OA sends a request to iLO 2 to create a new user, iLO 2 attempts to create a user in the local iLO 2 user database. Creation of an OA user could fail for a number of reasons:

- The local user database is disabled in iLO 2 and LDAP authentication is being used.
- The iLO 2 user database has reached the maximum number of users (19 users).
- There is already a user registered with the same login name.

User Login

After an OA user has been created in the iLO 2 database, the OA user login can still fail for a number of reasons:

- The iLO 2 upgrade is currently in progress, and no new connections are allowed.
- Maximum number of connections for the requested connection type (SSH, Telnet, web GUI) to iLO 2 has been reached.
- Requested connection type (SSH, Telnet or web) to iLO 2 is currently disabled.

User Deletion

When the OA sends a request to iLO 2 to delete a user, iLO 2 attempts to delete that user from the local iLO 2 user database. Deletion of an OA user could fail for a number of reasons:

- A user with the specified login does not exist (user could have been deleted through other iLO 2 user interface).
- The specified user cannot be deleted because it is the only user in the local database with user administration right.

Additional Setup

This section provides additional information to set up iLO 2.

Modifying User Accounts and Default Passwords

Integrity iLO 2 comes preconfigured with default factory settings, including a default user account and password. The two default user accounts on initial login are:

- All Rights (Administrator) level user:

  login = **`Admin`**

  password = **`Admin`**

- Console Rights (Operator) level user:

  login = **`Oper`**

  password = **`Oper`**

  Login and password are case sensitive.

TIP: For security reasons, HP strongly recommends you modify the default settings during the initial login session.

Make the following changes using any of the iLO 2 user interfaces.

To modify default account configuration settings:

1. Log in as the administrator to modify default user configuration settings
2. To modify default passwords:
   a. Access the MP Main Menu.
   b. Enter **`CM`** at the `MP>` prompt.
   c. Enter **`UC`** at the `MP:CM>` prompt and follow the prompts to modify default passwords.
3. To set up user accounts:
   a. Access the MP Main Menu.
   b. Enter **`CM`** at the `MP>` prompt.
   c. Enter **`UC`** at the `MP:CM>` prompt and follow the prompts to modify user accounts.

Setting Up Security

For greater security and reliability, HP recommends that iLO 2 LAN management traffic be on a separate dedicated management network or network subnet and that only administrators be granted access to that network. This not only improves performance by reducing traffic load across the main network, it also acts as the first line of defense against security attacks. A separate network enables you to physically control which workstations are connected to the network.

Setting Security Access

Determine the security access required and what user accounts and privileges are needed. iLO 2 provides options to control user access. Select one of the following options to prevent unauthorized access to iLO 2:

- Change the default user name and password. See "Modifying User Accounts and Default Passwords" (page 45).

CAUTION: When DHCP is enabled, the system is vulnerable to security risks because anyone can access iLO 2 until you change the default user name and password.

HP strongly recommends you assign user groups and rights before proceeding.

- Create local accounts. You can store up to 19 user names and passwords to manage iLO 2 access. This is ideal for small environments such as labs and small-to-medium sized businesses.
- Use corporate directory services to manage iLO 2 user access. This is ideal for environments with a large number of frequently changing users. If you plan to use directory services, HP recommends leaving at least one local account enabled as an alternate method of access.

For more information on how to create local accounts and use directory services, see Chapter 9: "Installing and Configuring Directory Services " (page 169).

Setting iLO 2 MP LAN From EFI

Integrity iLO 2 supports an EFI utility to view or configure the iLO 2 MP LAN parameters. If the parameters have not been previously configured, you can use this utility to set them from EFI.

To view the iLO 2 MP LAN parameters from EFI:

1. Boot to the EFI Shell.
2. Run `ilosetup.efi` from EFI.

```
fs0:\EFI\TOOLS> ilosetup get
Current LAN parameters:
   IP Address : 15.255.96.44
   Subnet     : 255.255.248.0
   Gateway    : 15.255.96.1
```

To configure the iLO 2 MP LAN parameters from EFI:

1. Boot to the EFI Shell.
2. Run `ilosetup.efi` from EFI.

```
fs0:\EFI\TOOLS> ilosetup get
Current LAN parameters:
   IP Address : 127.0.0.1
   Subnet     : 255.255.255.0
   Gateway    : 127.0.0.1

fs0:\EFI\TOOLS>
fs0:\EFI\TOOLS> ilosetup set -l -i 15.255.96.44 -g 15.255.96.1 -s 255.255.248.0
Attemping to set iLO LAN parameters...
LAN parameters have been set.
```

The iLO 2 resets after you have successfully configured the LAN parameters.

4 Logging In to iLO 2

This chapter provides instructions on how to log in to iLO 2.

Integrity iLO 2 standard features provide basic system board management functions, diagnostics, and essential Lights-Out functionality on iLO 2-supported HP servers. For a list of the standard features, see "Standard Features" (page 18).

Logging In to iLO 2 Using the Web GUI

To log in to iLO 2 using the web GUI:

1. Open a web browser and enter the DNS name or the IP address for the iLO 2.
2. Log in using the default iLO 2 user name and password (Admin/Admin).

TIP: For security reasons, HP strongly recommends you modify the default settings during the initial login session. See "Modifying User Accounts and Default Passwords" (page 45).

Logging In to iLO 2 Using the Command Line Interface

To log in to the iLO 2 command line interface:

1. Access iLO 2 using the console serial port (RS-232), or enter through the LAN, using Telnet, SSH, or console emulation method. The iLO 2 MP login prompt appears.
2. Log in using the default the iLO 2 user name and password (Admin/Admin).

TIP: For security reasons, HP strongly recommends you modify the default settings during the initial login session. See "Modifying User Accounts and Default Passwords" (page 45).

Following is the MP Main Menu:

```
   CO:    Console
  VFP:    Virtual Front Panel
   CM:    Command Menu
   CL:    Console Logs
   SL:    Show Event Logs
SMCLP:    Server Management Command Line Protocol
   HE:     Main Menu Help
    X:     Exit Connection
```

See Section : "Text User Interface" (page 75) for information on the iLO 2 MP menus and commands.

TIP: When logging in using the local or remote console serial ports, the login prompt may not display if another user is logged in through these ports. In this case, use **Ctrl-B** to access the MP Main Menu and the `MP>` prompt.

Network Port Usage

The open network ports iLO 2 uses are listed in the following tables. Table 12 lists the TCP ports and Table 13 lists the UDP ports.

Table 12 TCP Ports

Port Identifier	Port Type	Port Functionality
Port 22	SSH port	This is the default port used by clients connecting to iLO 2 using SSH protocol.
Port 23	Telnet port	This is the default port used by clients connecting to iLO 2 using Telnet protocol.
Port 80	http port	This is the default port used by clients connecting to iLO 2 using the web interface or a web browser. This port is not secure. This port provides basic iLO 2 identification information when queried. Any web connection made on port 80 is redirected to the login on the https port for a secure web session.
Port 443	https port	This is the port used by clients connecting to iLO 2 using the web interface or a web browser securely. This is a secure port.
Port 2023	remote serial console port	Clients connect to this port by default when using the Remote Serial Console connection.
Port 4644	vKVM port	Clients connect to this port when using the Integrated Remote Console connection.
Port 17988	vMedia port	Clients connect to this port when using the Virtual Media applet connection.

Table 13 UDP Ports

Port Number	Port Functionality
Port 161	This port is used by clients to query SNMP information from iLO 2.
Port 623	This port is used by clients to issue IPMI commands to iLO 2.

5 Adding Advanced Features

Integrity iLO 2 advanced features are enabled on Integrity servers in one of two ways.

- For Integrity entry class and server blades, the advanced features are enabled with a license key.
- For Integrity cell-based servers, the advanced features are enabled with a PCI-X accessory card instead of a key.

For a description of the iLO 2 advanced features and information on how to add advanced features, see "Advanced Features" (page 21).

Lights-Out Advanced KVM Card for sx2000 Servers

The HP Lights-Out Advanced KVM card is a PCI-X card that you install into any sx2000-based mid range or high end HP Integrity server such as rx7640, rx8640, and Superdome sx2000.

The card works in conjunction with the iLO 2 management processor built into your server and enables the iLO 2 management processor and web GUI interface to access the IRC and vMedia in each hard partition (nPar).

The iLO 2 communicates with the Lights-Out Advanced KVM card over an internal system bus. The card has an external management LAN port which must be connected externally to the same subnet as the iLO 2 MP LAN. The Lights-Out Advanced KVM card uses this LAN port to provide IRC and vMedia communication with the remote user.

The card offers physical video functionality (VGA) for servers running Windows, and USB functionality for servers running HP-UX, Windows, and OpenVMS.

This Lights-Out Advanced KVM card (AD307A) is a superset of the previous graphics/USB card (A6869A or A6869B). The AD307A card should be used instead of A6869A or A6869B cards.

TIP: The AD307A is not "iLO on a card". It is not like the ProLiant Lights-Out 100 cards, or RILO cards. The AD307A is a card that adds the logic and firmware to enable the Lights-Out Advanced features of vMedia and the IRC. This card works by extending the features of the iLO2 of the main chassis. This card does not require any additional license keys (no "Advanced Pack license").

You must install one card in each hard partition (nPar) where the Lights-Out Advanced features are required. You can assign an IP number to the Lights-Out Advanced KVM card through the iLO 2 web GUI or the MP command line interface. The Lights-Out Advanced KVM card features are presented to you through the main iLO 2 interfaces.

IMPORTANT: Lights-Out Advanced features are fully enabled on the Lights-Out Advanced KVM card. You do not need to purchase an additional "advanced pack" license to access the functionality.

The Lights-Out Advanced KVM card offers the following features:

- Provides extra features for flexibility and manageability of sx2000-based Integrity servers for both remote management when being physically in the datacenter is inconvenient or impractical; and management while in the datacenter.
- The Lights-Out Advanced KVM card enables the advanced IRC and virtual CD/DVD/ISO image file (vMedia) features of iLO 2.
  - Load software from a DVD using vMedia instead of making a trip to the datacenter.
  - IRC enables full VGA graphical console support remotely.
  - View the Windows console or Windows boot process with the IRC instead of a crash cart (monitor, keyboard).

- vMedia enables remote attachment of a USB read-only CD or DVD storage device, or ISO file image, including support for bootable media.
  - Use vMedia to easily upgrade firmware on npars.
  - Create an ISO file of a `vfat` file system with the required files
    - Start vMedia, present .iso file to npar, boot to EFI, go to the fsX: that corresponds to the vMedia, run e.g. `update.nsh` and repeat on next partition
  - For Windows, you can do installs remotely without having to cable up the VGA/USB card to an IP console switch or a physical monitor, keyboard, and mouse.
- Integrated VGA graphics and USB ports offer flexibility in the datacenter to monitor a system with full KVM functionality from boot, to desktop, to shutdown.
- Easily accessed through the iLO 2 web GUI.

Additional Lights-Out Advanced KVM card Information

HP Lights-Out Advanced KVM Card for sx2000 Servers White Paper on the HP website at:

http://docs.hp.com/en/AD307-90001/AD307-90001.pdf

You can read about the Lights-Out Advanced KVM card on the HP website at:

http://www.hp.com/go/integrityilo

You can read the Quick Specs on the HP website at:

http://h18000.www1.hp.com/products/quickspecs/12602_na/12602_na.HTML

You can read an example of ordering and configuration information on the HP website at:

http://ccesalewspr02.cce.hp.com/docfiles/V7%20Content/KGNew/6158816/c00430232.pdf

Lights-Out Advanced KVM card Requirements

This section addresses the following Lights-Out Advanced KVM card requirements and conditions:

- You need Java on the browser system to use vMedia.
- You need Internet Explorer Active-X controls to use the IRC.
- Internet Explorer 6.0 SP1 (minimum) is required for the IRC.
- You need to be running Internet Explorer (with Active-X) on the browser system to use the IRC. Currently, IRC only supports partitions running Windows.
- You can only launch one vMedia per complex. For example, if you have vMedia running for nPar1, you cannot run vMedia for nPar2.
- A network link to the partition's Lights-Out Advanced KVM card is required to launch vMedia. If there is no network link, the following message displays `Status: vMedia is in use or unavailable`.
- Vista client systems are not currently supported. You can still run your SSH and Telnet sessions to the MP for VFP, character console, and streaming live system event logs.

Table 14 lists the supported system configurations for the Lights-Out Advanced KVM card at the time this document was written. For the most recent product specifications, see **`www.hp.com/go/integrityilo`**.

Table 14 Supported System Configurations

System Component	Description
nPartition operating system	• Microsoft Windows Server 2003 • HP-UX 11i v2 or later • OpenVMS Version 8.3 or later • Windows 2008
Supported platforms	• rx7640 • rx8640 • Superdome sx2000

You can install the Lights-Out Advanced KVM card on any sx2000-based Integrity server with updated management processor firmware that provides iLO 2 functionality and uses the web interface to access iLO 2. The Lights-Out Advanced KVM card must be installed in a PCI-X mode-1 slot. It cannot be used in PCI-X mode 2 slots or in PCIe slots. To determine which slots are mode-1 compatible, see the documentation for your server product. A Lights-Out Advanced KVM card is required for each hard partition (nPartition) where you want virtual keyboard, video, mouse (vKVM) and vMedia functionality; Lights-Out Advanced functionality is not currently supported on virtual partitions (vPar).

TIP: Remember, you do not need an iLO 2 Advanced Pack license key to use this card.

Table 15 lists which features of the Lights-Out Advanced KVM card are available on each operating system.

Table 15 Availability of Features

nPartition Operating System	IRC[1]	vMedia	VGA Graphics Port	USB Ports
Windows	Yes	Yes	Yes	Yes
HP-UX	No	Yes	No	Yes
OpenVMS	No	Yes	No	Yes
Linux	Not currently supported under Linux.			

[1] The remote management workstation must be running Windows with Active-X enabled on Internet Explorer 7.

Configuring the Lights-Out Advanced KVM Card

Usually, the Lights-Out Advanced KVM card obtains its IP address automatically from a DHCP server. If you do not have a DHCP server on your network, you must manually set the Lights-Out Advanced KVM card IP address. To manually set the Lights-Out Advanced KVM card IP address:

- If you are using the web GUI, use the LAN Settings page on the Administration tab.
- If you are using the MP CLI, use the `LC` command.
  - MP:CM> lc

    MP Configurable LAN devices:

    1. MP Customer LAN
    2. Integrity LO Advanced KVM Card: Cab 0, IO Chas 1, Slot 7
    3. Enter LAN device to change, or [Q] to Quit:

NOTE: If the Lights-Out Advanced KVM card IP settings are not configured, the card still works as a local VGA/USB card, but IRC and vMedia do not work.

NOTE: Before the `LC` command allows you to configure an IP address, you must boot the system to EFI so the Lights-Out Advanced KVM card can be detected by system firmware.

TIP: You never need to connect serial cables to the Lights-Out Advanced KVM card. The Lights-Out Advanced KVM card communicates to iLO 2 through an internal bus.

Lights-Out Advanced KVM Card IRC Feature

The iLO 2 MP that is built into your server provides, as a standard feature, a virtual serial console where you can view the entire managed server in the standard HP-UX, Linux, OpenVMS, or Windows headless console format. The IRC feature of the Lights-Out Advanced KVM card enables you to view video output from the managed OS hard partition (nPartition) where the Lights-Out Advanced KVM card is installed, providing a seamless view from the server boot to OS desktop.

The Lights-Out Advanced hardware captures three essential components for the managed (host) nPartition:

- **K**eyboard input to the console
- **V**ideo output
- **M**ouse input to the console

When a user activates the remote console on the Windows management workstation, the Lights-Out Advanced KVM card sends all keyboard and mouse input from the IRC / vKVM client to the host nPartition.

For information on how to use the IRC, see "Integrated Remote Console" (page 109).

Lights-Out Advanced KVM Card vMedia Feature

Virtual Media support, which is part of the Lights-Out Advanced KVM card feature set, provides users with a virtual disk drive that connects to the managed server through the same management LAN as the iLO/MP, just as if it were physically connected to the server.

The Lights-Out Advanced KVM card uses a client-server model to perform vMedia functions. The Lights-Out Advanced KVM card streams virtual media data across a live network connection between the remote management console and the host server. The virtual media Java applet provides data to the Lights-Out Advanced KVM card as it is requested.

The Lights-Out Advanced KVM card contains a USB device that is viewed by the host OS as if it were a physical USB device connected to the server. Under the control of the Lights-Out Advanced KVM card firmware, a virtual USB device can be remotely connected to the host server. When the virtual media is connected, an OS that is USB-aware loads its standard USB mass storage driver. Once the USB mass storage driver is loaded, the server OS does not require additional HP drivers running on the server OS.

Additionally, the host server EFI system firmware is extended to support USB virtual devices, making virtual media available end-to-end (in a pre-boot environment, through OS loading and while the OS is operational).

NOTE: The Lights-Out Advanced KVM card must be connected to the same subnet as the MP LAN to enable vKVM and vMedia functionality.

For information on how to use vMedia, see "Virtual Media" (page 115).

Installing the Lights-Out Advanced KVM Card in a Server

You can install the HP Lights-Out Advanced KVM card into any mode-1 slot in a PCI-X backplane, or any mode-1 PCI-X slot in a PCI-X/PCIe backplane.

CAUTION: Observe all electrostatic discharge (ESD) safety precautions before attempting this procedure. Failure to follow ESD safety precautions could cause damage to the server.

CAUTION: You cannot add or replace a Lights-Out Advanced KVM card while the nPartition is running. You must first shut down the nPartition before adding or replacing the card. For more information on shutting down nPartitions and powering off hardware components, see your server documentation.

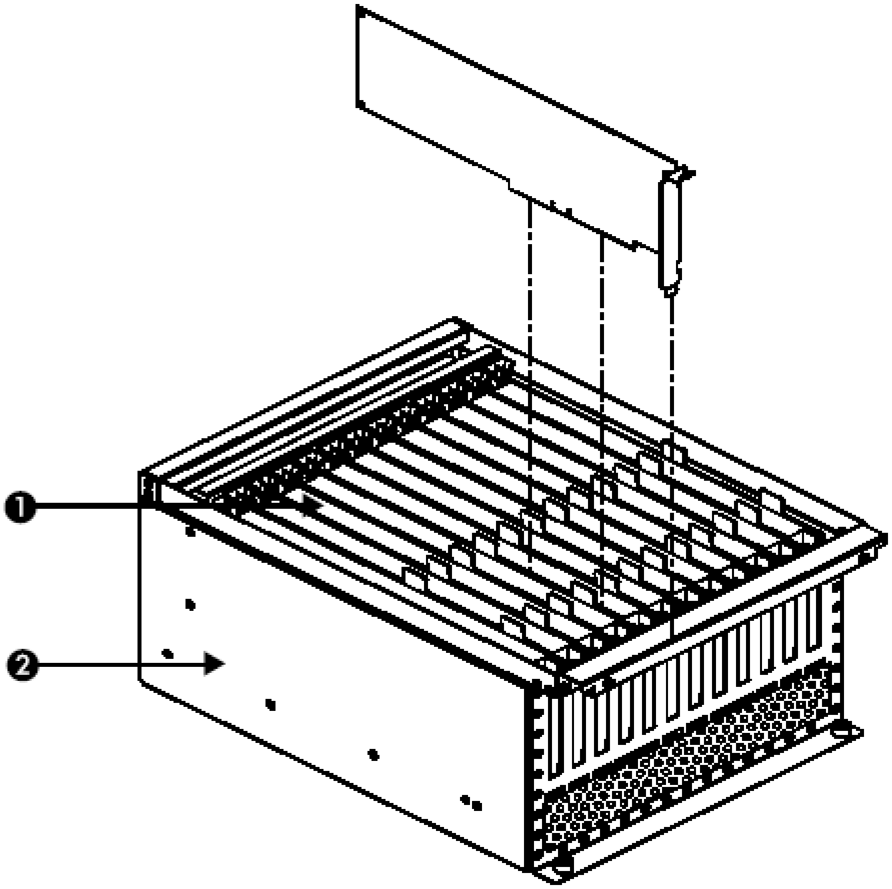
IMPORTANT: The HP Lights-Out Advanced KVM card requires that your server has the minimum system firmware installed. To see the firmware versions, go to the HP website at www.hp.com/go/integrityilo.

Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

IMPORTANT: The HP Integrity rx8640 and rx7640 midrange servers support only one Lights-Out Advanced KVM card per partition, and the card must be installed in an I/O chassis with a core I/O card installed. If you install multiple Lights-Out Advanced KVM cards on one partition, only the first card that is detected is fully enabled. Subsequent cards will have only USB functionality enabled.

IMPORTANT: The graphics functionality of the Lights-Out Advanced KVM card also takes precedence over the A6869B graphics/USB PCI card. If both a Lights-Out Advanced KVM card and an A6869B card are present on a partition, the A6869B card has only USB functionality enabled. HP recommends removing the A6869B card if you have both cards installed on a partition.

Figure 10 PCI-X or PCI-X/PCIe Card Cage (Common to all supported servers)



1 PCI-X/PCIe Cards
2 PCI-X or PCIe Backplane

IMPORTANT: Cabling requirements:

- You must connect the LAN port on the Lights-Out Advanced KVM card to the same network as the MP LAN port on the server.
- You need a network cable to your regular core I/O MP port - one per complex.
- You need one network cable to each Lights-Out Advanced KVM card.

To install the Lights-Out Advanced KVM card, perform the following steps:

1. Shut down the nPartition and power-off the appropriate PCI power domain.
2. Locate an empty mode-1 PCI-X slot where the card will be installed.
3. Position the card over the empty slot, ensuring that the edge connector keyways match on the PCI-X or PCI-X/PCIe backplane connector.
4. Using slow, firm pressure, seat the card in the slot.
5. Connect the management LAN cable to the LAN port on the card.

   NOTE: If you do not wish to use the on-card KVM features, ignore steps 6 and 7, and proceed to step 8.

6. Connect the monitor cable to the VGA port on the card, and connect the mouse and keyboard cables to the USB ports on the card.
7. Connect the monitor power cable, and then turn on the monitor.

8. Power on the PCI power domain, and then boot the nPartition.

   By default, the Lights-Out Advanced KVM card uses Dynamic Host Control Protocol (DHCP) to obtain an IP address. Alternatively, you can assign a static IP address to the Lights-Out Advanced KVM card through a menu in the main iLO 2 web GUI interface or other iLO 2 MP command line.

To remove the Lights-Out Advanced KVM card, reverse these steps.

Lights-Out Advanced KVM Card Quick Setup Steps

To perform a quick setup of the Integrity Lights-Out Advanced KVM card for vMedia and the IRC:

1. Plug the LAN cable into the MP of the core I/O card for the complex.
2. Plug the LAN cable into the LAN slot of the Lights-Out Advanced KVM card for each nPar.

   NOTE: Usually, the Lights-Out Advanced KVM card obtains its IP address automatically from a DHCP server. If you do not have a DHCP server on your network, you must manually set the Lights-Out Advanced KVM card IP address. To manually set the Lights-Out Advanced KVM card IP address, see “Configuring the Lights-Out Advanced KVM Card” (page 52)

3. Browse to iLO 2 (MP) and login.
   a. -> Administration -> Network Settings -> Device to modify: `<npar> KVM`
   b. -> assign a network address (DHCP or static) -> Submit.

      NOTE: You may also need to set up the Domain Name Server if you are not using DHCP.

4. Check the status of vMedia availability.
   a. Virtual Media -> select partition: `<npar name>` -> (check status directly under “select partition status”) it should read “Status: vMedia is available”.
      - If not, there may not be network connectivity to the Lights-Out Advanced KVM card – check this with ARP ping.
      - If the network is OK, check that another vMedia window for this complex is not open somewhere.

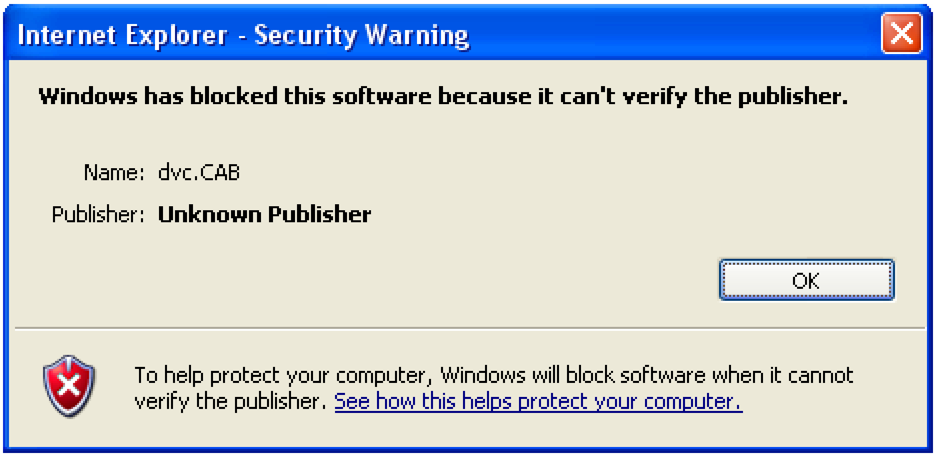
      NOTE: Only one vMedia window is shared among all the npars in the complex.

   b. If this fails, log out of iLO 2 and log back in again.
5. Once the vMedia window opens, select `Local Image File`.
6. Browse to the iso file and click `Connect`.

   NOTE: The IRC is only supported on Windows systems. You can only open one IRC session at a time with one iLO 2 web GUI session.

7. If not yet done, go to the EFI Shell: `acpiconfig` windows and reset.
8. Start the IRC. If you get the following “dvc.cab unknown publisher” error:

Figure 11 dvc.CAB Error



Internet Explorer - Security Warning

Windows has blocked this software because it can't verify the publisher.

Name: dvc.CAB

Publisher: **Unknown Publisher**

To help protect your computer, Windows will block software when it cannot verify the publisher. See how this helps protect your computer.

Follow these steps:

a. Close the IRC window.

b. Open a vMedia window for that npar (no need to connect).

c. Select `Always trust content from this publisher` in the Warning - Security window after opening vMedia.

d. Re-open the IRC window.

9. When rebooting. you should see the output of the console on both the serial console and the IRC. This will not appear if `acpiconfig` is in default mode. When it displays in graphic mode, you only see it on the IRC.

Using Lights-Out Advanced KVM Features

To access the iLO 2 web GUI, browse to the main iLO 2. The following functionality is available:

- Server status
- Firmware versions
- System event log
- Remote power
- Remote reset for partitions
- MP and Lights-Out Advanced-KVMs
- MP user administration
- MP and Lights-Out Advanced-KVM network settings

The only user access to the Lights-Out Advanced KVM card is through the main iLO 2 web GUI.

- The Lights-Out Advanced KVM card is not “iLO on a card”; and it is not a RILOE.
- The web browser does not connect directly to the Lights-Out Advanced KVM card. The web browser connects to the main iLO 2 for the whole chassis.
- The iLO 2 then communicates with the Lights-Out Advanced KVM card.
- The firmware does not allow direct communication with the Lights-Out Advanced KVM card.

In the main iLO 2 web GUI, there are a number of new tools that are unique to the Integrity cell-based servers. Specifically, there are pull-down tabs that enable you to select individual partitions for power (on/off/reset) management, vMedia, and IRC / vKVM. The last two, vMedia and IRC, are enabled per partition with the Lights-Out Advanced KVM card. The pull-down tabs for vMedia and IRC only show partitions that have Lights-Out Advanced KVM cards installed.

Mid Range PCI Backplane Power Behavior

On Integrity cell-based servers, you can power off the Lights-Out Advanced KVM card separately from the iLO 2 management processor. For example, you can power off a partition containing a Lights-Out Advanced KVM card, while keeping other partitions powered on. Or, you can power off the entire complex (all the partitions). In either case, the iLO 2 management processor is still accessible because it is powered separately from the partitions.

If iLO 2 is accessed while a partition is powered off, the Lights-Out Advanced KVM card in that partition could still appear in the partition drop-down lists for vMedia or IRC. However, you will not be able to start a vMedia or IRC session and the status will be “In use or unavailable”. If a vMedia or IRC session was already open when the partition was powered off, the session window remains open, but is not active.

Troubleshooting the Lights-Out Advanced KVM Card

When troubleshooting the Lights-Out Advanced KVM card, consider the following:

- Verify that the card is installed in the proper/supported slot. Be aware of slot restrictions.
- Check for Lights-Out Advanced KVM card seating and connections to the slot connector.
- Check that the slot MRL is closed.
- Make sure the supported firmware version for the MP, the server, and the Lights-Out Advanced KVM card is installed.
- Check that the Lights-Out Advanced and MP network cables are connected correctly.
- Check the LED link indicators on the bulkhead LAN port.
- Understand the Lights-Out Advanced RJ45 LAN connector LED definitions.
- Check that the cables are correctly connected to the Lights-Out Advanced bulkhead ports (LAN, VGA, USB1, & USB2).
- Check for the use of the correct DNS name for access/connection.
- Check the web browser support and configuration/restrictions.

Table 16 lists possible problems with the Lights-Out Advanced KVM card, and provides suggested solutions.

Table 16 General Troubleshooting

Problem	Solutions
Graphics error: Black screen. No text is displayed.	Hardware problem: • Must have supported power enabled. • Must have a functional mode-1 PCI-X slot. Try selecting another mode-1 slot on same partition/backplane. • Must have the card firmly seated in PCI-X/PCI-Xe backplane slot. • Must have a supported monitor. • Must have verified cable connections to the card. • Must have a functional Lights-Out Advanced KVM card.

Table 16 General Troubleshooting *(continued)*

Problem	Solutions
	`acpiconfig` problem: • Must have `acpiconfig` set to windows or enable `vgaroute`. • Boot to EFI mode and check with `acpiconfig` command.
Graphics error: Display is unreadable.	• Ensure that the system firmware supports the Lights-Out Advanced KVM card. • Ensure that the graphics resolution is compatible and set correctly.
vKVM or vMedia features are not available.	• Ensure that the LAN cable is connected properly. • Ensure that the Lights-Out Advanced KVM card is connected to the same network as the server iLO 2 MP.
Error message received when launching vKVM: Windows has blocked this software because it can't verify the publisher.	ActiveX Error: • Open a vMedia session on the server before running vKVM.
Publisher: Unknown Publisher `dvc.CAB`	• Select `Always trust content from this publisher.` in Warning – Security window after opening vMedia. • Open vKVM again.
Error message when using vKVM and Reflection X.	vKVM in fullscreen mode is not supported when using Reflection X.
Web display not formatted properly when using Firefox or Mozilla.	Use Internet Explorer only (other browsers are not supported).
Internet Explorer errors when opening vMedia or vKVM.	Ensure that the latest versions of Java and ActiveX are installed.

Core I/O Card Configurations

Both the HP Integrity rx7640 8-socket server and the HP rx8640 16-socket server always have at least one core I/O card (factory installed in I/O chassis 1 in the rx7640, and in I/O chassis 0 in the rx8640).

- In an rx7640 with only one core I/O card and one Lights-Out Advanced KVM card, you must install the Lights-Out Advanced KVM card in I/O chassis 1.
- In an rx8640 with only one core I/O card and one Lights-Out Advanced KVM card, you must install the Lights-Out Advanced KVM card in I/O chassis 0.
- For rx7640 or rx8640 servers with two core I/O cards, you can install the Lights-Out Advanced KVM card in either I/O chassis (with only one Lights-Out Advanced KVM card per partition).

Table 17 lists examples of unsupported core I/O card configurations with the Lights-Out Advanced KVM card and possible solutions.

Table 17 Unsupported Core I/O Configurations with Possible Solutions

Server	Configuration	Result	Solution
rx7640	• One core I/O card installed in I/O chassis 1. • Lights-Out Advanced KVM card installed in I/O chassis 0.	Operating system does not boot with this unsupported configuration.	Move the Lights-Out Advanced KVM card to I/O chassis 1.
rx8640	• One core I/O card installed in I/O chassis 0. • Lights-Out Advanced KVM card installed in I/O chassis 1.	Operating system does not boot with this unsupported configuration.	Move the Lights-Out Advanced KVM card to I/O chassis 0.

Supported PCI-X Slots

Table 18 lists supported mode-1 PCI-X slots for each supported server with either PCI-X or PCI-X/PCIe backplanes.

Table 18 Mode-1 PCI-X Slots by Server and Backplane

Server	PCI-X Backplane	PCI-X/PCIe Backplane	Notes
rx7640	• Use slots 1, 2, or 7 • Do not use slots 3, 4, 5, or 6	• Use slots 1, 2, or 7 • Do not use slots 3, 4, 5, or 6	• Slot 8 must be occupied by a core I/O card for the Lights-Out Advanced KVM card to function. • If a core I/O board is not present, use the lowest numbered cell with a core I/O board. • Use slot 7, 8, or the lowest numbered slot in the rootcell I/O chassis if a core I/O board is present. When using slot 7 or 8, make sure there are no other Lights-Out Advanced KVM cards in the I/O chassis, or they will be selected over the cards in slots 7 or 8.
rx8640	• Use slots 1, 2, 7, 8 • Do not use slots 3, 4, 5, or 6	• Use slots 1, 2, 7, 8 • Do not use slots 3, 4, 5, or 6	• Use the lowest numbered slot in the rootcell I/O chassis if a core I/O board is present. • If a core I/O board is not present, use the lowest numbered cell with a core I/O board. • Must be installed in slot 0 on Windows partitions. • In `acpiconfig` = default mode, USB devices (including vMedia) are not initialized by default. • Use the `search` and `map -r` EFI Shell commands to attach drivers and map file systems. (Create a boot option to avoid this step on future resets.)
Superdome sx2000	• Use slots 0, 1, 2, 3, 4, 7, 8, 9, 10, 11 • Do not use slots 5 or 6	• Use slots 0, 1, 8, 9, 10, 11 • Do not use slots 2, 3, 4, 5, 6, or 7	Use the lowest numbered slot in the rootcell I/O chassis.

Upgrading the Lights-Out Advanced KVM Card Firmware

The following utilities and the associated firmware files are available on the HP website at www.hp.com.

kvmFlasher — An EFI utility used to update the firmware of the RMP3 on the Lights-Out Advanced KVM card.

fpgaFlasher An EFI utility to update the firmware of the virtual video FPGA chip on the Lights-Out Advanced KVM card.

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

6 Accessing the Host (Operating System) Console

This chapter describes several ways to access the host console of an HP Integrity server.

Accessing a Text Host Console through iLO 2 Virtual Serial Console

Web browser access is an embedded feature of iLO 2.

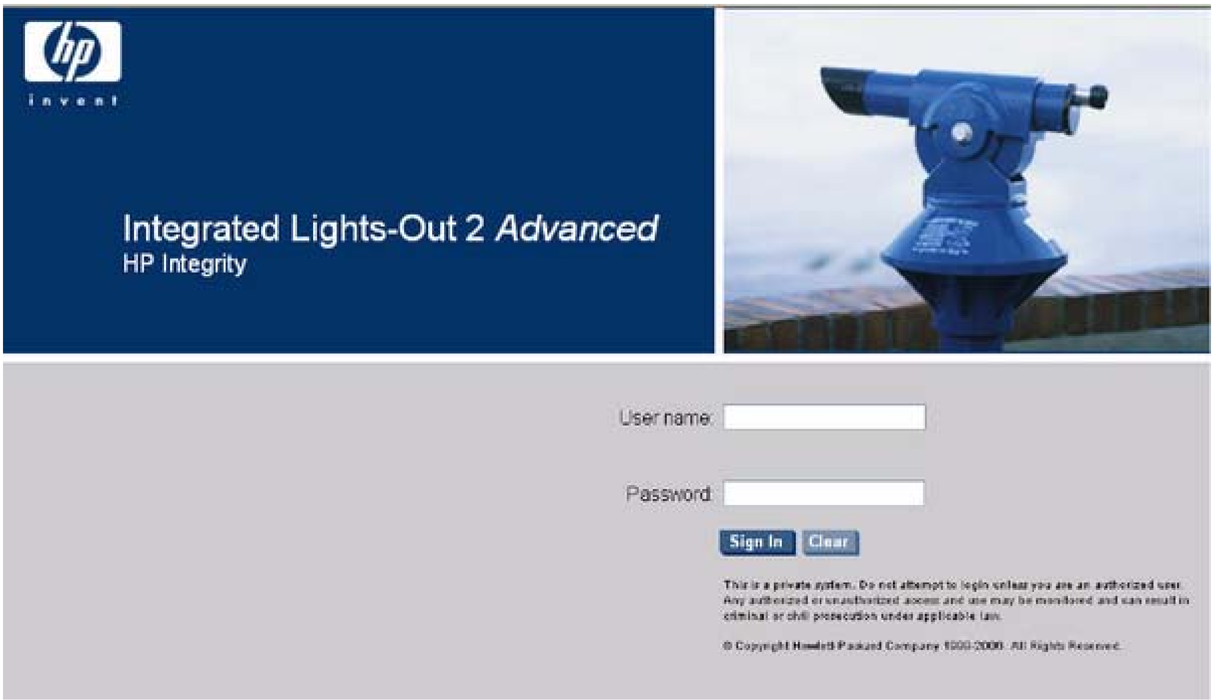
Before starting this procedure, you must have the following information:

- DNS name for the iLO 2 MP LAN. This is found on the iLO Network Information Tag on the server.
- Host name

To interact with iLO 2 through the web:

1. Open a web browser and enter the DNS name or the IP address for the iLO 2 MP.
2. Log in using your user account name and password at the login page. (Figure 12).

Figure 12 Web Login Page



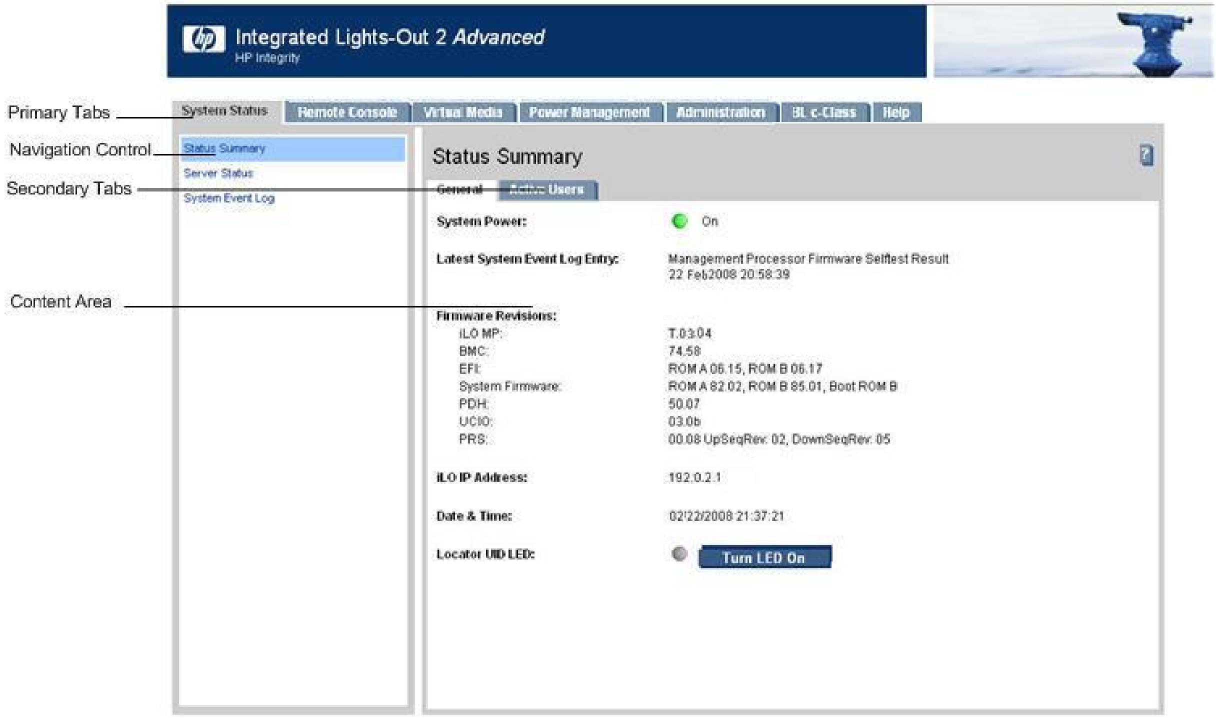
This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

© Copyright Hewlett Packard Company 1999-2006. All Rights Reserved.

NOTE: The iLO 2 web interface session times out after five minutes if there is no activity. If you open a remote console terminal window, the system remains open in the web interface session until you sign out. Also, the web session does not timeout if vMedia is connected.

3. Click **Sign In**. The Status Summary page (Figure 13) appears after login.

Figure 13 Status Summary Page



Status Summary

System Power: On

Latest System Event Log Entry: Management Processor Firmware Selftest Result
22 Feb2008 20:58:39

Firmware Revisions:

iLO MP:	T.03.04
BMC:	74.58
EFI:	ROM A 06.15, ROM B 06.17
System Firmware:	ROM A 82.02, ROM B 85.01, Boot ROM B
PDH:	50.07
UCIO:	03.0b
PRS:	00.08 UpSeqRev: 02, DownSeqRev: 05

iLO IP Address: 192.0.2.1

Date & Time: 02/22/2008 21:37:21

Locator UID LED:

4. Select the web interface functions by clicking the **Primary** tabs at the top of the page. Each function lists options in the **Navigation Control** on the left side of the page.
5. To display data in the content area; select an option and click **Refresh** to update the display.
6. Click the Remote Console tab. The remote console provides the following options to access the console:
   - A serial console that behaves similarly to the TUI
   - The virtual KVM console

Accessing Online Help

The iLO 2 web interface has a robust help system. To launch iLO 2 help, click **Help**. Alternately, click the **?** at the top right corner of each page to display help about that page.

Accessing a Text Host Console Using the TUI

To access the host console using the text user interface (TUI):

1. Log in using your user account name and password at the login page.
2. To switch the console terminal from the MP Main Menu to mirrored/redirected console mode, enter the `CO` command at the `MP>` login prompt. All mirrored data appears.
3. To return to the iLO 2 MP command interface, enter **Ctrl-B** or **Esc (**.

Help System

Integrity iLO 2 has a robust help system.

To access the Help menu from the TUI, enter **`HE`** at the `MP>` prompt. The following is the MP Help Main Menu:

```
==== MP Help: Main Menu ===============================================

Integrated Lights-Out for HP Integrity and HP 9000 - Management Processor (MP) MP Help System

Enter a command at the help prompt:
          OVerview   : Launch the help overview
          LIst       : Show the list of MP Main Menu commands
```

```
           <COMMAND> : Enter the command name for help on individual command
           TOPics    : Show all MP Help topics and commands
           HElp      : Display this screen
           Q         : Quit help

====
MP:HE
```

To display the Main Menu Command List, enter **`LI`** at the `MP HE:` prompt.

To return to the MP Main Menu, enter **`Q`**.

To access help from the web GUI, click **Help**. You can also click the ? at the top right corner of each page to display help about that page.

Accessing a Graphic Host Console Using the Integrated Remote Console

For information on how to access the host console using the vKVM feature through the Integrated Remote Console (IRC), see "Accessing the IRC" (page 112).

Accessing a Text Host Console Using SMASH SM CLP

For information on how to access the host console using the SMASH SM CLP, see "Accessing the SM CLP Interface" (page 142).

7 Configuring DHCP, DNS, LDAP, and Schema-Free LDAP

This chapter provides information on how to configure DHCP, DNS, LDAP extended schema, and schema-free LDAP.

Configuring DHCP

DHCP enables you to automatically assign reusable IP addresses to DHCP clients. This section provides information on how to configure DHCP options such as the Domain Name System (DNS).

The iLO 2 MP host name you set through this method displays at the iLO 2 MP command mode prompt. Its primary purpose is to identify the iLO 2 MP LAN interface in a DNS database.

NOTE: The HP-UX system name displayed by the `uname -a` command is different than the iLO 2 MP host name.

If the IP address, gateway IP address, and subnet mask are obtained through DHCP, you cannot change them without first disabling DHCP. If you change the host name and the IP address was obtained through DHCP and registered with dynamic DNS (DDNS), a “delete old name” request for the old host name and an “add name request” for the new host name are sent to the DDNS server.

If you change the DHCP status between enabled and disabled, the IP address, subnet mask, and gateway IP address are set to default values (127.0.0.1:0xffffff00). Also, the DNS parameters are voided. When you change the DHCP status from enabled to disabled, the DNS parameters for using DHCP are set to disabled, and the `Register with DDNS` parameter is set to `No`. When you change the DHCP status from disabled to enabled, the DNS parameters for using DHCP are set to enabled, and the `Register with DDNS` parameter is set to `Yes`.

NOTE: DNS is the comprehensive RFC standard; DDNS provides only a part of the DNS standard functionality.

To configure DHCP, use the `LC` command to perform the following actions:

- Set all default LAN settings.

  ```
  MP:CM> LC -all DEFAULT –nc
  ```

- Display current LAN settings.

  ```
  MP:CM> LC -nc
  ```

- Modify the MP DHCP status.

  ```
  MP:CM> LC -dhcp disabled
  ```

- Modify the MP IP address.

  ```
  MP:CM> LC -ip 192.0.2.1
  ```

- Modify the MP host name.

  ```
  MP:CM> LC -h hostname
  ```

- Modify the MP subnet mask.

  ```
  MP:CM> LC -s 255.255.255.0
  ```

- Modify the MP gateway address.

  ```
  MP:CM> LC -g 192.0.2.1
  ```

- Set the link state to autonegotiate.

  ```
  MP:CM> LC -link auto
  ```

- Set the link state to 10 BaseT.

  `MP:CM> LC -link t`

- Set the remote console serial port address.

  `MP:CM> LC -web 2023`

- Set the SSH console port address.

  `MP:CM> LC -ssh 22`

Configuring DNS

To use the DNS command to display and modify the DNS configuration:

1. From the MP Main Menu, enter command mode.
2. At the `MP:CM>` prompt, enter **`DNS`**. The screen displays the current DNS data.
3. When prompted, enter **`A`** to select all parameters. The screen displays the current DHCP for DNS servers status.
4. When prompted, enter **`Enabled`** or **`Disabled`**. The screen displays the current DHCP for DNS domain name status.
5. When prompted, enter **`Enabled`** or **`Disabled`**. The screen displays the current register with DDNS server value.
6. When prompted, enter **`Yes`** or **`No`**. The screen displays the current DNS domain name.
7. When prompted, enter a new value. The screen displays the primary DNS server IP address.
8. When prompted, enter a new value. The screen displays the optional secondary DNS server IP address.
9. When prompted, enter a new value. The screen displays the optional tertiary DNS server IP address.
10. When prompted, enter a new value.

The DNS configuration is updated as follows:

```
New DNS Configuration (* modified values):

   * S - DHCP for DNS Servers      : Disabled
   * D - DHCP for DNS Domain Name  : Disabled
     R - Register with DDNS Server : Yes
   * N - DNS Domain Name           : mpdns.company.com
   * 1 - Primary DNS Server IP     : 192.0.2.1
     2 - Secondary DNS Server IP   :
     3 - Tertiary DNS Server IP    :

Enter parameter(s) to revise, Y to confirm, or [Q] to Quit: Y

-> DNS Configuration has been updated

[mpserver] MP:CM>
```

Configuring LDAP Extended Schema

The following procedure shows how to configure iLO 2 to use a directory server to authenticate a user login using the iLO 2 MP TUI.

NOTE: The LDAP connection times out after 30 minutes of inactivity in Active Directory. For Novell directory, there is no inactivity timeout.

To configure using the web interface, see "Group Accounts" (page 130).

NOTE: The LDAP feature is only available if you have the iLO 2 Advanced Pack license.

To configure LDAP extended schema:

1. From the MP Main Menu, enter command mode.
2. At the `MP:CM>` prompt, enter **LDAP**.
3. To select **Directory Settings**, enter **D**. The current LDAP directory settings appear.
4. To select all parameters enter **A**. The current LDAP directory authentication status appears. The local iLO 2 user accounts database status also appears. If enabled, the local iLO 2 user database is used if there is an authentication failure using the LDAP Directory.
5. Enter **D** for disabled, or **E** for enabled. You must enter **E** if LDAP directory authentication is disabled. The current LDAP server IP address appears.
6. Enter the IP address of the LDAP server. The current LDAP server port address appears.
7. Enter a new port number. The screen displays the current object distinguished name. This specifies the full distinguished name of the iLO 2 device object in the directory service. For example, `CN=RILOE2OBJECT, CN=Users, DC=HP, DC=com`. Distinguished names are limited to 255 characters maximum plus one for the `NULL` terminator character.
8. Enter a new name. The **Current User Search Context 1** appears.
9. Enter a new search setting. The **Current User Search Context 2** appears.

   NOTE: The context settings 1, 2, and 3 point to areas in the directory service where users are located, so that users do not have to enter the complete tree structure when logging in. For example, `CN=Users, DC=HP, DC=com`. Directory user contexts are limited to 127 characters maximum plus one for the `NULL` terminator character for each directory user context.

10. Enter a new search setting. The screen displays the Current User Search Context 3.
11. When prompted, enter a new search setting.

The updated LDAP configuration is as follows:

```
New Directory Configuration (* modified values):

* L - LDAP Directory Authentication : Enabled
  M - Local MP User database        : Enabled
* I - Directory Server IP Address   : 192.0.2.1
  P - Directory Server LDAP Port    : 636
  D - Distinguished Name (DN)       : cn=mp,o=demo
  1 - User Search Context 1         : o=mp
  2 - User Search Context 2         : o=demo
  3 - User Search Context 3         : o=test

Enter Parameter(s) to revise, Y to confirm, or [Q] to Quit: y

 -> LDAP Configuration has been updated
```

Login Process Using Directory Services with Extended LDAP

You can choose to enable directory services to authenticate users and authorize user privileges for groups of iLO 2s. The iLO 2 directory services feature uses the industry-standard LDAP. HP layers LDAP on top of SSL to transmit the directory services information securely to the directory servers. More information about using iLO with directory services is available from the HP website at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf?jumpid=reg_R1002_USEN

HP provides a tool for Active Directory support of HP management processors. This tool, `HPQLOMIG.exe`, is part of *HP Directories Support for Management Processors* softpaq (SP31581.exe). It assists with installing the schema and snap-ins needed for Active Directory to work with iLO 2 products including Integrity iLO 2. This is for set up and management. It will not do automatic migration for you. For Integrity iLO 2, you must manually add iLO 2 objects to the directory server and set up user accounts and privileges. You can find the tool on the HP website at:

http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?lang=en&cc=US&swItem=MTX-UNITY-I23896

Using directory services after users enter their login and password, the browser sends the cookie to iLO 2. The iLO 2 processor accesses the directory service to determine which roles are available for that user login. iLO 2 first uses the credentials to access the iLO 2 device object in the directory. The directory service returns only the roles for which the user has rights. If the user credentials allow read access to the iLO 2 device object and the role object, iLO 2 determines the role object's distinguished name and the associated user privileges. iLO 2 then calculates the current user privileges based on those roles and grants them to that user.

Configuring Schema-Free LDAP

IMPORTANT: Due to command syntax changes in schema-free LDAP, some customer-developed scripts may not run. You must change any scripts you developed to enable them to run with the new schema-free LDAP syntax.

Integrity iLO 2 schema-free directory integration enables you to use the standard directory schema instead of adding HP's schema to the directory database. You accomplish this by authenticating users from the directory database and authorizing iLO 2 privileges based on matching groups stored on each iLO 2.

NOTE: Schema-Free LDAP is available only if you have the iLO 2 Advanced Pack license.

In addition to general directory integration benefits, iLO 2 schema-free integration provides the following advantages:

- Easy implementation without schema extensions.

  iLO 2 schema-free integration is configured from any iLO 2 user interface (browser, command line, or script).

- Minimal administration and maintenance.

  - After initial setup, only groups and permissions require maintenance support on iLO 2; typically group and permission changes occur infrequently.
  - The schema-free approach does not require updating directory databases with new iLO 2 devices objects.

- Reliable security.

  Integrity iLO 2 schema-free integration does not affect standard directory attributes, avoiding conflicting use of attributes that can result over time.

- Complements two-factor authentication.

  Integrity iLO 2 schema-free integration can be used in conjunction with iLO 2 two-factor authentication to provide asset protection using strong authentication.

NOTE: If you have already extended your directory with HP schema, there is no need to switch to the schema-free approach. Schema extension provides the lowest maintenance approach for directory integration. Once this process has taken place, there is no advantage for the schema-free approach until a schema change is required.

To configure schema-free LDAP:

1. Follow the procedure for "Configuring LDAP Extended Schema" (page 65), but omit Step 8. It is not necessary to enter a new port number.
2. Set up directory security groups.

Setting Up Directory Security Groups

The following procedure describes how to set up directory security groups in schema-free LDAP using the iLO 2 MP TUI. To use the web interface, see “Group Accounts” (page 130).

NOTE: Due to command syntax changes in schema-free LDAP, some customer-developed scripts may not run. You must change any scripts you developed to enable them to run with the new schema-free LDAP syntax.

NOTE: You must select the default schema from the LDAP command for the schema-free LDAP settings to work.

To set up directory security groups, follow these steps.

1. At the MP:CM> prompt, enter **LDAP**. The screen displays the current LDAP options.

```
[hqgstlb3] MP:CM> ldap

LDAP

Current LDAP options:
     D - Directory settings
     G - Security Group Administration
```

2. Enter **G**. The current group configuration appears.

```
Enter menu item or [Q] to Quit:G

Current Group Configuration:

       Group Names        Group Distinguished Names        Access Rights

  --------------------------------------------------------------------------

   1 - Administrator                                       C, P, M, U
   2 - User                                                C, P
   3 - Custom1                                             None
   4 - Custom2                                             None
   5 - Custom3                                             None
   6 - Custom4                                             None

   Only the first 30 characters of the Group Distinguished Names are displayed.

Enter number to view or modify, or [Q] to Quit:
```

3. Enter the number for the group you want to view or modify. The current LDAP group settings appear.
4. Set up a group distinguished name.
5. Select rights for the group.
6. Enter **Y** to confirm.

Login Process Using Directory Services Without Schema Extensions

You can control access to iLO 2 using directories without schema extensions. iLO 2 acquires the user name to determine group membership from the directory. iLO 2 then cross-references the group names with its locally stored names to determine user privilege level. iLO 2 must be configured with the appropriate group names and their associated privileges. To configure iLO 2, use one of the following methods:

- Web GUI (Administration > Directory Settings > Group Administration page)
- iLO 2 MP TUI (LDAP command)

LDAP and MP Login for Integrity Cell-Based Servers

This section provides information on LDAP and MP login access rights and partition configuration in iLO 2 for Integrity cell-based servers. System administrators can use this information to create and assign access rights.

This section explains the following:

- User login functions when configured with different rights for different partitions
- User management and privileges required to execute commands in iLO 2

Integrity iLO 2 is an independent support processor that provides system manageability features for a multi-partition server.

The following rules apply:

- Multiple users can simultaneously log in through the LAN port and independently manage partitions or view the server status.
- Local or LDAP users can have rights.
- A user who has rights on multiple partitions can have the same or different rights for each partition.
- For all operations that are not partition-specific, a user must have a specific right for all partitions to which access is granted.

The iLO 2 supports multiple sessions that perform independent tasks and enables the following usage models:

- A user can have multiple windows logged into iLO 2, and can perform long-term tasks such as monitoring virtual front panels or studying event logs in some windows while simultaneously performing short-term tasks like administering partitions from other windows.
- A user can independently connect to different partitions and manage them simultaneously.
- A user can reset a partition from one window and monitor the boot from another window while interacting with the console from yet another.

User Accounts

LDAP enables you to define iLO 2 user accounts in a centralized database on an LDAP server. LDAP directory support is an iLO 2 advanced feature that enables centralized, user account administration using directory services.

Commands

The iLO 2 commands have access levels to manage users effectively. Because iLO 2 commands work at different combinations of these access levels, you must understand how to categorize the commands.

The iLO 2 user interface has commands that can be classified into the following categories. Each category requires certain access rights as shown in Table 21.

Partition-specific Commands

These commands are partition-specific. They include commands that operate on a specified partition.

Composite Commands

These commands have sub commands within them that require different rights to execute. For example the SO command has `User Parameters`, `MP-wide parameters` within it. Each sub command needs rights as follows:

- MP:CM> `so`
  - MP wide parameters [U]
  - User parameters [M]
  - IPMI password [M]
  - OS initiated firmware update permissions [M]
  - Regenerate the SSH server public key [M]

Special Commands

These commands include operations that affect the cell, cabinet, or complex, and only users having 'All' rights for 'All' supported partitions are allowed to execute these commands.

MP-wide Commands

MP-wide commands require a specific command right for all partitions that a user has access to.

The iLO 2 commands are grouped in the above-mentioned categories, as shown in Table 19.

Table 19 Command Categories

MP-Wide Commands		Partition-Specific Commands	Composite Commands	Special Commands
cp	cc	bo	xd	pe
de	date	rr	so	re
df	dc	rs	cl	ru (KMIX only)
du	di	tc	sl	vm (sx2000 only)
he	fw	co		
if	id	cl		
ls	lt			
ma	lc			
ps	ldap			
te	parperm			
who	rl			
x	sa			
he	sysrev			
pwrgrd	dns			
pd	loc			
vfp	snmp			
ups				
fw				
io				

Access Rights

An iLO 2 user can have any, or all, of the following access rights:

Table 20 Access Rights for Cell-Based Servers

Access Right	Single Letter Representation	Description
Login Access	L	This right is required to perform any operation on iLO 2. A user must have this right for each partition to which access is granted. With this right, a user can run Status or Read-only commands.
Console Access	C	This right enables a user to access the console of the specified partition (such as the host OS). Console Access Level `CO` Command.
Server Power Access	P	This right enables a user to power on and off or reset the host platform.
MP Configuration Access	M	This right enables a user to configure iLO 2 parameters. Some examples of commands that are used to configure MP parameters are `CA, CC, CG, DATE, DC, DI, ID, IT, LC, LDAP, MFG, PARPERM`, and `RL`.
User Administration Access	U	This right enables a user to create, modify, and delete local iLO 2 user accounts and set the default partition for a session. Examples of an MP Local User Administration Level Command are `SO` and `PD`.
Virtual Media Access	V	This right enables a user to control and access vMedia for the selected partition.

Table 21 lists the iLO 2 commands and the access right associated with each command.

Table 21 Commands and Associated Access Right

Command	Location	Access Right
BO	Command Menu	Server Power Access
RR		Server Power Access
RS		Server Power Access
TC		Server Power Access
CC		MP Configuration Access
CP		Login Access
DATE		MP Configuration Access
DC		MP Configuration Access
DE		Login Access
DF		Login Access
DI		MP Configuration Access
DU		Login Access
HE		Login Access
ID		MP Configuration Access
IF		Login Access

Table 21 Commands and Associated Access Right *(continued)*

Command	Location	Access Right
IT		MP Configuration Access
LC		MP Configuration Access
LDAP		MP Configuration Access
LS		Login Access
MA		Login Access
PARPERM		MP Configuration Access
PD		User Administration Access
PE		All for all supported partitions
PS		Login Access
PWRGRD		Server Power Access
RE		All for all supported partitions
RU (KMIX only)		All for all supported partitions
SA		MP Configuration Access
SO		1. MP Wide Parameters - MP Configuration rights for all partitions to which the user has access 2. User Parameters - User Admin rights for all partitions to which the user has access 3. IPMI Password - MP Configuration rights for all partitions to which the user has access 4. OS initiated FW - MP Configuration rights for all partitions to which the user has access 5. Regenerate SSH Certificate - MP Configuration rights for all partitions to which the user has access
SYSREV		MP Configuration Access
TE		Login Access
WHO		Login Access
XD		1. Parameters Checksum and Ping - Login rights for all partitions that user has access to 2. Soft Reset for Master/Slave & IOX Master/Slave MP - MP Configuration rights for all partitions to which the user has access 3. Clear Persistent Parameters - User Admin rights and MP Configuration rights (for all partitions to which the user has access) 4. Reset Security Parameters - User Admin rights for all partitions to which the user has access 5. Force/Recover Master - Slave FailOver - MP Configuration rights for all partitions to which the user has access 6. Toggle Master/Slave FailOver Enable - MP Configuration rights for all partitions to which the user has access
DNS		MP Configuration Access
LOC		MP Configuration Access
SNMP		MP Configuration Access
UPS		MP Configuration Access
FW		MP Configuration Access

Table 21 Commands and Associated Access Right *(continued)*

Command	Location	Access Right
CI		1. View logs - Console rights for a partition 2. Clear logs - MP Configuration rights for all partitions to which the user has access
CO		Console Access
HE		Login Access
SL		1. View SEL, FPL, LIVE - Login rights for all partitions to which the user has access 2. View iLO 2 event log - Login rights for all partitions to which the user has access 3. View MPEL Logs - MP Configuration rights for all partitions to which the user has access 4. Clear SEL & FPL Logs - MP Configuration rights for all partitions to which the user has access
VFP		Login Access
X		Login Access
MPEL		MP Configuration Access
IO (sx2000 only)	Command Menu	Login Access
VM (sx2000 only)	Command Menu	All for all supported partitions

These access rights work in conjunction with the three different kinds of partition user support options.

Partition User Support Options

In a server that supports multiple partitions, the following options are available for partition users. A user can be configured for any of the following partition usage levels:

Single Partition Use

A user could have access to any one partition with rights defined.

Multipartition User, Same Rights

A user can have access to multiple partitions of a server but with the same rights for all the partitions.

Multipartition User, Different Rights

A user can have access to multiple partitions with different rights for all the partitions.

If a server has multiple partitions, the following rules apply for a user:

- Each user, at the time of creation, is classified either as an `all` or `#partition` user. A partition might or might not be configured in the system.
- Login rights are required for a user to login. These rights are checked before running each command to ensure that LOGIN rights are not revoked in the interim. A user with `L` rights can run all commands related to status and read-only commands.
- When a user tries to run partition-specific commands but the partition is not configured, a message appears that the partition is not configured
- Special commands such as `pe`, `ru`, and `re` require a user to have all rights to all partitions. These commands can affect cells that are considered ‘free cells’ (not associated with any partitions). Therefore, this mandate applies to users before running special commands.

- For all MP-wide commands (such as `ldap`, `lc`, and so on), a user must have corresponding rights for all partitions that the user has access to.
- When assigning rights to user logins in a multiserver environment, remember the various combinations of available rights, types of commands, and partition authority.

8 Using iLO 2

This chapter provides information on the different interfaces you can use to interact with iLO 2 such as text user interface, web GUI, and SMASH SM CLP.

Text User Interface

This section provides information on the text user interface commands you can run in iLO 2.

NOTE: HP Integrity server blades do not have fans or power supplies. Therefore, their response to certain commands are different than a rackmount server.

MP Command Interfaces

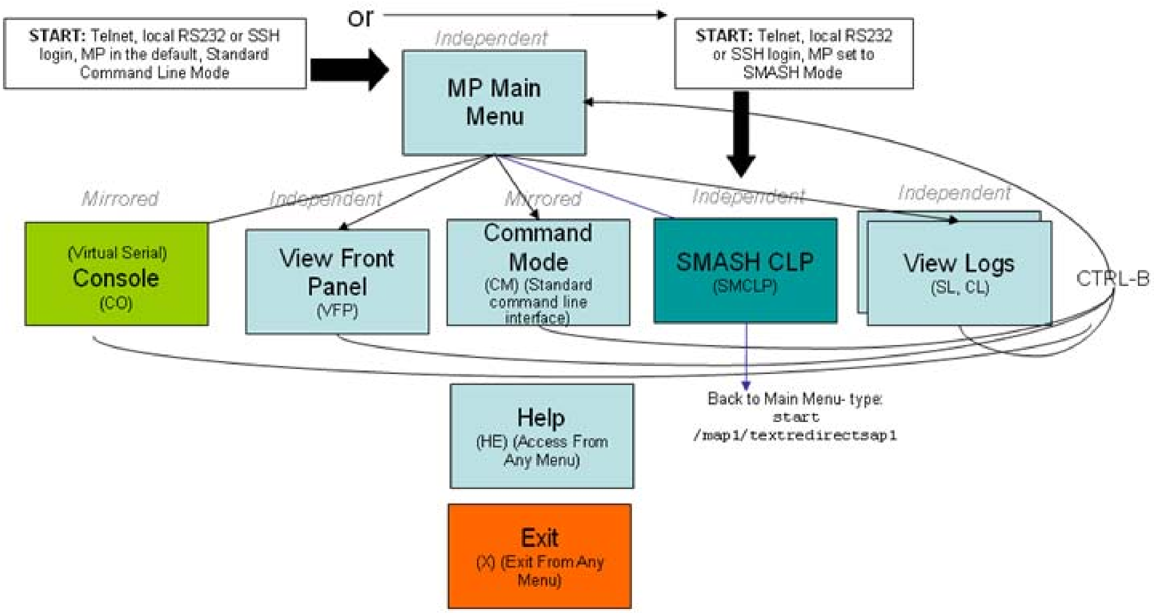
Table 22 lists and describes the available MP command interfaces.

Table 22 MP Command Interfaces

MP Command Interface	Description
MP Main Menu	The MP Main Menu appears when you first access the iLO 2 MP. The MP Main Menu supports the basic MP commands for server control and the iLO 2 MP configuration, such as setting up the iLO 2 MP LAN, retrieving events, resetting and powering on control of the server, switching to the console, and so on. You can enter the MP Main Menu commands at the `MP>` prompt.
Command Menu	The Command menu provides a set of commands that help monitor and manage the server. It switches the console terminal from the MP Main Menu to command interface mode. You can access commands that are not displayed in the MP Main Menu by entering `CM` at the MP Main Menu and entering **`HE LI`** at the `MP:CM>` prompt to get a list of the available commands.
SMASH SM CLP	The Systems Management Architecture for Server Hardware (SMASH), Server Management Command Line Protocol (SM CLP) initiative is an effort within the Distributed Management Task Force (DMTF) to standardize commands for servers. The SMASH SM CLP specifies common command line syntax and message protocol semantics for server management. **NOTE:** SMASH SM CLP commands are only available for entry class servers. For information on using SMASH SM CLP scripting commands, see Section : "SMASH Server Management Command Line Protocol" (page 141).

Figure 14 displays the MP command interface options.

Figure 14 MP Command Interfaces



START: Telnet, local RS232 or SSH login, MP in the default, Standard Command Line Mode
or
START: Telnet, local RS232 or SSH login, MP set to SMASH Mode
Independent
MP Main Menu
Mirrored
(Virtual Serial) Console (CO)
Independent
View Front Panel (VFP)
Mirrored
Command Mode (CM) (Standard command line interface)
Independent
SMASH CLP (SMCLP)
Independent
View Logs (SL, CL)
CTRL-B
Back to Main Menu- type: start /map1/textredirectsap1
Help (HE) (Access From Any Menu)
Exit (X) (Exit From Any Menu)

MP Main Menu

After logging in to the iLO 2 MP, the MP Main Menu appears. The MP Main Menu runs as a private session. Other iLO 2 users do not see the actions you perform in the private session.

Integrity iLO 2 can support multiple sessions to perform independent tasks:

- Multiple windows logged into iLO 2 to monitor VFP or study event logs in one window while administering the server from another window.
- Resetting a server from one window and monitoring the boot from another window while interacting with the console from a third window.

Table 23 lists the MP Main Menu commands.

Table 23 MP Main Menu Commands

Command	Description
`CO`	Selects console mode
`VFP`	Displays the virtual front panel
`CM`	Enters command interface mode
`SMCLP`	Accesses the SMASH SM CLP
`CL`	Views the console log
`SL`	Shows event logs
`HE`	Displays help for the menu or command
`X`	Exits

TIP: An effective method for using iLO 2 is to log in more than once with different views for each session. For instance, one window logged in viewing the console, and another viewing the virtual front panel.

MP Main Menu Commands

MP Main Menu command descriptions are listed as follows:

CO (Console): Leave the MP Main Menu and enter console mode

CO switches the console terminal from the MP Main Menu to mirrored/redirected console mode. All console output is mirrored to all users in console mode. Only one of the mirrored users at a time has write access to the console. To get console write access, press **Ctrl-Ecf**.

Press either **Ctrl-B** or **Esc** and **(** to return to the iLO 2 MP command interface. Verify that all mirrored consoles are of the same terminal type for proper operation.

To run an ASCII screen-oriented application (SAM) or a file transfer program (ftp), the console is not the recommended connection. HP recommends using the LAN and connecting directly with Telnet or the web to the system over the system LAN.

VFP (Virtual Front Panel): Simulate the display panel

VFP simulates the display panel on the front of the server. It gives realtime feedback on the results of system events and user actions. VFP works by decoding system events. It provides a live display of major states of the system, the latest system activity, and the state of front panel LEDs.

VFP shows forward progress during boot by indicating how many events have been received since the boot started and whether there have been any errors (events with alert level 3 or greater) since the last boot. To clear the yellow attention indicator on the front of the system, use the SL command and access the System Event Log (SEL).

Each user viewing VFP is in private session mode.

See also: LOC (locator LED) and, SL (show logs).

CM (Command Mode): Enter command mode

CM switches the console terminal from the MP Main Menu to mirrored command interface mode. The Command menu provides you with a set of standard command line interface commands that help monitor and manage the server.

To display the list of MP command mode commands that are not displayed in the MP Main Menu:

1. From the MP Main Menu, enter **HE**.
2. Enter **LI** after the MP HELP:> prompt.

If a command is in progress, a system status message appears.

To return to the MP Main Menu, press **CTRL-B**.

SMCLP (Server Management Command Line Protocol): Switch to the SMASH SMCLP

SMCLP switches the console terminal from the MP Main Menu to the SMASH SMCLP interface. For information on SMASH SM CLP see “SMASH Server Management Command Line Protocol” (page 141).

CL (Console Log): View the history of the console output

CL displays up to 60 KB of logged console data (about 60 pages of display in text mode) sent from the system to the console path and stored for later analysis.

Console data is stored in a buffer in nonvolatile memory. By default, data is displayed from the beginning of the buffer to end of the buffer. You can control the starting point from which the data displays and navigate through the data.

An image of the console history appears when you enter the CL command. Console output continues to be logged while this buffer is read, and nothing is lost.

SL (Show Logs): View events in the log history

SL displays the contents of the event logs that are stored in nonvolatile memory.

Events communicate system information from the source of the event to other parts of the system, then to you. Events are produced by intelligent hardware modules, the operating system, and system firmware. Events funnel into the BMC from different sources throughout the server. iLO 2 polls the BMC for new events and stores them in nonvolatile memory.

SL also displays the contents of the iLO 2 Event Log. The records the following events:

- iLO 2 MP login and logout attempts
- Command logging for specific commands
- All entries in the existing history log with more detail

Each time a user logs in or out of iLO 2, an event is logged. In the event of a login failure, an event is logged if the number of continuous login failure attempts equals the password fault value.

Command logging is run for the following commands: BP, CA, DC, DI, DNS, FW, ID, IT, LC, LDAP, LM, PC, PM, PR, RB, RS, SA, SNMP, SO, TC, UC

Events are listed as follows:

SEL: System Error Log	High-attention events and errors
FPL: Forward Progress Log	All events
Boot Log	All events between start of boot and boot complete
Previous Boot Log	The events from the previous boot

Reading the SEL is the only way to turn off the attention LED (flashing yellow light).

Table 24 lists the events and actions used to navigate within the logs.

Table 24 Events

Event	Action
+	Displays the next block (forward in time)
-	Displays the previous block (backward in time)
Enter (<CR>)	Continues to the next or previous block
D	Dumps the entire log for capture or analysis
F	Displays the first entry
L	Displays the last entry
J	Jumps to entry number
H	Displays the mode configuration (hex)
K	Displays the mode configuration (keyword)
T	Displays the view mode configuration (text)
A	Displays the alert level filter options
U	Displays the alert level unfiltered
Q	Quits and returns to the Event Log Viewer Menu
?	Displays the Help Menu
Ctrl-B	Exits and returns to the MP Main Menu

Integrity iLO 2 Event Log navigation provides additional filtering options as shown in Table 25.

Table 25 iLO 2 Event Log Filter Options

Filtering Option	Filter Criteria
N: User Login	Filter by user Login ID
P: Port Name	Filter by port name (Serial, Telnet, SSH, WEB)

Table 25 iLO 2 Event Log Filter Options *(continued)*

Filtering Option	Filter Criteria
I: IP Address	Filter by user IP Address (dotted decimal format)
M: Date	Filter by date stamp of the records entries (MM/DD/YYYY)

If you select more than one filtering option, it acts as an additional filter. For example, if you select the filtering option `N` followed by `P`, the logs displayed are the logs that satisfy the filtering criteria for options `N` and `P`.

NOTE: The iLO2 Event Logs cannot be cleared.

A finite number of records are stored. The older records are replaced as the log fills up.

Table 26 lists alert (severity) levels.

Table 26 Alert Levels

Severity	Definition
0	Minor forward progress
1	Major forward progress
2	Informational
3	Warning
5	Critical
7	Fatal

See also: DC (default configuration) and VFP (virtual front panel).

SL Command for Integrity Cell-Based Servers

`SL`: Show Logs - View the events in the log history.

`SL` displays the contents of the events that have been stored in nonvolatile memory.

Events are data items that communicate system information from the source of the event to other parts of the system, and ultimately to the system administrator. Events are produced by intelligent hardware modules, the operating system, and system firmware. Events funnel into iLO 2 from different sources throughout the server.

Events can be a result of a failure or an error (such as fan failure, machine-check, and so on). They can indicate a major change in system state (firmware boot start, system power on/off) or they might be forward progress markers, (such as CPU self test complete). Event data indicates what the event was, where it happened, and the severity of the event. The most important events are error logs (alert level 3 or higher), and major change of state logs, because they give information that can provide clues about the cause of anomalous behavior. The log viewer contains an event decoder to help you interpret events.

Table 27 lists events, actions, and functions of the logs.

Table 27 Events and Actions

Event	Action	Functions
FPL	Forward Progress Log - Stores all events of level 0 or greater	New events overwrite old FPL events once the FPL is full.
SEL	System Error Log - Stores all events of level 2 or greater	New events are not logged to the SEL when the SEL is full. Thus, it is necessary for a user or an application to periodically clear the SEL. Reading the SEL turns off the attention LED. Accessing this buffer is the only way to turn off the attention LED when it is flashing.

Table 27 Events and Actions *(continued)*

Event	Action	Functions
MPEL	MP Event Log - Stores user action events including user login	New events overwrite old MPEL events once the MPEL is full. The iLO 2 MPEL records the following events: • iLO 2 MP login, logout attempts and login failure records • MP firmware upgrade • MP firmware activate event • Console access • Clearing of logs MPEL logs cannot be cleared. Formatting options are not available for MPEL.
Live Logs	Displays events, live as they occur	The `Live Logs` feature enables you to apply a filter, and filter out logs by cell or by partition, or to view only error logs.
Clear Logs	Clears the activity and error log buffers	The `Clear Logs` command clears both the FPL and SEL. It is useful for getting a "clean log trace". A user with Console access right can view the System Event Log. Only a user with iLO Configuration access right can clear the logs. Login rights are sufficient to view the logs. But for clearing the logs, iLO Configuration rights are required for all the partitions to which user has access. But MPEL logs cannot be cleared.

Keyword Format

For the event logs, the default format is Keyword (keyword plus hex). SEL and FPL provide formatting options, the other two formats are raw hex mode and text mode. Text mode gives a multi-line display that is more readable and decodes any physical location data.

The `(D)`ump command dumps the entire log in keyword format. It is useful for capturing the log contents to a file and emailing it for analysis by support personnel.

Navigation

Navigation commands enable you to move forward or back a screen at a time, and to jump to a specific log number or to the first or last log entry.

Table 28 lists the navigation commands and their actions.

Table 28 Navigation Commands

Navigation Command	Action
D	Dump log starting at current block for capture and analysis (for SEL and FPL) Dump log starting from the beginning (for MPEL)
F	Display first (oldest) block
L	Display last (newest) block
J	Jump to specified entry and display previous block
+	Display next (forward in time) block
-	Display previous (backward in time) block
<cr>	Repeat previous +/- command
<sp>	Repeat previous +/- command
?	Display help
Ctrl-B	Exit viewer

NOTE: The MPEL log history display provides the same navigation commands as the FPL and the SEL except for the `D` command.

MPEL log navigation provides the following filtering options:

Table 29 MPEL Log Navigation Filter

MPEL Log Navigation Filter	Action
S : User Login	Filter by User Login ID
P : Login Method	Filter by User Login Method (Serial, Telnet, SSH, WEB)
I : IP Address	Filter by user IP Address (dotted decimal format)
T : Date	Filter by date stamp of the record entries (MM/DD/YYYY)
U : Unfiltered	Switch back to unfiltered state

`HE` (Help): Display help for the menu or command in the MP Main Menu

`HE` displays help for the menu or command.

- If executed from the MP Main Menu, `HE` displays general information about iLO 2, and those commands available in the MP Main Menu.
- If executed in command mode, `HE` displays a list of Command menu commands available. It also displays detailed help information in response to a topic or command at the help prompt.

`X` (Exit): Exit iLO 2

`X` exits you from the MP Main Menu. If the terminal is the local serial port, the login prompt appears. For all other types of terminals, you are disconnected from iLO 2.

Command Menu

The Command menu provides you with a set of standard command line interface commands that help monitor and manage the server.

Table 30 lists the Command menu commands.

Table 30 Command Menu Commands

Command	Description
`BP`	Resets the BMC passwords
`BLADE`	Displays blade parameters **NOTE:** This command is available only on a server blade.
`CA`	Configures asynchronous local serial port
`DATE`	Displays the current date
`DC`	Resets all parameters to default configuration
`DF`	Displays field replaceable unit (FRU) information
`DI`	Disconnects the LAN console
`DNS`	Sets the DNS configuration
`FW`	This command is only available to authorized HP service personnel
`HE`	Displays help for the menu or command
`ID`	Displays or modifies system information

Table 30 Command Menu Commands *(continued)*

Command	Description
`IT`	Modifies the iLO 2 inactivity timeouts
`LC`	Displays the LAN configuration
`LDAP`	Displays the LDAP configuration
`LM`	License management
`LOC`	Displays and configures locator LED
`LS`	Displays the LAN status
`PC`	Remote power control
`PM`	Remote power mode control
`PR`	Configures the power restore policy
`PS`	Displays the power management module status
`RB`	Resets the BMC
`RS`	Resets the system through the RST signal
`SA`	Sets access options
`SNMP`	Configures SNMP parameters
`SO`	Configures security options
`SS`	Displays system processor status
`SYSREV`	Displays all firmware revisions
`TC`	Resets through transfer of control (TOC)
`TE`	"Tell" (sends a message to other users)
`UC`	Displays a user configuration
`WHO`	Displays connected iLO 2 users
`XD`	Diagnoses or resets iLO 2

The following is a quick reference list that provides MP Command mode activities:

To access the Command menu, enter **`CM`** at the MP Main Menu.

To see all the available commands, enter **`HE LI`** at the `MP:CM>` prompt.

To access the Command menu help, enter **`HE`** at the `MP:CM>` prompt. The Command menu help provides information on all the Command menu items.

To modify the inactivity timeout, enter the **`IT`** command. The inactivity timer aborts a command if you do not complete it within a certain time period and redirects you back to the command prompt.

To abort most commands, enter **`Q`** at the point when the iLO 2 MP is asking for input.

To return to the MP Main Menu from any of these commands, press **`Ctrl-B`**.

Command Line Interface Scripting

A command line interface is provided for all commands to assist you in scripting. This section provides syntax examples used in the iLO 2 MP command-line or scripted interface.

Typically, tools like Expect (see "Expect Script Example" (page 83)) and (http://expect.nist.gov/) are used to string together several commands to accomplish a task. These scripting tools enable you to write a script for one iLO 2, and use it to apply the same commands to additional iLO 2s. Scripting tools have capabilities that enable you to do the following:

- Write scripts that make decisions based on the output of commands
- Use variables in the script to customize it for each target automatically
- Compensate for delays in output

Scripting tools and the command-line interfaces enable you to carry out commands to multiple iLO 2s such as setting the IP address on 10 iLO 2s pulled from a list of 10 IP addresses read from a file local to your script. To automatically administer any part of the system during any stage of its operation, you can use the scripting tool to log in to iLO 2, access the console, and send and receive commands in EFI or the OS.

NOTE: This guide is not meant as a substitute for instruction on various scripting tools that are available for automating command-line interfaces. The iLO 2 MP TUI (when used with command-line arguments) and the SMASH command-line interface were created with these types of scripting tools in mind to facilitate powerful automation capabilities.

Expect Script Example

The following provides a simple Expect script example with no timeouts and no error checking using Telnet instead of SSH.

```
#!/usr/local/bin/expect -f
#
# (Portions of) this Expect script (were) was generated by autoexpect on
#     Tue Nov 21 08:45:11 2006
# Expect and autoexpect were both written by Don Libes, NIST.
#
# Note that autoexpect does not guarantee a working script.  It
# necessarily has to guess about certain things.  Two reasons a script
# might fail are:
#
# 1) timing - A surprising number of programs (rn, ksh, zsh, telnet,
# etc.) and devices discard or ignore keystrokes that arrive "too
# quickly" after prompts.  If you find your new script hanging up at
# one spot, try adding a short sleep just before the previous send.
# Setting "force_conservative" to 1 (see below) makes Expect do this
# automatically - pausing briefly before sending each character.  This
# pacifies every program I know of.  The -c flag makes the script do
# this in the first place.  The -C flag allows you to define a
# character to toggle this mode off and on.

set force_conservative 0  ;# set to 1 to force conservative mode even if
     ;# script wasn't run conservatively originally
if {$force_conservative} {
        set send_slow {1 .1}
        proc send {ignore arg} {
               sleep .1
               exp_send -s -- $arg
 }
}

#2) differing output - Some programs produce different output each time
# they run.  The "date" command is an obvious example.  Another is
# ftp, if it produces throughput statistics at the end of a file
# transfer.  If this causes a problem, delete these patterns or replace
# them with wildcards.  An alternative is to use the -p flag (for
# "prompt") which makes Expect only look for the last line of output
# (i.e., the prompt).  The -P flag allows you to define a character to
# toggle this mode off and on.
#
# Read the man page for more info.
```

```
#
# -Don
#
# (End of auto-expect generated content)

#######################################################################

# USER
set mp_user "Admin"

# PASSWORD- get password from terminal instead of storing it in the script
stty -echo
send_user "For user $mp_user\n"
send_user "Password: "
expect_user -re "(.*)\n"
set mp_password $expect_out(1,string)
stty echo

# Other Constants
set timeout 20

########################################################################
## BEGIN
##
spawn $env(SHELL)
match_max 100000

#foreach mp_name {puma_mp lion_mp cougar_mp} {
set mp_name "puma_mp"

  send_user "\n\n----- $mp_name -----\n\n"
  # Frequently used Strings
  set MA_PROMPT "$mp_name\] MP> $"
  set CM_PROMPT "$mp_name\] MP:CM> $"

  # Expect the UNIX prompt...
  #expect "-> $"

  #### Log into the MP  #####
  send -- "telnet $mp_name\r"
  expect ".*MP login: $"
  send -- "$mp_user\r"
  expect "MP password: $"
  send -- "$mp_password\r"

  expect "$MA_PROMPT"
#Run SL command to dump logs
  #send "sl -forward -view text -nc\r"
  send -- "cm\r"

  expect "$CM_PROMPT"

#Run PC command to power on the system
  send -- "pc -on -nc\r"
  expect "$CM_PROMPT"

  send "ma\r"
  expect "$MA_PROMPT"
  send "x\r"

#}

expect eof
```

Command Menu Commands and Standard Command Line Scripting Syntax

The following list of commands is provided to help you learn about the Command menu commands. Command-line interface scripting syntax for each command is provided to help you accomplish a scripting task. The following rules apply to scripting syntax:

- The `-nc` (no confirmation) is optional. This special keyword designates that no user confirmation is required to execute the command. If you enter **`-nc`** at the end of the command line, the command is executed without asking you for user input. Without the `-nc` option, you are asked to confirm the changes. The only exception to this rule is when a password must be entered. In that case, you are prompted for a password separately. However, commands that require a password can have that password entered on the command line (`FW`, `UC`).

  If `-nc` is specified on a command with no other parameters or with only a specific multilevel selector, the command displays all or just the specific multilevel parameters. The absence of a specific multilevel parameter on a command that has multilevels causes *all* the multilevel parameters to display.
- Most commands accept `-all default`. This causes all parameters for that command to be set to their default values.
- In some multilevel commands, you can use `default` to set that level to its default values.
- Further use of `default` on many individual parameters causes that parameter to be set to its default value.
- `-?` (MP command-specific help) is optional. If you enter **`-?`** by itself with the command, a usage display appears. In the event of an incorrect command line usage, in addition to the the error message, the usage display appears.
- Arguments in brackets `[ ]` are optional.
- Without arguments, the system prompts you for answers to questions.
- Entering a command without parameters takes you through the command interactively and prompts you for all the options.

BP: Reset BMC passwords

Command access level: MP configuration access

`BP` resets the passwords that control the interface between the SFW and the BMC.

NOTE: The passwords that control the interface between the SFW and the BMC have nothing to do with the MP login/passwords.

Setting these passwords at EFI, enables you to restrict access to various information. To clear these passwords, use the `BP` command.

Command line usage and scripting:

```
BP  [ -nc ]
      -?
```

See also: `DC, RB, UC`

`BLADE`: Display BLADE parameters

NOTE: This command is available only on a server blade.

Command access level: Login access

`BLADE` facilitates the cabling and initial installation of HP Integrity server blades. It also provides a quick view of the enclosure status. You must have configuration access right to turn the enclosure locator UID LED on or off.

Onboard Administrator Configuration

OA IP Address IP address of the OA.

OA MAC Address MAC address of the OA.

Server Blade Configuration

Rack Name Logically groups together enclosures in a rack. The rack name is shared with the other enclosures in the rack.

Rack UID Rack unique identifier.

Bay Number The blade enclosure can support up to eight HP Integrity server blades. When viewed from the rack front, the bays are numbered from left to right, from 1 to 8. The bay number is used to locate and identify a blade.

Enclosure Information

Enclosure Name Logically groups together the server blades installed in the same enclosure. The enclosure name is shared with the other server blades in the enclosure.

Health Indicates one of three states of health of this enclosure.

OK Normal operation, any issues have been acknowledged.

Degraded Typically loss of redundancy or partial failure of a component.

Critical Failure with loss or imminent loss of system function.

Command line usage and scripting:

```
  BLADE  [ -nc ]
  blade -?
```

Example of the `BLADE` Command With Output

```
[gstlhpg1] MP:CM> blade

BLADE

Onboard Administrator Information:
     IP Address             : 192.0.2.1
     MAC Address            : 0x00xxxxxexxbb


Server Blade Information:
    Rack name               : RACK
    Rack UID                : 000z00xx0000
    Bay Number              : 3

Enclosure Information:
    Enclosure name          : encl
    Health                  : OK

-> Command successful.

[gstlhpg1] MP:CM>
```

CA: Configure asynchronous local serial port

Command access level: MP configuration access

CA sets the parameters for the local and the remote serial console. Input and output data rates are the same. The value returned by the `stty` command on HP-UX is the local serial port console speed.

Set up the local serial port parameters as follows:

BAUD RATES Input and output data rates are the same. Possible values are as follows: 4800, 9600, 19200, 38400, 115200 bit/sec.

FLOW CONTROL Hardware uses RTS/CTS; software uses Xon/Xoff.

For HP Integrity server blades, the CA command also provides an option to change between the Integrity iLO mode or the dedicated AUX UART mode. Switching to AUX UART mode when MP remote access is disabled or LAN parameters are not configured requires a push button reset to change back to iLO MP mode.

NOTE: Inconsistent bit rate settings can result in improper MP UI while switching between these modes.

The operation mode settings are saved on the MP NVRAM and are permanent for reset and firmware upgrade of iLO 2, but the settings are not permanent for power cycles or blade ejection. For power cycle to the blade, the console serial port is set back to the iLO mode.

If you cannot access iLO 2 through Telnet and the port mode of operation is AUX UART, you must change the port operation mode to Integrity iLO mode to access the MP through the serial port. To change the port operation mode to iLO, perform a hard reset to the MP by pushing the recessed push button through a hole in the front panel. The hard reset resets the MP hardware and sets the MP to the default settings. The hard reset returns the port default connection to MP.

NOTE: Both short and long reset button presses return the port default connection to the MP.

The iLO 2 mirrors the system console to the iLO 2 MP local and LAN ports. One console output stream is reflected to all connected console users. If several different terminal types are used simultaneously, some users can see unexpected results.

Command line usage and scripting:

```
CA  [ -local ] [ -bit <n> ] [ -flow >software|hardware> ] ] [ -nc ]
      -?
```

Server blade usage

```
CA  [ -local ] [ -bit <n> ] [ -flow >software|hardware> ]
               [ -mode ,aux|ilo> ] ] [ -nc ]
      -?
```

See also: SA

DATE: Display date

Command access level: Login access

DATE displays the date, as best known to iLO 2. The iLO 2 clock is updated from the BMC/SFW and cannot be modified. The realtime clock is used only when iLO 2 is first powered on or rebooted, until it can obtain the correct date from the BMC.

Command line usage and scripting:

```
DATE  [ -nc ]
      -?
```

DC (Default Configuration): Reset all parameters to default configurations

Command access level: MP configuration access

DC sets all iLO 2 parameters back to their default values. To restore specific configurations to their default values, use the following commands:

```
MP IP configuration                              : LC -all DEFAULT
Remote Access Configuration                      : SA -all DEFAULT
Command Interface configuration                  : IT -all DEFAULT
MP Security configuration                        : SO -opt DEFAULT
MP Session configuration                         : IT -all DEFAULT
MP User configuration                            : UC -all DEFAULT
MP LDAP directory configuration                  : LDAP -all DEFAULT
SNMP Configuration                               : SNMP - all DEFAULT
```

Use any of the following methods to reset passwords in iLO 2:

- In the UC command, change individual users or reset all users to default values.
- Reset passwords by pressing the MP reset button on the back panel of your HP server for longer than four seconds. After iLO 2 reboots, the local console terminal displays a message for five seconds. Responding to this message in time enables a local user to reset the passwords.

  NOTE: All user information (logins, passwords, and so on) is erased when you use any of the previous reset methods.

Command line usage and scripting:

```
DC  [ -all default [ -nc ] ]
      -?
```

DF: Display FRU information

Command access level: Login access

DF displays FRU information for FRU devices located behind the BMC. Information provided includes serial number, part number, model designation, name and version number, and manufacturer.

Command line usage and scripting:

```
DF [ -specific[ <fruid> ] | -all ] [ -view <text|hex> ] [ -nc ]
      -?
```

DI: Disconnect LAN, WEB, SSH, or Console

Command access level: MP configuration access

DI disconnects LAN, web SSL, or SSH users from iLO 2. It does not disable the ports. To disable the ports, see the SA command for LAN/WEB/SSH/IPMI over LAN access. Use the TE and WHO commands to identify the connected users before running this command.

Command line usage and scripting:

```
DI [ -telnet] [ –web ] [ -ssh ] [ -nc ]
      -?
```

See also: EX, SA, TE, WHO

DNS: DNS settings

Command access level: MP configuration access

DNS configures the DNS domain name and up to three DNS servers either manually or automatically with DHCP. You can use this command only with DHCP enabled. You can also perform a DDNS update through the primary DNS server as long as it is authoritative for the zone.

If no DNS server IP addresses are specified, or the DNS domain is undefined, DNS is not used.

If an IP address was obtained through DHCP, an add name request is sent to the DDNS server if it is enabled and registered.

Command line usage and scripting:

```
DNS [ [ -server <e|d> ] [ -domain <text> ] [ -name <e|d> ]
      [ -register <y|n> ] [ -1ip <ipaddr> ] [ -2ip <ipaddr> ]
      [ -3ip <ipaddr> ] ] | [ -all default ] [ -nc ]
      -?
```

See also: LC

FW: Upgrade the MP firmware

This command is only available to authorized HP service personnel.

The MP firmware is packaged along with system, BMC, and FPGA/PSOC firmware. You can download and upgrade the firmware package from the HP website at http://www.hp.com/go/bizsupport.

IMPORTANT: When performing a firmware upgrade that contains system programmable hardware, you must properly shut down any OS that is running before starting the firmware upgrade process.

Select **Download drivers and software**, select your server, and follow the directions provided.

After the upgrade, reconnect and log in as user **Admin** and password **Admin** (case sensitive).

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

HE: Display help for menu or command in command menu interface

Command access level: Login access

HE displays help for a menu or command.

- If executed from the MP Main Menu, HE displays general information about iLO 2 and those commands available in the MP Main Menu.
- If executed in command mode, HE displays the MP Help: Command Menu List. HE also displays detailed help information in response to a topic or command at the help prompt.

Command line usage and scripting:

```
HE [ -topic | command ] [ -nc ]
      -?
```

ID: System information settings

Command access level: MP configuration access

ID displays and modifies the following:

SNMP contact person	Name, telephone, email, and pager number.
Server information	Location, rack ID, position, asset tag.
System host name	The system host name of the operating system.

NOTE: The system host name information is not retained across iLO 2 reboots.

Command line usage and scripting:

```
ID [ { -host [ <text> ] }
   | { -person [ -name <text> ] [ -telephone <text> ]
     [ -email <text> ] [-pager <text> ] }
   | { -server [ -location <text> ] [ -rackid <text> ]
     [ -position <text> ] } ]
     [ -tag <text> } ] [ -nc ]
      -?
```

IT: Inactivity timeout settings

Command access level: MP configuration access

IT prevents sessions on the system from being inadvertently left open. When you initiate an iLO 2 MP command, other users are prohibited from running any commands until the first command has been completed or until it times out. Command interface inactivity timeout specifies that timeout value. This prevents a user from inadvertently keeping iLO 2 locked in a command, preventing other users from running iLO 2 MP commands.

The inactivity timeout effects how long a user can stay inactive within a command in the text user interface before they are placed back at the command prompt. There is no session timeout on the Integrity iLO 2 text interfaces.

NOTE: The iLO 2 MP command interface inactivity timeout cannot be deactivated.

Use the flow control timeout to prevent any user who is using a terminal that does not obey flow control from locking the system out from other users.

The following are IT command parameters:

iLO 2 inactivity timeout	One to 30 minutes (default is three minutes).
Flow control timeout	Zero to 60 minutes. If the flow control timeout is set to zero, no timeout is applied. A mirroring flow control condition ceases when no flow control condition exists on any port. This timeout prevents mirrored flow control from blocking other ports when inactive.

Command line usage and scripting:

```
IT [ -command <n> ] [ -flow <n> ] [ -nc ]
     -?
```

See also: SA

LC: LAN configuration usage

Command access level: MP configuration access

LC modifies the LAN configuration parameters.

IMPORTANT: If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 2 automatically resets once you confirm the change.

If you are connected through a serial console and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 2 alerts you to manually reset iLO 2.

Configurable parameters include the following:

- iLO 2 MP IP address
- DHCP status (default is enabled)
  - If the IP address, gateway IP address, or subnet mask was obtained through DHCP, you cannot change the DHCP status without first disabling DHCP.
  - If you change the DHCP status to enabled or disabled, the IP address, subnet mask, and gateway address are set to their default values (127.0.0.1:0xffffff00), and the DNS parameters are voided.
  - When you change the DHCP status from enabled to disabled, the DNS parameters for DHCP are set to disabled, and the Register with DDNS parameter is set to No.
  - When you change the DHCP status from disabled to enabled, the DNS parameters for DHCP are set to enabled, and the Register with DDNS parameter is set to Yes.

- iLO 2 MP host name
  - The iLO 2 MP host name set in this command is displayed at the iLO 2 MP command mode prompt. Its primary purpose is to identify the iLO 2 MP LAN interface in a DNS database.
  - If you change the iLO 2 MP host name and the IP address was obtained through DHCP and DDNS is registered, a *delete old name request for the old host name* and an *add name request for the new host name* are sent to the DDNS server.
  - Typically you enter the DNS name for the LAN IP. You can program this field to any useful name or phrase. For clarity, enter **`MPNAME-on-SYSTEM`** as the MP Host name, so both names show up in the prompt. The limit is 19 characters, and no spaces are allowed.
- Subnet mask
- Gateway IP address
- Local console serial port
- Link state
- SSH access port number

Command line usage and scripting:

```
LC [ -ip <ipaddr> ] [ -subnet <subnet> ] [ -gateway <ipaddr> ]
   [ -host <text> ] [ -web <n> ] [ -link <auto|T<10baseT)> ]
   [ -ssh <n> ] [ -dhcp <e|d> ] [ -nc ]
      -?
```

See also: `DNS, LS, SA`

`LDAP`: LDAP directory settings

Command access level: MP configuration access

`LDAP` displays and modifies the following LDAP directory settings:

- Directory Authentication: Activates or deactivates directory support on iLO 2.
  - Enable with Extended Schema: Selects directory authentication and authorization using directory objects created with the HP schema. Select this option if the directory server is extended with the HP schema and you plan to use it.
  - Enable with Default Schema: Selects directory authentication and authorization using user accounts in the directory which has not been extended with the HP schema. User accounts and group memberships are used to authenticate and authorize users. Data in the Group Administration page must be configured after you select this option. In the Group Administration page, configure one or more directory groups by entering the distinguished name of the group and privileges to be granted to users who are members of that group.
  - Disable: Deactivates directory support on iLO 2.
- Local User Accounts: Includes or excludes access to local iLO 2 user accounts. If local user accounts are enabled, you can log in to iLO 2 using locally stored user credentials. If they are disabled, access is limited to valid directory credentials only.

  NOTE: Locally stored user accounts can be active while directory support is enabled. This enables both local- and directory-based user access. If both directory authentication and local user accounts are enabled, login is attempted using the directory first, then using local accounts.

- Directory Server IP Address: IP address or host name of the directory server.

- Directory Server LDAP Port: Port number for the secure LDAP service on the server. The default value for this port is 636.
- Distinguished Name: Specifies where this iLO 2 instance is listed in the directory tree. For example: `cn=MP Server,ou=Management Devices,o=hp`
- User Search Contexts (1,2,3): User name contexts that are applied to the login name entered to access iLO 2.

  User name contexts are used to locate an object in the tree structure of the directory server and applied to the login name entered to access iLO 2. All objects listed in the directory can be identified using their unique distinguished name. However, distinguished names can be long, users might not know their distinguished names, or they might have accounts in different directory contexts. Search contexts enables users to specify common directory contexts, so that they do not have to enter their full distinguished name at login. iLO 2 attempts to authenticate a user in the directory first by the login name entered, and then by applying user search contexts to that login name until login succeeds. For example:

  Instead of logging in as `cn=user,ou=engineering,o=hp`, search context of `ou=engineering,o=hp` enables a user to log in as `user`

  When extended schema is selected and Active Directory is used as a directory server. Microsoft Active Directory has an alternate user credential format. A user can log in as: `user@domain.hp.com`, in which case a search context of `@domain.hp.com` enables the user to login as `user`.

  NOTE: For instances when user authentication uses the LDAP directory server that is configured for Microsoft Active Directory, a user can log in using the username format `user@domain.hp.com`. Currently, this user credential format is only supported on Internet Explorer.

Command line usage and scripting:

```
LDAP [ -directory [ -ldap <d|x|s> ] [ -mp <e|d>]
                  [ -ip <hostname/ipaddr> ] [ -port <n>]
                  [ -dn <text> ] [ -1context <test>]
                  [ -2context <text>] [ -3context <text>]
     | -groups    [ -change <groupNo.> [ -dn <text>]
                  [ rights <e|d>]
                         <console|mp|power|user|virtual|all|none> ]
                  [ -list <groupNo.> ]]
     | -nc ]
       -?
```

See also: `LOGIN, US`

LDAP: LDAP group administration

`LDAP` enters one or more directory groups by specifying the distinguished name of the group and privileges to be granted to users who are members of that group.

You must configure group administration information when the directory is enabled with the default schema.

The group administration section of the LDAP command enables users to enter one or more directory groups by specifying the distinguished name of the group and privileges to be granted to users who are members of that group.

When a user attempts to log in to iLO 2, iLO 2 reads that user’s directory name in the directory to determine which groups the user is a member of. iLO 2 compares this information with a list of configured groups. The rights of all the matched groups are combined and assigned to that user.

LDAP: Schema-Free LDAP

Schema-Free LDAP enables you to use directory authentication for logging in to iLO 2 without having to do any schema extension on the directory server or snap-in installation on the client.

For information on schema-free LDAP, see “Configuring Schema-Free LDAP” (page 67).

LM: License management

Command access level: MP configuration access

LM displays your current license status. Use it to enter a license key to enable the Advanced Pack license features.

Command line usage and scripting:

```
LM [ -key <license key> ] [ -nc ]
     -?
```

LOC: Locator UID LED configuration

Command access level: MP configuration access

LOC displays the current status of the locator UID LED and enables you to turn the locator UID LED on or off.

In HP Integrity server blades, this command also enables you to turn the enclosure locator UID LED on or off. The UID LED physically identifies the blade in a data center environment. It emits a blue light when turned on. It does not have an associated button. You can control the UID LED from the BMC only.

Command line usage and scripting:

```
LOC [ -on | -off  [ -nc ] ]
     -?
```

Server blade usage

```
LOC [ -server <on | off> ] [-enclosure <on | -off>]  [ -nc ]
     -?
```

LS: LAN status

Command access level: Login access

LS displays all parameters and the current status of the iLO 2 MP LAN connections. The LAN parameters are not modified by this command.

Command line usage and scripting:

```
LS [ -nc ]
     -?
```

See also: DNS, LC, SA

PC: Power control access

Command access level: Power control access

PC enables control of the power management module. It provides the following options for remote control of system power:

ON — Turns the system power on. This command has no affect if the power is already on.

OFF — Turns the system power off. This command is equivalent to turning the system power off at the front panel switch. There is no signal sent to the OS to shut the software down before power is turned off. To turn the system off gracefully, ensure that the OS is shut down before running this command.

`CYCLE` Turns the system power off, then on. The delay between off and on is 30 seconds.

`Graceful Shutdown` The BMC sends a signal to the OS to shut down prior to turning off the system power.

Command line usage and scripting:

```
  PC [ -on | -off | -graceful | -cycle ] [ -nc ]
      -?
```

Example:

```
[gstlhpg1] MP:CM> pc -on -nc

PC -on -nc

System will be powered on.

   -> System is being powered on.

-> Command successful.

[gstlhpg1] MP:CM>
```

See also: `PR, PS`

PM: Power regulator mode

Command access level: Power control access

`PM` provides the following options for remote control of the system power regulator:

Dynamic Enables the system to dynamically change the processor power level when needed based on current operating conditions. The system remains in this mode unless the system is reset or an OS-hosted application requests a processor state change. In these cases, power management mode changes to OS Control Mode.

Low Sets the processor to the lowest supported processor state and forces it to stay in that lowest state until the system is reset. If the processor is reset, the power mode changes to OS Control Mode.

High Sets the processor to the highest supported processor state and forces it to stay in that highest state unless the system is reset or an OS- hosted application requests a state change. If the processor is reset, the power mode changes to OS Control Mode.

OS Sets the control of the power regulator to the OS.

Command line usage and scripting

Example

```
[gstl0074] MP:CM> pm
  PM [ -dynamic | -low | -high | -os ] [ -nc ]
        PM -?
[gstl0074] MP:CM> pm

PM

Current System Power Mode   : Dynamic Mode

Power Regulator Menu:
     D - Dynamic Power Savings Mode
     L - Static Low Power Mode
     H - Static High Performance Mode
     O - OS Control Mode

Enter menu item or [Q] to Quit: O
O
```

```
Power mode will be set to OS Control.
   Confirm? (Y/[N]): y
y

   Please wait ..

   -> Power mode has been successfully changed
```

See also: PC, PR

PR: Power restore policy configuration

Command access level: MP configuration access

PR configures the power restore policy. The power restore policy determines how the system behaves when AC power returns after an AC power loss.

- If PR is set to On, the system powers on after AC is applied.
- If PR is set to Off, the system stays powered off after AC is applied. Push the system power button or run the PC command to power on the system.
- If PR is set to Previous, the power is restored to the state that was in effect when the AC power was removed or lost.

Command line usage and scripting:

```
PR [ -on | -off | -previous ] [ -nc ]
     -?
```

See also: PC

PS: Power status

Command access level: Login access

PS displays the system power state, the temperature, and status of the power supplies and fans. You can obtain an instant power reading without a license key using this command.

Command line usage and scripting:

```
PS [ -nc ]
     -?
```

See also: PC, SS

RB: Reset BMC

Command access level: MP configuration access

RB resets the BMC by toggling the GPIO BMC reset line.

Command line usage and scripting:

```
RB [ -nc ]
     -?
```

See also: PC, SS

RS: Reset system through the RST signal

Command access level: Power control access

IMPORTANT: During normal system operation, shut down the OS before issuing the RS command.

RS resets the system (except iLO 2) through the RST signal.

Running this command irrecoverably halts all system processing and I/O activity and restarts the system. The effect of this command is similar to cycling the system power. The OS is not notified, no dump is taken as the system shuts down, and so on.

Command line usage and scripting:

```
RS [ -nc ]
    -?
```

See also: TC

SA: Set access LAN/WEB/SSH/IPMI over LAN ports

Command access level: MP configuration access

SA sets access permissions for users logging in to iLO 2 over the LAN. You can set iLO 2 to allow Telnet access, web access, SSH, IPMI over LAN, or all four.

There is no capability to manage the IPMI user name or password in iLO 2. There is only the ability to enable or disable access with IPMI through the SA command.

If LAN or web users are connected when a disable from this command runs, they are disconnected. Any future incoming connection request to the corresponding port is rejected.

Command line usage and scripting:

```
SA [ -telnet <e|d> ] [ -web <e|d> ] [ -ssh <e|d> ]
   [ -lanipmi <e|d> ] [ -command <mpmenu|smclp> ] [ -nc ]
      -?
```

SNMP: Configure SNMP parameters

Command access level: MP configuration access

⚠ **WARNING!** Until it is completely booted, iLO 2 does not send out SNMP trap information. If the SNMP traps are enabled and if an MP reset occurs, iLO 2 cannot send SNMP trap information from the start of the reset.

SNMP performs the following actions:

- Enable or disable the SNMP server. Disabling the SNMP server prevents all access to the SNMP management information base (MIB) objects and also prevents sending of any SNMP alerts.
- Enable or disable the SNMP alerts feature separate from the general SNMP server.
- Configure up to four destination IP addresses where SNMP alerts will be sent. Alerts are sent by iLO 2 to these destinations for power shutdown, system reset, and system fatal error events.
- Configure the community string, thereby securing the access to the MIB objects.

To configure SNMP parameters:

1. At the MP:CM> prompt, enter **SNMP**.
2. To change the SNMP status, enter **N**. Enabled is the default.
3. Enter **E** to enable or **D** to disable all SNMP access. The screen displays the new SNMP configuration settings.
4. To change the SNMP alert status, enter **T**. Disabled is the default.
5. Enter **E** to enable or **D** to disable all SNMP alerts. The screen displays the new SNMP configuration settings.
6. To configure a destination IP address for SNMP alerts, enter **1 2 3 4**. The default is blank (unused).
7. To configure the community string to secure the access to the MIB objects, enter **C**. The default is public.

Command line usage and scripting

```
SNMP [ -status <e|d> ] [ -community [ <text> ] ] [ -nc ]
      -?
```

Command line usage and scripting for server blades:

```
SA [ -status <e|d> ] [ -community [ <text> ] ] [ -traps <e|d> ]
   [ -1dest <ipaddr> ] [ -2dest <ipaddr> ] [ -3dest <ipaddr> ]
```

```
      [ -4dest <ipaddr> ] [ -nc ]
         -?
```

See also: ID

SO: Security option help

Command access level: MP configuration access

SO modifies the security option of iLO 2 (login timeouts, password faulty, SSL certificate generation, SSH keys).

The following are SO command parameters:

- Login timeout: Zero to five minutes. This is the maximum time allowed to enter login name and password after the connection is established. The connection is interrupted when the timeout value is reached. The local console restarts the login; for all other terminal types, the connection is closed. A timeout value of 0 means there is no timeout set for the login.

  The login timeout and the timeout value is effective on all ports including the local port. However, the local port cannot be disconnected like other ports on login timeout. For example, if a local port user sits at the MP Login: prompt, nothing happens even if a timeout occurs. But, if a local port user enters a login name, sits at the MP Password: prompt, and if a timeout occurs at this stage, this login is cancelled and the MP Login: prompt reappears.
- Number of password faults allowed: 1 to 10. This parameter defines the number of times a user can attempt to log in to a console before being rejected and having its connection closed.
- SSL certificate: Enables the generation of SSL certificates.
- SSH keys generation: Enables SSH keys authorization.
- iLO 2 reset: Enables an iLO 2 reset through IPMI from BMC, system, or IPMI over LAN.
- iLO 2 password reset: Enables iLO 2 password reset through IPMI from BMC, system, or IPMI over LAN.

Command line usage and scripting:

```
SO   [ { -options [ -login <n> ] [ -number <n> ] [ -fwpci <e|d> ]
                  [ -reset <e|d> ] [ -pwdreset <e|d> ] }
     | { -ss1 [ -name <text> ] [ -organization <text>] [ -unit <text> ]
              [ country <text> ] [ -region <text> ] [ -locality <text> ]
              [ -email <text> ] }
     | { -ssh } ] [-nc ]
       -?
```

SS: System Status

Command access level: Login access

SS displays the status of the system processors and which processor is the monarch.

The iLO 2 learns the system configuration through the events it receives from the system. There is usually a delay between any processor configuration change and what is displayed by this command. For the most up-to-date processor configuration information, use the EFI or BCH prompt.

Command line usage and scripting:

```
SS [ -nc ]
     -?
```

See also: PS

SYSREV: Firmware revisions

Command access level: Login access

SYSREV displays the current firmware revisions in the system.

Command line usage and scripting:

```
  SYSREV [ -nc ]
           -?
```

Example:

```
MP:CM> SYSREV

Current firmware revisions
MP  FW     : F.01.57
BMC FW     : 75.12
EFI FW     : ROM A 05.63, ROM B 05.60
System FW : 01.40
PDH FW     : 00.0d
UCIO FW    : 03.0a
PRS FW     : 00.08 UpSeqRev: 01, DownSeqRev: 01
```

TC: System reset through INIT or TOC signal

Command access level: MP configuration access

NOTE: During normal operation, shut down the OS before issuing this command.

TC resets the system through the INIT or TOC signal. Running this command irrecoverably halts all system processing and I/O activity and restarts the computer system. It is different from the RS command in that the processors are signaled to dump state as they shut down.

Command line usage and scripting:

```
  TC [ -nc ]
       -?
```

See also: RS

TE: Send a message to other mirroring terminals

Command access level: MP configuration access

TE treats all displayable characters following the command as a comment. Characters typed are broadcast to the connected console clients when you press **Enter**. The string size is limited to 80 characters. Any extra characters are not broadcast to other console clients.

NOTE: The broadcast message is sent only to Command menu clients, and does not include users connected to MP Main Menu functions.

Command line usage and scripting:

```
  TE <text> [ -nc ]
       -?
```

UC: User Configuration (users, passwords, and so on)

Command access level: User administration access

UC adds, modifies, re-enables, or deletes any of the following user parameters:

- Login ID
- Password
- User Name
- User Workgroup
- User Access Rights
- User Operating Mode
- User Enabled

There are two default users, `Admin` and `Oper`. The `Admin` user has all rights `(C, P, M, U, and V)`. The `Oper` user has the console access right by default. You can change the configuration of these default users with the `UC` command.

All users have the right to log in to iLO 2 and to run Status (read-only) commands (view event logs, check system status, power status, and so on), but not to run any commands that alter the state of iLO 2 or the system.

The following commands are available to all users: `CL`, `DATE`, `DF`, `HE`, `LS`, `PS`, `SL`, `SS`, `SYSREV`, `TE`, `VFP`, `WHO`, `XD` (status options)

An iLO 2 user can also have any or all of the following access rights:

Console Access

Right to access the system console (the host OS). This does not bypass host authentication requirements, if any.

Command: `CO`

Power Control Access

Right to power on, power off, or reset the server, and to configure the power restore policy.

Commands: `PC`,`PR`, `RS`, `TC`

Local User Administration Access

Right to configure locally stored user accounts.

Commands: `UC`

MP Configuration Access

Right to configure all iLO 2 MP settings (and some system settings, such as the power restore policy).

Commands: `BP`, `CA`, `CL`, `DC`, `DI`, `FW`, `ID`, `IT`, `LC`, `LDAP`, `LOC`, `PG`, `RB`, `SA`, `SO`, `XD`

Virtual Media Access

Enables Advanced Pack license users the right to use the vMedia applet.

NOTE: The vMedia feature is available only if you have the iLO 2 Advanced Pack license and the user vMedia access right.

Command line usage and scripting:

```
  UC [ -new <login> –user <text> [ -workgroup <text> ]
     [ -rights <e|d> <console|mp|power|user|virtual|all|none> ]
     [ -mode <single|multiple> ] [ -enable <e|d> ]
     [ -password <value> ] ]
     [ -change <login> [-login<newlogin> ] [ -user <text> ]
     [ -rights <e|d> <console|mp|power|user|virtual|all|none> ]
     [ -workgroup <text> ] [ -mode <single|multiple> ]
     [ -enable <e|d> \ [ -password [ <value> ]
     [ -delete <login> ] | [ -list <login> ] ] [ -nc ]
       -?
```

Example:

```
[gstlhpg1] MP:CM> uc -delete Oper -nc

UC -delete Oper -nc


Current User Parameters:
     User Login ID         : Oper
     User Password         : ************
     User Name             : Default Operator
     User Workgroup        :
     User Access Rights    : Console access, Virtual Media
     User Operating Mode   : Multiple
     User Enabled/Disabled : Enabled
```

```
   -> Current User will be deleted

User may be disconnected in this process

   -> User Configuration has been updated.

-> Command successful.

[gstlhpg1] MP:CM>
```

See also: `CA, SO, LDAP`

`WHO`: Display a list of iLO 2 connected users

Command access level: Login access

`WHO` displays the login name of the connected console client users, the ports on which they are connected, and the mode used for the connection.

- Login name
- Login type (LDAP or local authentication)
- User access rights
- Connection port (local, remote, Telnet, web, SSH)
- IP address (for Telnet, web, SSH)
- Current MP mode that user is in (MA-MP Main Menu, CM-Command menu, LIVE-live event viewer, VFP-VFP mode)

For LAN and serial console clients, the command displays the IP address. When DNS is integrated, the host name appears as well.

The local port now requires a login. A user must be logged into the system, or no local port displays.

Command line usage and scripting:

```
WHO [ -nc ]
      -?
```

See also: `DI, TE`

`XD`: iLO 2 Diagnostics or reset

Command access level: MP configuration access for resetting the iLO 2, console access for all other `XD` options

`XD` performs simple checks to confirm the iLO 2 health and its connectivity status. The following tests are available:

- iLO 2 Parameter Checksum in NVRAM
- Verify I2C connection (get BMC device ID)
- LAN connectivity test using the `ping` command

You can use the `XD` command plus its `R` command option to reset iLO 2. You can safely perform an iLO 2 reset without affecting the operation of the server.

You can also reset iLO 2 through the web interface or by pressing the MP reset button.

Command line usage and scripting:

```
XD [ -parameter | -i2c |-lan <ipaddr> | -reset ] [ -nc ]
     -?
```

Web GUI

This section describes the functions and features of the web graphical user interface (GUI).

Some of the functionality in the web GUI only display if you have the iLO 2 Advanced Pack license. For more information on the iLO 2 Advanced Pack license, see "Obtaining and Activating iLO 2 Advanced Pack Licensing" (page 23) and the HP website at:

http://h71028.www7.hp.com/enterprise/cache/279991-0-0-0-121.html

NOTE: Cookies must be enabled on the web browser in order to successfully login to the iLO 2 web GUI.

System Status

The System Status tab enables you to access the following pages:

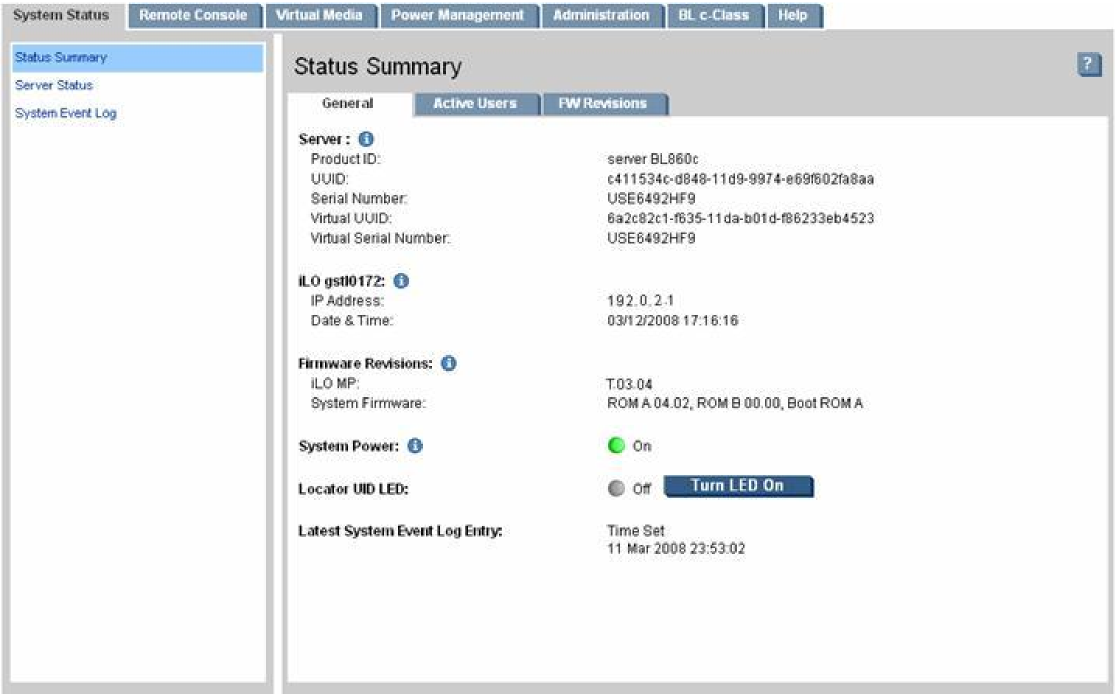
- **Status Summary: General, Active Users, and FW Revisions**
- **Server Status: General and Identification**
- **SEL**

Status Summary > General

The Status Summary General page (Figure 15) displays a brief status summary of the system.

NOTE: Depending on your server, this page might look slightly different.

Figure 15 Status Summary General Page



Status Summary

Server :
Product ID: server BL860c
UUID: c411534c-d848-11d9-9974-e69f602fa8aa
Serial Number: USE6492HF9
Virtual UUID: 6a2c82c1-f635-11da-b01d-f86233eb4523
Virtual Serial Number: USE6492HF9

iLO gstl0172:
IP Address: 192.0.2.1
Date & Time: 03/12/2008 17:16:16

Firmware Revisions:
iLO MP: T.03.04
System Firmware: ROM A 04.02, ROM B 00.00, Boot ROM A

System Power: ● On

Locator UID LED: ○ Off

Latest System Event Log Entry: Time Set
11 Mar 2008 23:53:02

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 31 lists the fields and descriptions.

Table 31 Status Summary General Page Description

Field	Description
System Power	The current power state (`ON/OFF/STANDBY`) of the system and the corresponding power LED state.
Latest SEL Entry	The most recent entry in the SEL.

Table 31 Status Summary General Page Description *(continued)*

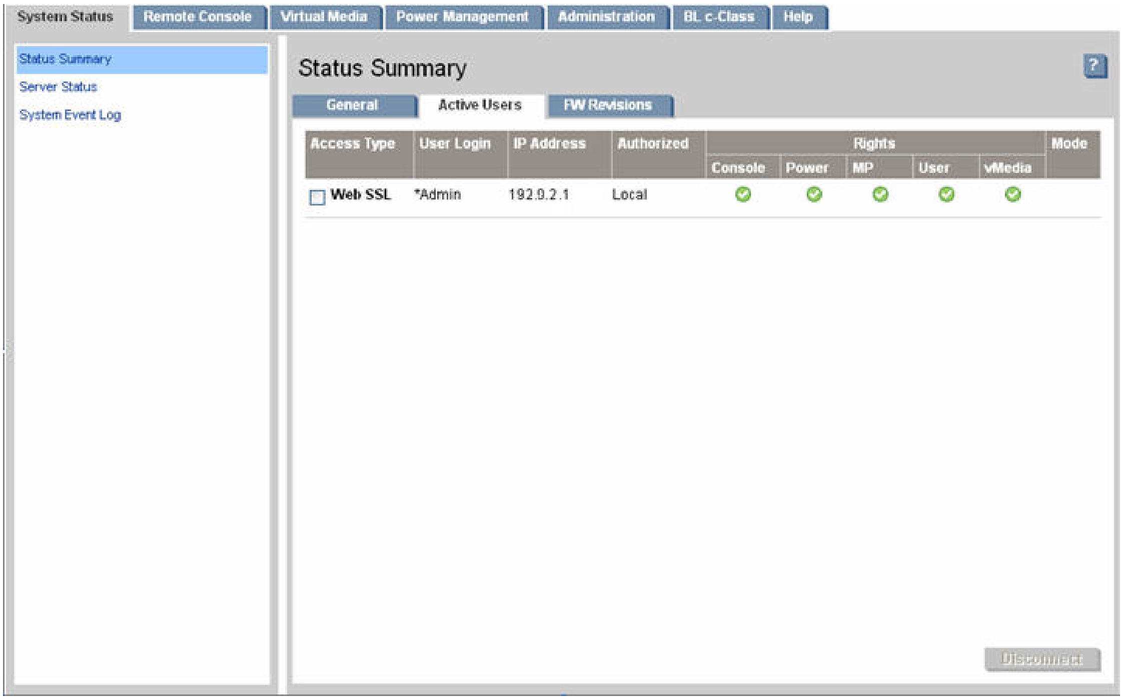
Field	Description
Firmware Revisions	Displays the current firmware revisions for iLO MP, BMC, EFI, system firmware, PDH, UCIO, PRS, and PMPIC for entry class server blades.
iLO 2 MP IP Address	The IP address of the iLO 2 subsystem.
Date & Time	Displays the date and time as known to the iLO 2.
Locator UID LED	Displays the status of the blue locator or UID LED and enables you to turn the Locator LED on or off. Note: The system's (Yellow) attention LED, which is separate from the locator LED, is lit automatically if a Warning event is present in the SEL. To clear the attention LED, read the SEL.

Status Summary > Active Users

The Active Users page (Figure 16) displays information about the users currently logged in to iLO 2.

NOTE: Depending on your server, this page might look slightly different.

Figure 16 Status Summary Active Users Page



Status Summary

Access Type	User Login	IP Address	Authorized	Rights					Mode
				Console	Power	MP	User	vMedia	
□ Web SSL	*Admin	192.0.2.1	Local	✓	✓	✓	✓	✓	

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 32 lists the fields and descriptions.

Table 32 Active Users Page Description

Field	Description
Access Type	Multiple access methods are available: Serial, Telnet, SSH, SSL web or IPMI over LAN. IPMI, vMedia, and IRC/vKVM users are not listed in web GUI sessions.
User Login	The user currently logged in through a particular access type.
IP Address	The IP address of the active user.

Table 32 Active Users Page Description *(continued)*

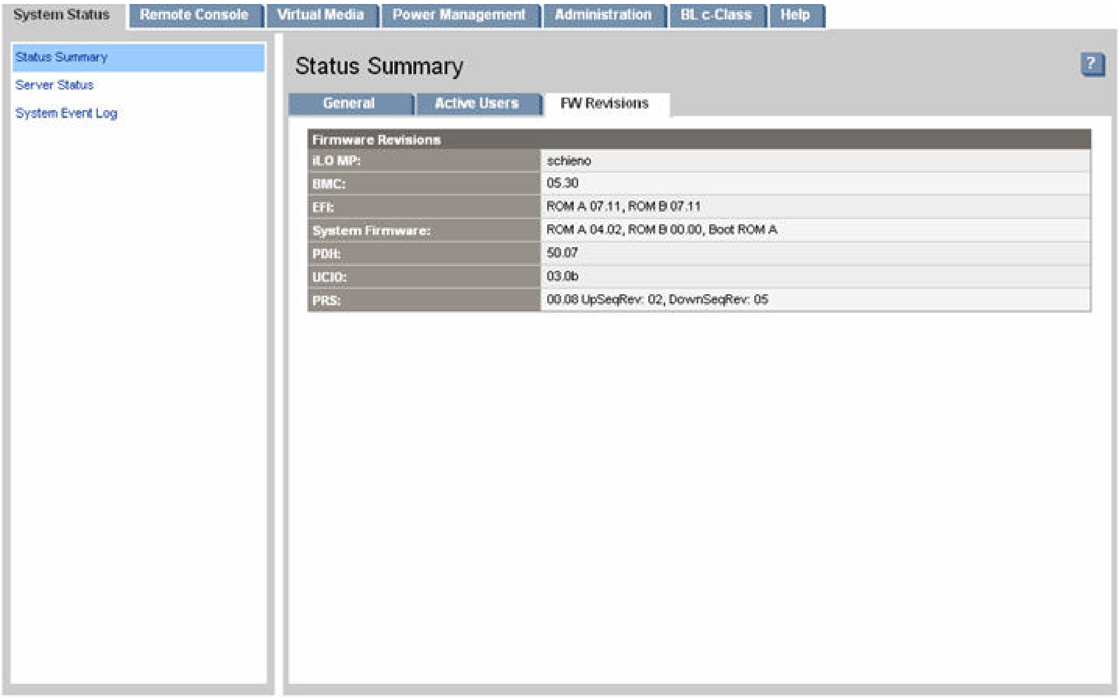
Field	Description
Authorized	The type of authentication: LDAP directory user authentication (LDAP) or locally stored iLO 2 user accounts (local).
Rights	Rights control the iLO 2 functions a user can perform. There are five user access rights: console access, MP configuration, power control, virtual media, and user administration. A user can be configured to have some, none, or all the access rights.
Mode	Current iLO 2 mode that the user is in. TUI modes are: MA, MP Main Menu; CM, MP Command menu; CO, console; LIVE, Live event viewer; VFP, VFP mode.
Disconnect	Enables a user with sufficient privileges to disconnect users of a certain access type.

Status Summary > FW Revisions

The FW Revisions page displays current revisions of the system firmware.

NOTE: Depending on your server, this page might look slightly different.

Figure 17 FW Revisions Page



Firmware Revisions	
iLO MP:	schieno
BMC:	05.30
EFI:	ROM A 07.11, ROM B 07.11
System Firmware:	ROM A 04.02, ROM B 00.00, Boot ROM A
PDH:	50.07
UCIO:	03.0b
PRS:	00.08 UpSeqRev: 02, DownSeqRev: 05

Table 33 lists the fields and descriptions.

Table 33 FW Revisions Page Descriptions

Field	Description
iLO MP	iLO Management Processor firmware version
BMC	Base Management Controller firmware version
EFI	Extensible Firmware Interface firmware version
System Firmware	System platform firmware version
PDH	Platform Dependent programmable Hardware version
UCIO	Universal Core I/O firmware version

Table 33 FW Revisions Page Descriptions *(continued)*

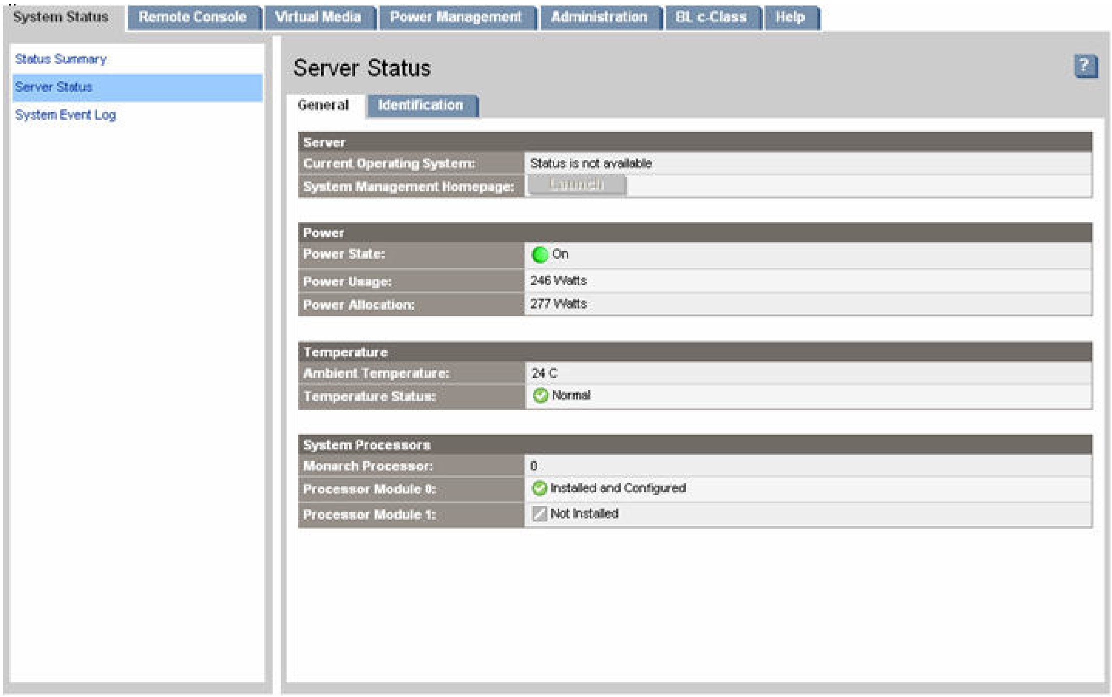
Field	Description
PRS	Power Reset Sequencer
PMPIC	Power Management Programmable Interrupt Controller for entry class server blades

Server Status > General

The Server Status General page (Figure 18) displays the status of server components. It also displays the status of the system processors and which processor is the monarch.

NOTE: Depending on your server, this page might look slightly different.

Figure 18 Server Status General Page



Server Status

Server	
Current Operating System:	Status is not available
System Management Homepage:	Launch
Power	
Power State:	● On
Power Usage:	246 Watts
Power Allocation:	277 Watts
Temperature	
Ambient Temperature:	24 C
Temperature Status:	✓ Normal
System Processors	
Monarch Processor:	0
Processor Module 0:	✓ Installed and Configured
Processor Module 1:	Not Installed

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 34 lists the fields and descriptions.

Table 34 Server Status General Page Description

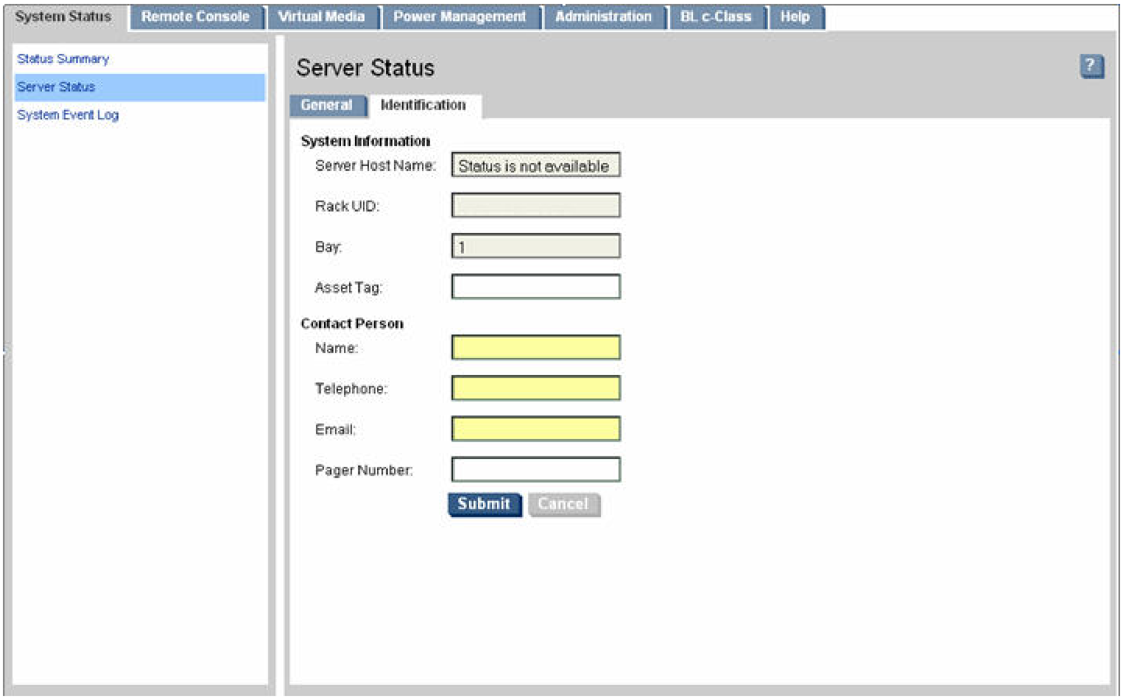
Field	Description
System Power	Displays the current power state of the system and the corresponding power LED state.
Temperature	Displays the temperature status.
Power Supplies	Lists the power supplies and their status and type.
Fans	Lists the fans and fan status.
System Processors	Displays the status of the processor. **NOTE:** For **BL c-Class** servers, you can obtain information on power supplies and fans through the OA. See "BL c-Class" (page 139).

Server Status > Identification

The Identification page enables you to configure system information for identifying the server.

NOTE: Depending on your server, this page might look slightly different.

Figure 19 Server Status Identification Page



Server Status

System Information

Server Host Name: Status is not available

Rack UID:

Bay: 1

Asset Tag:

Contact Person

Name:

Telephone:

Email:

Pager Number:

Table 35 lists the fields and descriptions.

Table 35 Server Status Identification Page Description

Field	Description
Server Host Name	Displays the server host name.
Rack UID	Displays the rack unique identifier: a known unique identifier for the rack.
Bay	Displays the bay number. The blade enclosure can support as many as eight HP Integrity server blades. When viewed from the rack front, the bays are numbered from left to right and from 1 to 8. The bay number is used to locate and identify a blade.
Asset Tag	Enter the asset tag information.
Contact Person	Enter the contact information in these fields.

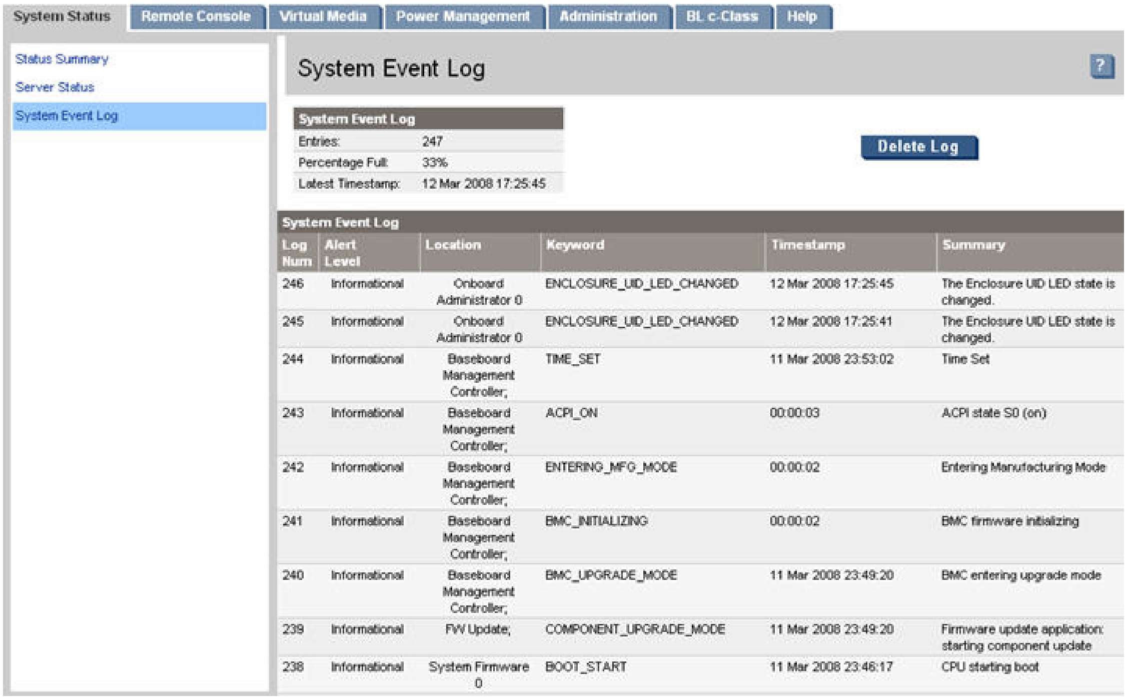
NOTE: Many of the fields are published by the iLO 2's SNMP for visibility to management applications on the network.

System Event Log

The System Event Log (SEL) page (Figure 20) enables you to view the contents of the event logs that have been stored in nonvolatile memory. If you have login rights, you can view the SEL. You must have iLO configuration access right to clear the logs.

NOTE: Depending on your server, this page might look slightly different.

Figure 20 System Event Log Page



System Event Log	
Entries:	247
Percentage Full:	33%
Latest Timestamp:	12 Mar 2008 17:25:45

System Event Log

Log Num	Alert Level	Location	Keyword	Timestamp	Summary
246	Informational	Onboard Administrator 0	ENCLOSURE_UID_LED_CHANGED	12 Mar 2008 17:25:45	The Enclosure UID LED state is changed.
245	Informational	Onboard Administrator 0	ENCLOSURE_UID_LED_CHANGED	12 Mar 2008 17:25:41	The Enclosure UID LED state is changed.
244	Informational	Baseboard Management Controller;	TIME_SET	11 Mar 2008 23:53:02	Time Set
243	Informational	Baseboard Management Controller;	ACPI_ON	00:00:03	ACPI state S0 (on)
242	Informational	Baseboard Management Controller;	ENTERING_MFG_MODE	00:00:02	Entering Manufacturing Mode
241	Informational	Baseboard Management Controller;	BMC_INITIALIZING	00:00:02	BMC firmware initializing
240	Informational	Baseboard Management Controller;	BMC_UPGRADE_MODE	11 Mar 2008 23:49:20	BMC entering upgrade mode
239	Informational	FW Update;	COMPONENT_UPGRADE_MODE	11 Mar 2008 23:49:20	Firmware update application: starting component update
238	Informational	System Firmware 0	BOOT_START	11 Mar 2008 23:46:17	CPU starting boot

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 36 lists the fields, buttons, and descriptions.

Table 36 System Event Log Page Description

Fields and Buttons	Description
System Event Log	High attention events and errors. Reading the SEL off the attention LED (blinking yellow light).
Forward Progress Log	Contains events of all types. Does not need to be cleared. In a web GUI session you cannot view forward progress logs, only SEL logs.
Boot Log	All events between start of boot and boot complete. You cannot view boot logs or previous boot logs from a web session.
Previous Boot Log	The boot log from the previous boot.
Delete Log	Deletes the log.

NOTE: You can view only the most pertinent fields for each event on the web. For a more complete decoding of the events, use the TUI available by logging in to iLO 2 through Telnet or SSH.

Events

Events can be a result of a failure or an error (such as fan failure, Machine-Check Abort, and so on). They can indicate a major change in system state (such as, firmware boot start or, system power on/off), or they can be forward progress markers (such as CPU selftest complete).

Events are produced by intelligent hardware modules, the OS, and system firmware. Events funnel into the BMC from different sources throughout the server. iLO 2 polls the BMC for new events and stores them in nonvolatile memory. Events communicate system information from the source of the event to other parts of the system, and ultimately to the system administrator.

The log viewer contains an event decoder to help you interpret events.

The following event severity (or alert) levels are defined:

0: Minor forward progress

1: Major forward progress

2: Informational

3: Warning

5: Critical

7: Fatal

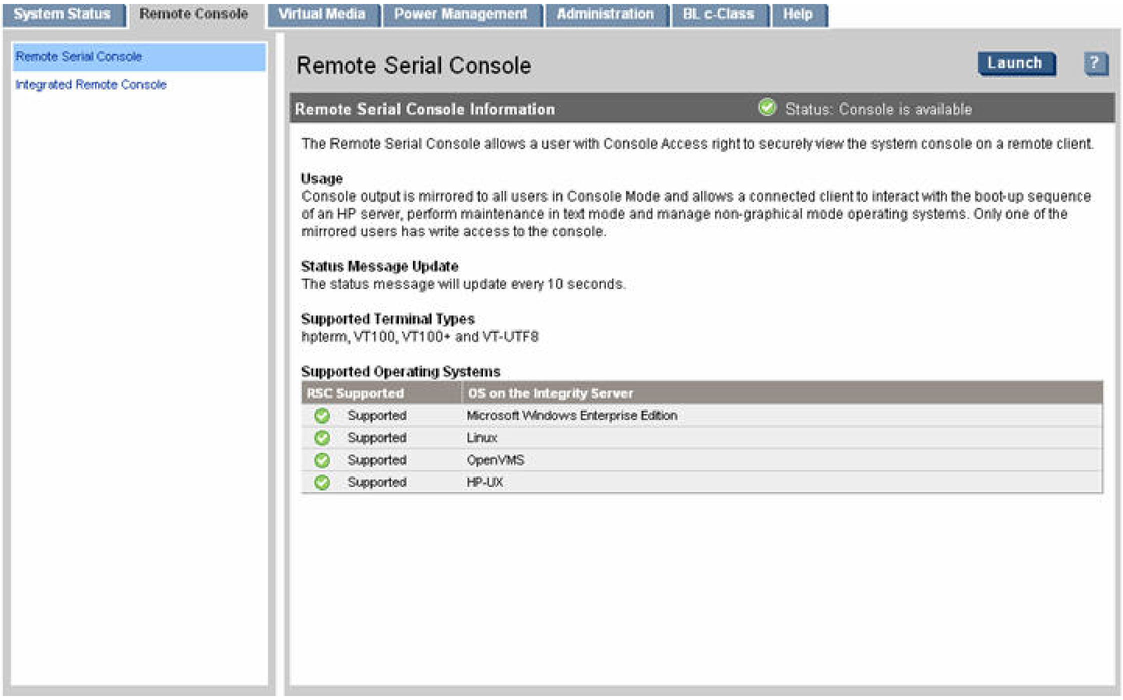
Remote Serial Console

The Remote Serial Console page (Figure 21) enables you to securely view and manage a remote server. You must have console access right to use this feature.

You can also connect to the system console by launching **View Console** from the Remote Serial Console page.

NOTE: Depending on your server, this page might look slightly different.

Figure 21 Remote Serial Console Page



Remote Serial Console

Remote Serial Console Information ✓ Status: Console is available

The Remote Serial Console allows a user with Console Access right to securely view the system console on a remote client.

Usage
Console output is mirrored to all users in Console Mode and allows a connected client to interact with the boot-up sequence of an HP server, perform maintenance in text mode and manage non-graphical mode operating systems. Only one of the mirrored users has write access to the console.

Status Message Update
The status message will update every 10 seconds.

Supported Terminal Types
hpterm, VT100, VT100+ and VT-UTF8

Supported Operating Systems

RSC Supported	OS on the Integrity Server
✓ Supported	Microsoft Windows Enterprise Edition
✓ Supported	Linux
✓ Supported	OpenVMS
✓ Supported	HP-UX

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

The remote serial console is a Java applet that requires Java Plug-in 1.4.2-10 to be installed on the client system. This applet enables connection to the server serial console over default port 2023. You can configure this port through the Administration > Access Settings page. All data on this port is encrypted using RC4. The remote serial console provides terminal emulation. Remote serial console operates with all the operating systems and browsers supported by iLO 2.

NOTE: Pop-up blocking applications prevent remote serial console from running. Disable any pop-up blocking applications before starting the remote serial console.

The iLO 2 mirrors the system console to the iLO 2 MP local, remote, and LAN ports. One console output stream is reflected to all of the connected console users. If several different terminal types are used simultaneously by the users, some users may see unexpected results. Only one of the mirrored users at a time has write access to the console. Write access is retained until another user requests console write access. To get console write access, enter **`Ctrl-Ecf`**.

To ensure proper operation of the remote serial console, verify the following conditions:

- Your emulator can run the supported terminal type.
- The iLO 2 terminal setting in the applet is a supported setting.
- The operating system environment settings and your client terminal type are set properly.
- All mirrored consoles are of the same terminal type for proper operation. Supported terminal types are:

Table 37 Supported Terminal Types

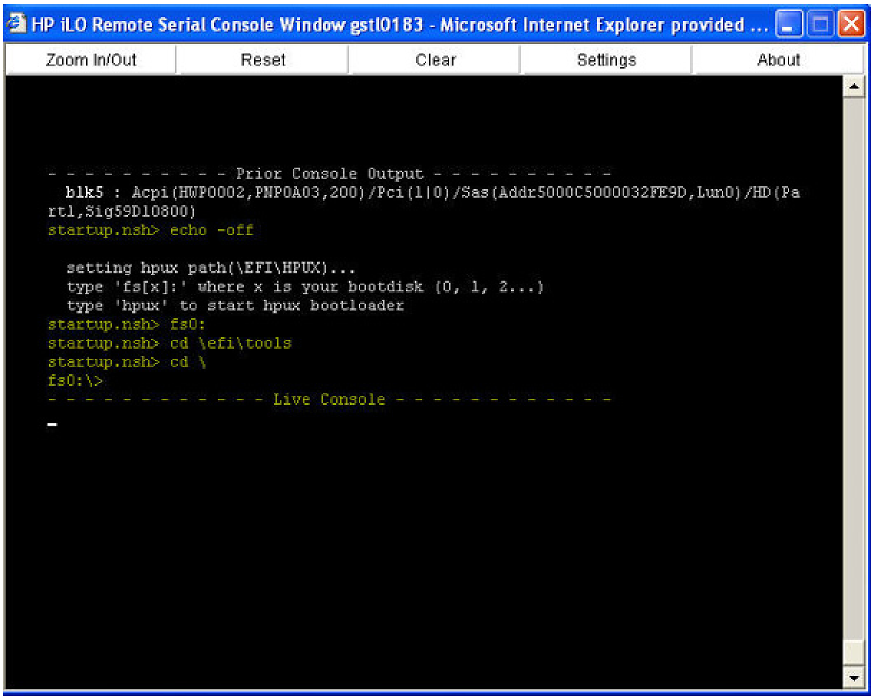
	HP-UX	Windows	Linux	EFI
hpterm	X	NS	NS	NS
Vt100	X	NS	X	X
Vt100+	NS	NS	X	X
Vt-utf8	NS	X	NS	X

IMPORTANT: Do not mix hpterm and vt100 terminal types at the same time. If there are two users collaborating and viewing console output with different emulation modes set, their clients will see garbled results if the output from the system is terminal specific.

To connect to the system console (Figure 22), click **Launch**.

NOTE: If **Launch** is disabled, the user does not have console access right. See the User Administration page under the Administration tab to add the access right.

Figure 22 Remote Serial Console Window



HP iLO Remote Serial Console Window gstl0183 - Microsoft Internet Explorer provided ...
Zoom In/Out
Reset
Clear
Settings
About

```
- - - - - - - - - - Prior Console Output - - - - - - - - - -
  blk5 : Acpi(HWP0002,PNP0A03,200)/Pci(1|0)/Sas(Addr5000C5000032FE9D,Lun0)/HD(Pa
rtl,Sig59D10800)
startup.nsh> echo -off

  setting hpux path(\EFI\HPUX)...
  type 'fs[x]:' where x is your bootdisk (0, 1, 2...)
  type 'hpux' to start hpux bootloader
startup.nsh> fs0:
startup.nsh> cd \efi\tools
startup.nsh> cd \
fs0:\>
- - - - - - - - - - - - Live Console - - - - - - - - - - - -
_
```

Using this feature you can do the following:

- View and interact with the boot sequence of your server.
- Perform maintenance activities in text mode.
- Manage non-graphical mode operating systems.

The console window remains open until you sign out of the iLO 2 interface using the provided link in the banner, leave the iLO 2 site, or refresh the entire page.

The remote serial console provides the console, and the GUI provides the iLO 2 MP Main Menu functionality.

Output from the console is stored in nonvolatile memory in the console log, regardless of whether or not any users are connected to a console. The Remote Serial Console page refreshes every 10 seconds.

The remote serial console option relies on the virtual serial port.

Virtual Serial Port

Integrity iLO 2 contains a virtual serial port that enables it to actually be the console hardware device for the OS. This port is a serial interface between the host system and iLO 2. iLO 2 converts the serial data stream to be available remotely through the remote serial console (a VT320 Java applet). The virtual serial port must be correctly enabled and configured in the host.

The virtual serial port function is a bidirectional data flow of the data stream appearing on the server's serial port. Using the remote console paradigm, a remote user can operate as if a physical serial connection is present on the server's serial port.

With the virtual serial port feature of iLO 2, an administrator can access a console application such as Windows EMS remotely over the network. iLO 2 contains the functional equivalent of the standard serial port (16550 UART) register set, and the iLO 2 firmware provides a Java applet that connects to the server serial port. If the serial redirection feature is enabled on the host server, iLO 2 intercepts the data coming from the serial port, encrypts it, and sends it to the web browser applet.

For Linux users, the iLO virtual serial port feature provides an important function for remote access to the Linux server. By configuring a Linux login process attached to the server serial port, you can use the iLO virtual serial port feature to remotely log in to the Linux operating system over the network.

For more information on using the virtual serial port, see *Integrated Lights-Out Virtual Serial Port configuration and operation HOW TO* on the HP website at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00263709/c00263709.pdf

Integrated Remote Console

The Integrated Remote Console (IRC) is a high-performance graphical console interface for Windows clients running Internet Explorer. The IRC provides Virtual Keyboard, Video (monitor), and Mouse (vKVM) capabilities with KVM over IP performance. The IRC data stream is encrypted, enabling you to securely view and manage the server. The IRC does not use Java.

The IRC functionality enables a user with console access right and the Advanced Pack license to perform the following:

- View the server graphics console and control the keyboard and mouse, as if you were standing in front of the remote server
- Access the server from any location on the same network
- Perform maintenance activities.
- Diagnose server failures interactively
- Perform a controlled reset of the server, regardless of the state of the host operating system, and remain connected to monitor the reboot process
- View a complete boot sequence following an automatic server recovery event
- View a log of remote console events

- Modify login passwords without administrator access right
- Remotely change the configuration parameters of the IRC

Because the iLO 2 IRC is hardware-based, it is available regardless of the state of the operating system.

IRC Requirements and Usage

The IRC feature is only available if you have the iLO 2 Advanced Pack license. If iLO 2 is not licensed to use the IRC, see the Licensing page under the Administration tab to activate the Advance Pack license.

You can view the list of supported operating systems and browsers on the HP website at http://www.hp.com/go/integrityilo.

Only one user has access to the IRC at a time. You must have console access right to use this feature. If you do not have console access right, see the User Administration page under the Administration tab to add this access right.

You must allow downloading and usage of signed ActiveX controls. The IRC runs as an ActiveX control that is downloaded to clients running Internet Explorer 7.0 with Service Pack 1 and above on Windows clients. No additional software is required on the remote server or client system.

The ActiveX control automatically downloads from iLO 2 on the first client connection.

The IRC uses encryption and compression to provide a secure connection.

NOTE: When working on multiple systems, controls for each system are displayed on a separate screen for each server. Additionally, you must allow downloading and usage of signed ActiveX controls.

Before running the IRC, note the following:

1. Verify that the IRC is available. Only one user can control the IRC at a time. If a remote console session already exists on the system, you are notified that IRC use is unavailable. To determine if the remote console/IRC is available for use, click **`Remote Console Integrated Remote Console`**. If **Launch** is grayed out and the `Maximum console number has been reached` status message appears, the remote console/IRC is in use by another client.
2. Verify that you have console access right on the User Administration page, or if the right must be granted.
3. Verify that the system is licensed for IRC use. View this information on the Administration□Licensing tab. For more information, see "Obtaining and Activating iLO 2 Advanced Pack Licensing" (page 23).
4. Disable any popup-blocking applications. Popup-blocking applications prevent the IRC from running.
5. Accept the IRC certificate. Refusing to accept the IRC certificate causes a red **X** to be displayed in the IRC and prevents the IRC from working on that client.
6. If you are using a Japanese keyboard on a Windows operating system, but are communicating in English, make sure the keyboard layout is set to Japanese. This ensures that the Japanese keyboard is properly working while running the IRC.

Limitations of the IRC Mouse and Keyboard

The IRC does not yet provide identical virtualization of the Windows keyboard. Some known issues are:

- No support for system-level commands such as `Ctrl + Esc`, or `Print Screen`.
- Pressing the **Ctrl** key locks the virtual mouse. Releasing the **Ctrl** key unlocks the virtual mouse.
- No support for simultaneous mouse click and keystroke combinations.

- The web session will timeout after 15 minutes if no mouse or keyboard activity is detected in the web interface and the vMedia, RSC, or IRC are not launched. An inactivity timeout configuration option is currently unavailable.
- A slight delay might be observed between the physical and virtual mouse pointer.

NOTE: If you run system discovery utilities such as MAPPER or IOSCAN, the output might display an extra keyboard and mouse that are not physically connected. This is a consequence of the IRC feature.

Browsers and Client Operating Systems that Support the IRC

You can view the list of supported browsers and client operating systems for IRC and vKVM on the HP website at http://www.hp.com/go/integrityilo.

IRC-Supported Resolutions and Browser Configurations

This section provides information on Microsoft Windows and HP-UX graphics settings for the IRC.

Microsoft Windows Server 2003 and HP-UX Graphics Resolution Settings for the IRC

To properly access and view the IRC and optimize performance, set your Windows-based HP Integrity server to the specifications listed below.

For display and mouse properties, the following settings are suggested:

Server Display Properties

- Set the background to plain (no wallpaper pattern) on the host server.
- Set the client screen resolution higher than the host server for best remote console performance.
- Set the display resolution to 800 x 600 pixels, or the maximum supported resolution of 1024 x 768 pixels.

  NOTE: The resolution on the host server must not exceed 1024 x 768 pixels. Higher resolutions can produce unpredictable results.

- Set the display color mode to 256 colors, or 24-bit colors.

Server Mouse Properties

- For mouse pointer scheme, select **None**.
- Select **Disable Pointer Trails**.
- Deselect **Enable Pointer Shadow**.
- Select **Motion** or **Pointer Options**, and set the pointer speed slider to the middle position.
- Deselect **Enhanced pointer precision**.

To automate setting an optimal mouse configuration, download the Lights-Out Optimization utility from the HP website at:

http://www.hp.com/servers/lights-out

Click the **Best Practices** graphic and select **Maximize Performance** .

Console Settings

The default console is the serial console.

HP recommends leaving the console settings on serial to preserve SSH access and the iLO 2 console logs.

Console settings affect the information that you see on the IRC. In HP-UX, if you modify the console settings in EFI to graphics, the modivication affects the IRC as follows:

- If you set VGA-Primary and Serial-Not Configured in EFI, the IRC is a system console. If you configure HP-UX to start X Windows, IRC also acts as an X terminal.
- If you set Serial-Primary and VGA-Not Configured in EFI, the IRC is only an X terminal.

In all cases, the EFI console is available on the remote serial console as well as the IRC. But, the OS console for HP-UX appears according to the device settings in EFI.

If an HP-UX operating system is configured to use VGA as the console, the HP-UX console is available only through the IRC and VGA. iLO 2 no longer receives HP-UX console traffic through the serial connection. The remote serial console data stream stops, so:

- Serial cable, SSH, Telnet, and remote serial console through the web do not provide the HP-UX console.
- The console log in iLO 2 does not contain any HP-UX console output.
- The HP-UX console is only available from iLO 2 through the IRC application.

For instructions on how to configure the system console to use VGA, see the *HP-UX 11i v3 Installation and Update Guide* on the HP website at http://docs.hp.com/en/5992-5795/index.html and follow the instructions on Task 1: Selecting Your HP-UX Console for Itanium-based Systems.

Enabling X Windows on HP-UX

You can use the IRC to access the graphics display not only when X Windows is running, but also before X Windows starts.

Typically, X Windows is disabled by default on HP-UX. For instructions on enabling X Windows using the graphics application through the IRC, see the *graphics administration guide for HP-UX servers* on the HP website at http://docs.hp.com/en/5992-5398/5992-5398.pdf.

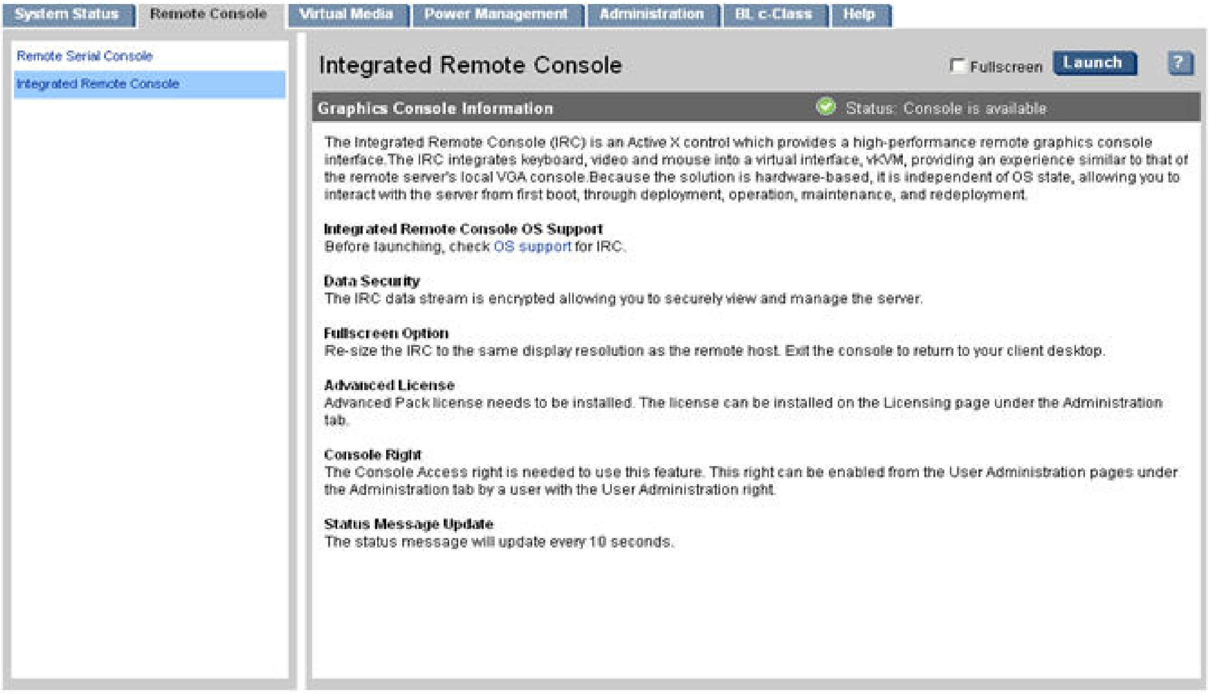
Accessing the IRC

Figure 23 shows the IRC page.

IMPORTANT: The operating system server console output does not display on the console device screen until the server boots to the EFI Shell. To view console output prior to booting to the EFI Shell, either start a console session using the console serial port (RS-232), or access iLO 2 virtual serial port, or IRC. See“Configuring the iLO 2 MP LAN Using the Console Serial Port” (page 37).

NOTE: Depending on your server, this page might look slightly different.

Figure 23 Integrated Remote Console Page



Integrated Remote Console

Graphics Console Information — Status: Console is available

The Integrated Remote Console (IRC) is an Active X control which provides a high-performance remote graphics console interface.The IRC integrates keyboard, video and mouse into a virtual interface, vKVM, providing an experience similar to that of the remote server's local VGA console.Because the solution is hardware-based, it is independent of OS state, allowing you to interact with the server from first boot, through deployment, operation, maintenance, and redeployment.

Integrated Remote Console OS Support
Before launching, check OS support for IRC.

Data Security
The IRC data stream is encrypted allowing you to securely view and manage the server.

Fullscreen Option
Re-size the IRC to the same display resolution as the remote host. Exit the console to return to your client desktop.

Advanced License
Advanced Pack license needs to be installed. The license can be installed on the Licensing page under the Administration tab.

Console Right
The Console Access right is needed to use this feature. This right can be enabled from the User Administration pages under the Administration tab by a user with the User Administration right.

Status Message Update
The status message will update every 10 seconds.

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

To access the IRC, select **Remote Console > Integrated Remote Console** and click **Launch**. The IRC might experience a slight delay as it first loads on your browser.

The IRC page refreshes every 10 seconds.

Table 38 lists the fields, buttons, and actions.

Table 38 IRC Page Description

Fields and Buttons	Action
Fullscreen	Resizes the IRC page. For fullscreen with multi-head client, launch the browser from the primary display.
Launch	Resizes the IRC page to the same display resolution as the remote host. To open the server’s graphic console in a new browser window, click **Launch**.

The IRC displays the host server’s graphics console (Figure 24).

Figure 24 Integrated Remote Console Window

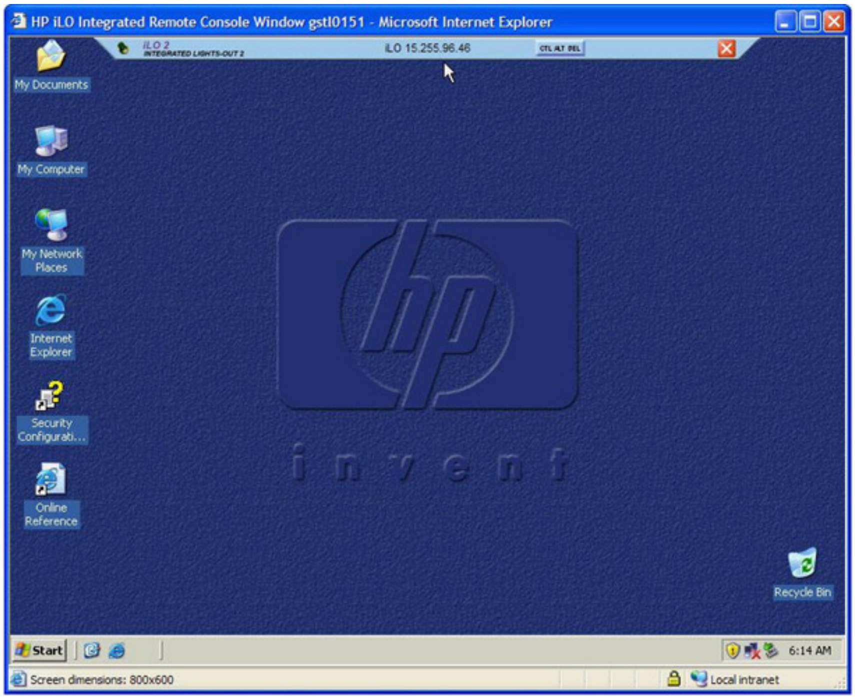


Table 39 lists the menu bar, buttons, and actions you can perform in the IRC window.

Table 39 IRC Window Description

Menu Bar Buttons	Action
Thumb Tack	Enables you to keep the menu open, or retracts it when the mouse is moved away.
Ctrl+Alt+Del	Enables you to simulate the **Ctrl Alt Del** keyboard sequence on a remote console.
Exit (red button)	Enables you to close and exit the console and return to the client desktop.

IMPORTANT: For security purposes, if you log in to a host server through the IRC, you should log out before closing the IRC.

NOTE: When you run system discovery utilities such as MAPPER or IOSCAN, the output might display an extra keyboard and mouse that are not physically connected. This is a consequence of the IRC feature.

Integrated Remote Console Fullscreen

The IRC Fullscreen causes your client to resize its screen to the same resolution as the remote server. The IRC Fullscreen automatically chooses the best client display settings for that resolution; however, some monitors have trouble with the highest screen refresh rates supported by the video adapter. If this occurs:

1. To check our desktop properties, right-click the desktop and select **Properties>Settings>Advanced>Monitor**.
2. Select a lower screen refresh rate.
3. To resize the IRC to the same display resolution as the remote host, select **Fullscreen** before you click **Launch**.
4. Use the red **X** to exit the IRC and return to your client desktop.

Virtual Media

Virtual Media (vMedia) provides you with virtual devices that mimic physical hardware devices such as a virtual floppy disk drive and a CD/DVD drive that connects through the network to the managed server just as if it was physically connected. The vMedia device can be a physical CD/DVD drive on the management workstation, or it can be an image file stored on a local disk drive or network drive.

Booting from the iLO 2 CD/DVD enables administrators to upgrade the host system ROM, upgrade device drivers, deploy an OS from network drives, and perform disaster recovery of failed operating systems, among other tasks.

The iLO 2 device uses a client-server model to perform the vMedia functions. The iLO 2 device streams the vMedia data across a live network connection between the remote management console and the host server. The vMedia Java applet provides data to the iLO 2 as it requests it.

The Virtual Media page refreshes every 10 seconds. Only one user can connect a virtual device at a time.

NOTE: The iLO 2 vMedia is automatically disconnected if the iLO 2 management processor is reset. HP does not recommend use of iLO 2 vMedia with firmware update tools such as HPOFM which reset the management processor mid-way through the update process.

Using iLO 2 Virtual Media Devices

Connect client-based vMedia to a host HP Integrity server through a graphical interface using a signed Java applet. Refusing to accept the applet certificate prevents browser-based vMedia from functioning (a red **X** appears). It also prevents the remote console applet from functioning because it is also signed using the same certificate.

Virtual media functionality is part of the iLO 2 Advanced Pack feature set and is enabled by purchasing the optional iLO 2 Advanced Pack license and granting the vMedia right. If not licensed, the message "`iLO 2 feature not licensed`" appears. For more information, see "Obtaining and Activating iLO 2 Advanced Pack Licensing" (page 23).

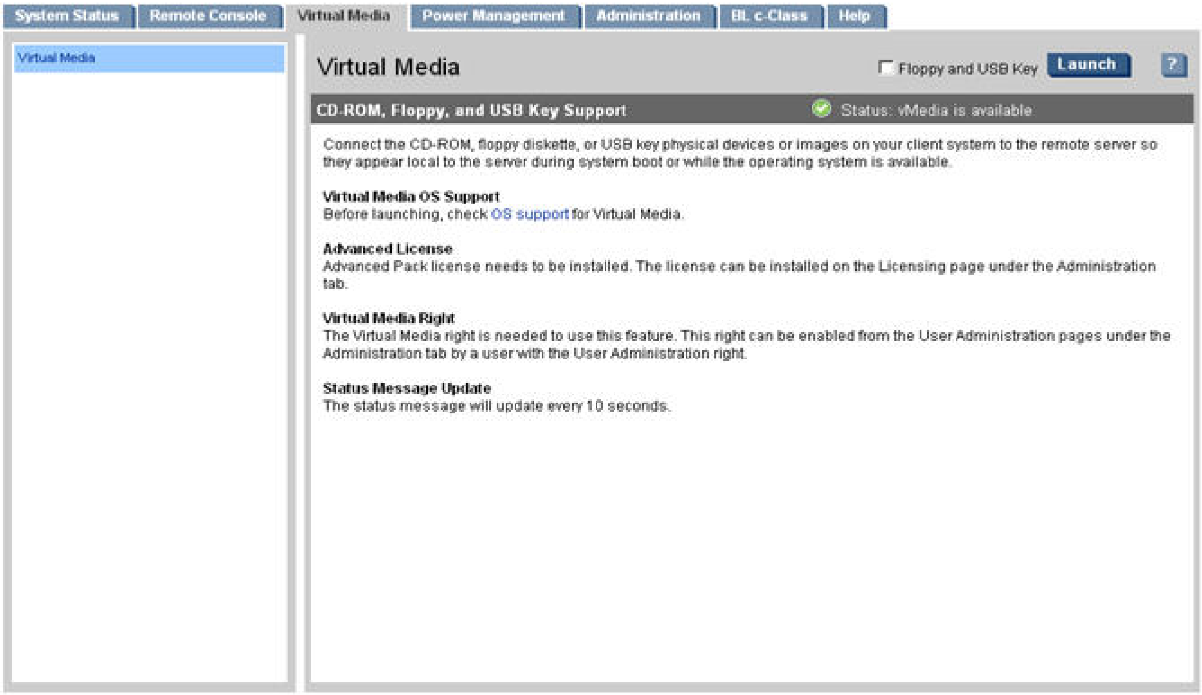
NOTE: You can use the vMedia applet only on x86 clients.

To access the iLO 2 vMedia devices using the graphical interface:

1. Select **Virtual Media**. The Virtual Media page appears (Figure 25)

   NOTE: Depending on your server, this page might look slightly different.

   Figure 25 Virtual Media Page

   Virtual Media

   CD-ROM, Floppy, and USB Key Support — Status: vMedia is available

   Connect the CD-ROM, floppy diskette, or USB key physical devices or images on your client system to the remote server so they appear local to the server during system boot or while the operating system is available.

   Virtual Media OS Support
   Before launching, check OS support for Virtual Media.

   Advanced License
   Advanced Pack license needs to be installed. The license can be installed on the Licensing page under the Administration tab.

   Virtual Media Right
   The Virtual Media right is needed to use this feature. This right can be enabled from the User Administration pages under the Administration tab by a user with the User Administration right.

   Status Message Update
   The status message will update every 10 seconds.

2. Click **Launch** to load the vMedia applet. The vMedia applet loads in support of the vMedia device.
3. At this point, you can connect to a virtual CD/DVD or virtual floppy/USB key device or create an iLO 2 disk image file.

NOTE: When you disconnect the iLO 2 vMedia, you might receive a warning message from the host operating system regarding unsafe removal of a device. This warning can be avoided by using the operating system's-stop-device function before disconnecting it from the vMedia.

Virtual CD/DVD

The iLO 2 virtual CD/DVD is available during server boot for operating systems specified in (insert operating system web link here)

Booting from the iLO 2 virtual CD/DVD enables you to deploy an operating system from network drives with DVDs or CDs that contain data in the El Torito Bootable CD format, as well as perform other tasks.

If the host server operating system supports USB mass storage devices, the iLO 2 virtual CD/DVD is also available after the host server operating system loads. Use the iLO 2 virtual CD/DVD when the host server operating system is running to upgrade device drivers, install software, and perform other tasks. Having the virtual CD/DVD available when the server is running can be especially useful if you must diagnose and repair a problem with the NIC driver.

The virtual CD/DVD can be the physical CD/DVD drive on the client system (which you are running on the web browser), or an image file stored on the client or network drive. For maximum performance, HP recommends using local image files stored either on the hard drive of your client system or on a network drive accessible through a high-speed network link.

The iLO 2 vMedia CD/DVD appears to your operating system just like any other CD/DVD. When using the iLO 2 for the first time, the host operating system might prompt you to complete a **New Hardware Found** wizard.

NOTE: This feature requires that the Java Plug-in 1.4.2 or 1.5 is installed.

This feature requires the vMedia right and the Advance Pack License. For more information, see "Obtaining and Activating iLO 2 Advanced Pack Licensing" (page 23). If a user does not have the vMedia right, it can be granted from the User Administration page under the Administration tab by a user with Admin privileges.

To use a physical CD/DVD drive in your client system:

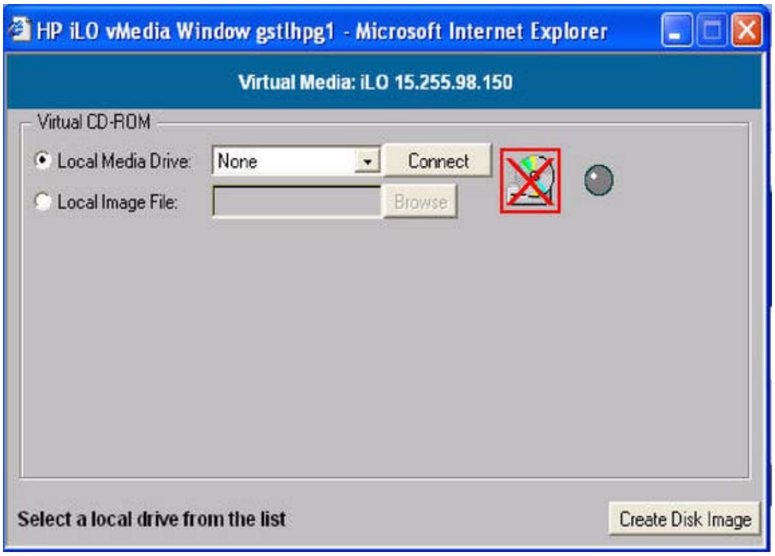
1. Select **Virtual Media**. The Virtual Media content page appears.
2. Click **Launch** to load the applet and connect to USB CD/DVD devices and disk image files available on the client as virtual devices on the server. The vMedia applet appears (Figure 26).

   NOTE: Only one user and one device can be connected at a time.

   IMPORTANT: Only CD and DVD-ROM image files are supported.

   If you use a USB key image file, you must select the Floppy/USB Key option. The USB key image file is not interchangeable with the CD or DVD-ROM and vice versa.

   Figure 26 Virtual Media Dialog Box (Before Connection)



HP iLO vMedia Window gstlhpg1 - Microsoft Internet Explorer

Virtual Media: iLO 15.255.98.150

Virtual CD-ROM

● Local Media Drive: None

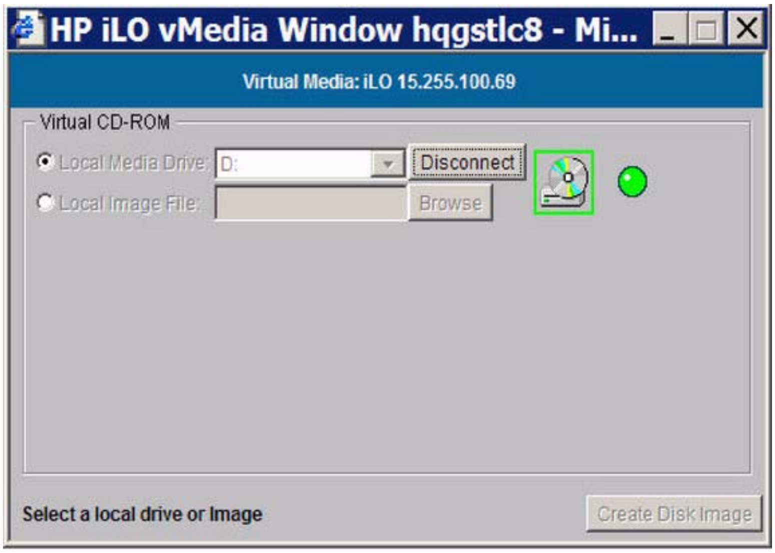
○ Local Image File:

Select a local drive from the list

3. Select **Local Media Drive**.
4. Select the drive letter of the desired physical CD/DVD drive on your client system from the list.

5. Click **Connect**. The connected drive icon and LED changes states to reflect the current status of the virtual CD/DVD.

Figure 27 Virtual Media Dialog Box (after connection)


HP iLO vMedia Window hqgstlc8 - Mi...
Virtual Media: iLO 15.255.100.69
Virtual CD-ROM
● Local Media Drive: D:
Disconnect
○ Local Image File:
Browse
Select a local drive or Image
Create Disk Image

After you are connected, virtual devices are available to the host server until you close the vMedia applet or sign out from a web session. When you are finished using the virtual CD/DVD, disconnect the device from the host server or close the applet.

NOTE: The vMedia applet must remain open when using a vMedia device.

Virtual Media CD/DVD Operating System

You can view the list of supported operating systems on the HP website at http://www.hp.com/go/integrityilo.

vMedia CD/DVD operating systems information is listed as follows:

- Currently, EFI console only supports El Torito bootable CD format media.
- Windows Server 2003:

  The virtual CD/DVD displays automatically after Windows has recognized the mounting of the USB device. Use it as you would a locally attached CD/DVD device.
- Linux

  On servers with a locally attached IDE CD/DVD, the virtual CD/DVD device is accessible at `/dev/cdrom1`. However, on servers without a locally attached CD/DVD (such as the HP Integrity server blades) the virtual CD/DVD is the first CD/DVD accessible at`/dev/cdrom`. The virtual CD/DVD can be mounted as a normal CD/DVD device using: `mount /mnt/cdrom1`.
- HP-UX 11.23

  To recognize the hardware path and special files, run the `ioscan -kfnC disk` command.

  To mount the virtual CD/DVD/image file on a directory, use the `# mount <special files path> /<dir-name>` command.
- OpenVMS

Creating the iLO 2 Disk Image Files

The iLO 2 vMedia feature enables you to create CD and DVD image files within the same applet. The image files created are ISO-9660 file system images and El Torito bootable CD images. The performance of the iLO 2 vMedia is faster when image files are used. The utility to create the iLO 2 CD/DVD disk image files is integrated into the vMedia applet.

Store image files on your client computer or on a network drive that can be accessed from the client using a fast network segment. A disk image file produces better performance than using a physical CD in your client computer.

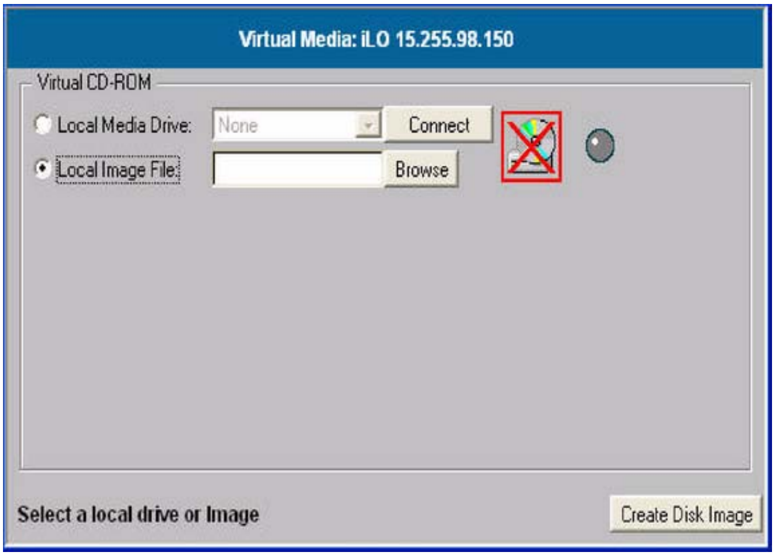
To create image files from physical diskettes, CDs, or DVDs, use the Disk>>Image option. The Image>>Disk option is not valid for a virtual CD/DVD image. The Disk>>Image button changes to Image>>Disk when clicked.

NOTE: The iLO 2 Create Media Image utility does not currently support USB devices in Linux or NetWare.

The following procedure explains how to create an iLO 2 disk image file:

1. Select **Local Image File** in the Virtual CD-ROM section of the vMedia applet.
2. Select **Local Media Drive** from the list.

Figure 28 Local Image File Dialog Box



Virtual Media: iLO 15.255.98.150

Virtual CD-ROM

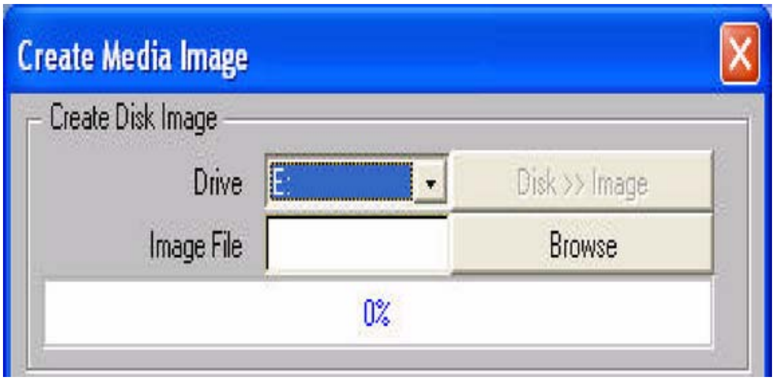
○ Local Media Drive: None

● Local Image File:

Select a local drive or Image

3. Enter the path or file name of the image in the text box or click **Browse** to open the Create Media Image dialog box and locate the image file.

Figure 29 Create Media Image Dialog Box



Create Media Image

Create Disk Image

Drive: E:

Image File:

0%

4. Click **Create Disk Image**. The vMedia applet begins the process of creating the image file. The process is complete when the progress bar reaches 100%. This creates a file that emulates a CD/DVD on the local system. To cancel the creation of an image file, click **Cancel**.

To insert the next CD during an OS installation or any application installation with multiple image files:

1. To select the next image file or to replace the CD/DVD with the next CD/DVD, click **Browse**
2. To continue the installation, click **OK** on the host server.

ⓘ **IMPORTANT:** Do not click **Disconnect** to select the next CD/DVD image file.

The connected drive icon and LED changes states to reflect the current status of the virtual CD/DVD. After you are connected, virtual devices are available to the host server until you close the vMedia applet. When you are finished using the virtual CD/DVD, you can choose to disconnect the device from the host server or close the applet. The vMedia applet must remain open when using a vMedia device.

The iLO 2 vMedia CD/DVD appears to your operating system just like any other CD/DVD. When using the iLO 2 for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

Virtual Floppy/USB Key

The iLO 2 vMedia devices connect to the host server using USB technology. Using USB also enables new capabilities for the iLO 2 vMedia devices when connected to USB-supported operating systems.

ⓘ **IMPORTANT:** If the virtual floppy/USB key capability is enabled, the floppy and USB key drive normally cannot be accessed from the client operating system.

Under certain conditions, you can access the virtual floppy and USB key drive from the client operating system while it is connected. However, it is important that access to the virtual floppy or USB key drive from the client operating system not be attempted while it is connected as a virtual media device. Doing so could cause data loss on the floppy drive. Always disconnect virtual media before trying to access it from the client operating system.

The iLO 2 virtual floppy disk is available at server boot time for all operating systems. Booting from the iLO 2 virtual floppy enables you to upgrade the host system ROM, deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

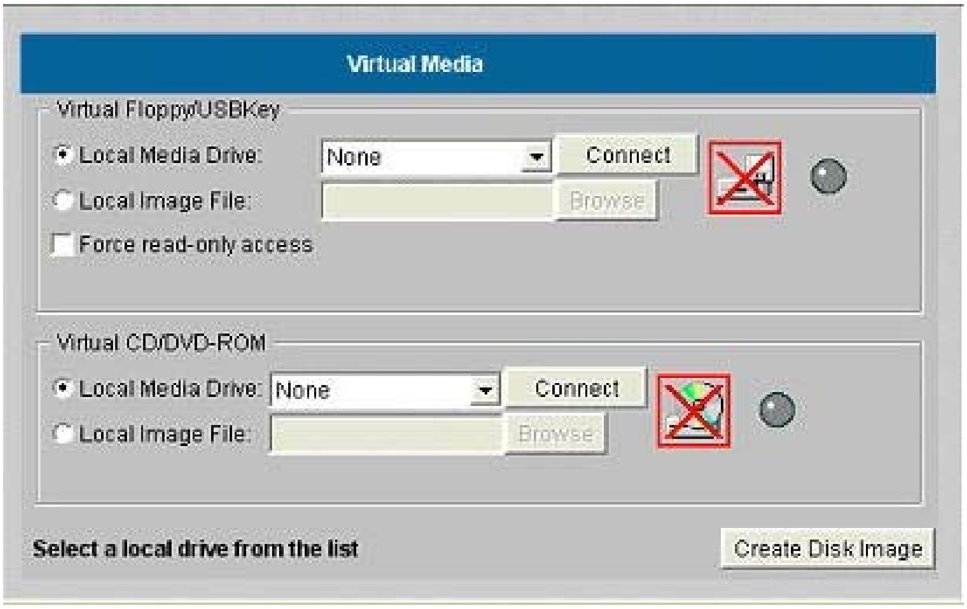
If the host server operating system supports USB mass storage devices, the iLO 2 virtual floppy/USB key is also available after the host server operating system loads. You can use the iLO 2 virtual floppy/USB key when the host server operating system is running to upgrade device drivers, create an emergency repair diskette, and perform other tasks. Having the virtual floppy available when the server is running can be especially useful if you must diagnose and repair a problem with the NIC driver.

The virtual floppy/USB key can be the physical floppy or USB key drive on which you are running the web browser, or an image file stored on your local hard drive or network drive. For maximum performance, HP recommends using the local image files stored either on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

To use a physical floppy or USB key drive in your client PC:

1. Select **Local Media Drive** in the virtual floppy/USB key section.
2. Select the drive letter of the desired local floppy or USB key drive on your client PC from the menu. To ensure the source diskette or image file is not modified during use, select **Force read-only access**.
3. Click **Connect**. The connected drive icon and LED changes state to reflect the current status of the virtual floppy Drive.

Figure 30 Virtual Floppy/USB Key


Virtual Media

Virtual Floppy/USBKey

● Local Media Drive: None Connect

○ Local Image File: Browse

□ Force read-only access

Virtual CD/DVD-ROM

● Local Media Drive: None Connect

○ Local Image File: Browse

Select a local drive from the list

Create Disk Image

To use an image file:

1. Click **Launch**.
2. Within the virtual USB key section of the vMedia applet, select **Local Image File**.
3. In the textbox, enter the path or file name of the image, or to locate the image file by using the Choose Disk Image File dialog, click **Browse**. To ensure the source diskette or image file is not modified during use, select **Force read-only access**.

IMPORTANT: You must select the USB key image file with this option.

If you use CD or DVD-ROM image files, you must select the CD/DVD-ROM option. The CD or DVD-ROM option is not interchangeable with the USB key image file and vice versa.

4. Click **Connect**. The connected drive icon and LED change state to reflect the current status of the virtual USB key drive. When connected, the virtual devices are available to the host server until you close the vMedia applet.
5. When you are finished using the virtual USB key, disconnect the device from the host server or close the applet.

The iLO 2 Virtual floppy/USB key is available to the host server at run time if the operating system on the host server supports USB floppy or key drives.

The iLO 2 Virtual floppy/USB key appears to your operating system just like any other drive. When using iLO 2 for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

Virtual Media Applet Timeout

The vMedia applet does not timeout when it is connected to a host server. The vMedia applet must remain open when using a vMedia device. The vMedia applet closes when you log out.

Supported Operating Systems and USB Support for vMedia

To use vMedia devices, your operating system must support USB mass storage devices.

Different operating systems provide different levels of USB support. iLO 2 uses the operating system's built-in USB drivers. The level of USB support in the operating system affects the level of support for iLO 2 vMedia. In general, any operating system issues that affect a USB CD/DVD drive also affect iLO 2 vMedia.

The HP server ROM provides support during server boot for vMedia with the El Torito bootable CD format.

You can view the list of supported operating systems on the HP website at http://www.hp.com/go/integrityilo.

Java Plug-in Version

The vMedia feature requires prior installation of Java Plug-in 1.4.2_10 or higher.

Client Operating System and Browser Support for vMedia

You can view the list of supported client operating systems on the HP website at http://www.hp.com/go/integrityilo.

Power Management

For entry class and server blades, the iLO 2 power management feature enables you to view and control the power state of the server, monitor power usage, monitor the processor, and modify power settings. The Power Management page has three menu options:

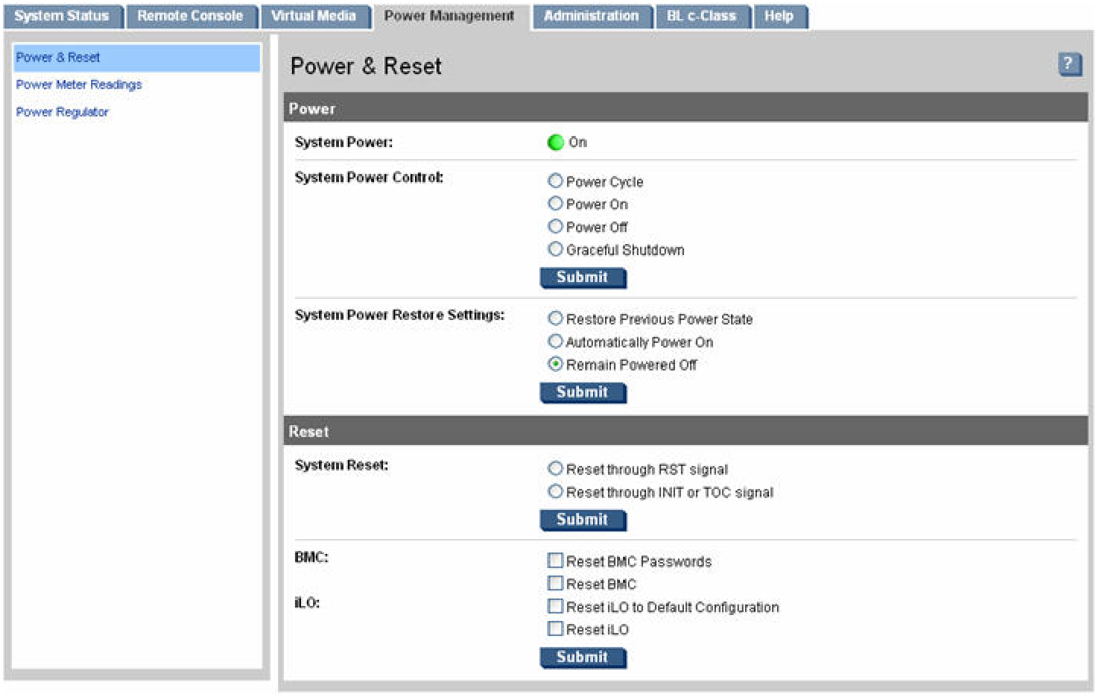
- Power & Reset
- Power Meter Readings
- Power Regulator

Power & Reset

The Power & Reset page (Figure 31) enables you to view and control the power state of the server. It also provides you with options to reset the system, the BMC, or iLO 2.

NOTE: Depending on your server, this page might look slightly different.

Figure 31 Power & Reset Page



Power & Reset

Power

System Power: ● On

System Power Control:
○ Power Cycle
○ Power On
○ Power Off
○ Graceful Shutdown

System Power Restore Settings:
○ Restore Previous Power State
○ Automatically Power On
● Remain Powered Off

Reset

System Reset:
○ Reset through RST signal
○ Reset through INIT or TOC signal

BMC:
□ Reset BMC Passwords
□ Reset BMC

iLO:
□ Reset iLO to Default Configuration
□ Reset iLO

NOTE: The BL c-Class tab is available only on HP Integrity server blades. For information on how to set the power management options in the OA, see the *HP BladeSystem Onboard Administrator User Guide* on the HP website at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00705292/c00705292.pdf

Table 40 lists the fields, buttons, and descriptions.

Table 40 Power & Reset Page Description

Fields and Buttons	Description
System Power	The current power state of the system.
System Power Control	A user with power control access can issue the following options for remote control of the system power: • Power Cycle: Turns system power off and on. The delay between off and on is 30 seconds. • Power On: Turns system power on (it has no effect if power is already on). • Power Off: Turns system power off. This is equivalent to forcing the system power off with the front panel power switch. There is no signal sent to the OS to bring the software down before power is turned off. For proper system shutdown, shutdown the OS before issuing this command. • Graceful Shutdown: BMC sends a signal to the OS to shutdown, prior to turning off system power supported by IPF operating systems.
System Power Restore Settings	This option enables you to configure the power restore policy. The power restore policy determines how the system behaves when AC power returns after an AC power loss. You must have iLO configuration access right to use this option. • Restore Previous Power State: The power is restored to the state that was in effect when AC was removed or lost. • Automatically Power On: The system is powered up after AC is applied. • Remain Powered Off: The system stays powered off after AC is applied. Pushing the system power switch or choosing the Power On option under System Power Control is required to power on the system.
System Reset	This feature has the following options: • Reset through RST signal: This option causes the system to reset through the RST signal. Under normal operation, shut down the OS before issuing this command. Execution of this command irrecoverably halts all system processing and I/O activity and restarts the computer system. The effect of this command is very similar to cycling the system power - the OS is not notified, no dump is taken on the way down, and so on. You must have power control access right to issue this option. • Reset through INIT or TOC signal: This option causes the system to be reset through the INIT or Transfer of Control (TOC) signal. Under normal operation, shut down the OS before issuing this command. Execution of this command irrecoverably halts all system processing and I/O activity and restarts the computer system. It is different from the previous option in that the processors are signaled to dump state on the way down. You must have iLO configuration access right to issue this option.
BMC	This feature has the following options: • Reset BMC passwords: This resets BMC (EFI Shell) passwords. • Reset BMC: This option enables you to issue a BMC reset. Under normal operation, shut down the OS before issuing this command. You must have iLO configuration access right to issue this option.

Table 40 Power & Reset Page Description *(continued)*

Fields and Buttons	Description
iLO 2	This feature has the following options: • Reset to the iLO 2 default configuration: This option enables you to set all iLO 2 parameters back to their default values. You must have iLO configuration access right to issue this option. • Reset the iLO 2: This option enables you to reset the iLO 2. You can safely perform an iLO 2 reset without affecting the operation of the server. You must have iLO configuration access right to issue this option.
Submit	Click to submit selections.

Power Meter Readings

The Power Meter Readings page (Figure 32) enables you to graphically view and monitor server power usage, temperature, and power regulator settings.

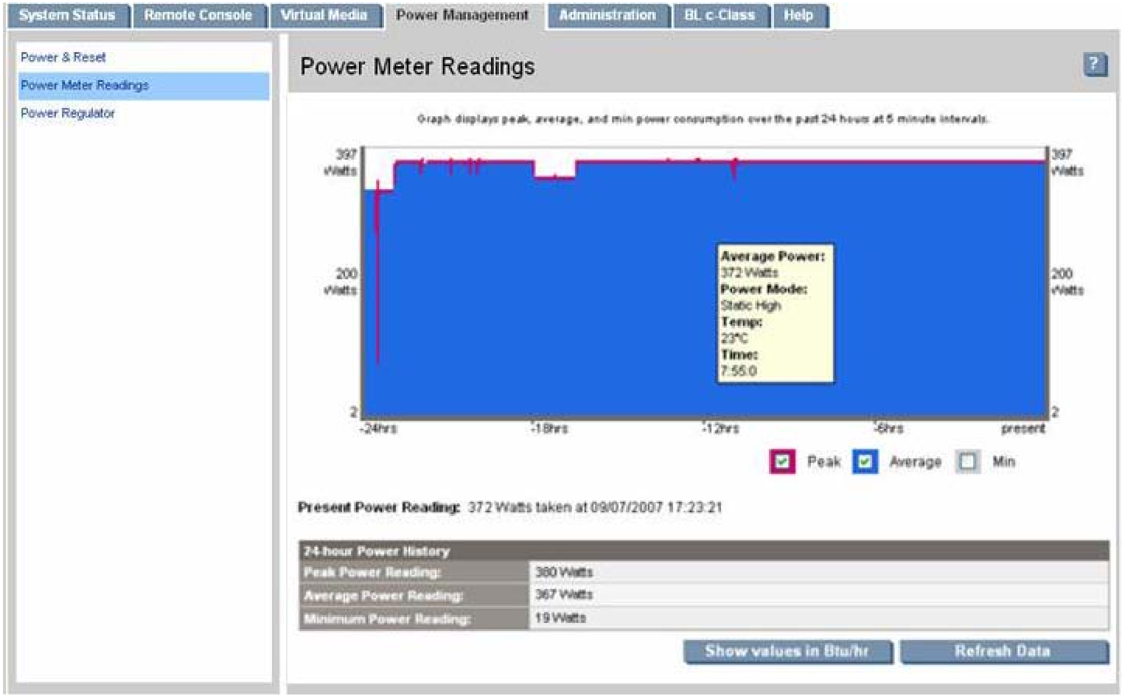
Power meter readings is a licensed feature and requires the Advanced Pack license to see the Power Regulator graphs from the iLO 2 web GUI. The license key also enables iLO 2 to share information with Insight Power Manager.

NOTE: You can obtain an instant power reading without a license key through the CLI using the PS command.

The Power Meter Readings page has two sections: Power Meter Readings and 24-hour Power History.

NOTE: Depending on your server, this page might look slightly different.

Figure 32 Power Meter Readings Page



Power Meter Readings

Graph displays peak, average, and min power consumption over the past 24 hours at 5 minute intervals.

Average Power: 372 Watts
Power Mode: Static High
Temp: 23°C
Time: 7:55.0

Present Power Reading: 372 Watts taken at 09/07/2007 17:23:21

24-hour Power History	
Peak Power Reading:	380 Watts
Average Power Reading:	367 Watts
Minimum Power Reading:	19 Watts

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

IMPORTANT: Power consumption data readings are dependent on the configuration, architecture, components, and levels of activity of the server at any given time.

Table 41 lists the fields, buttons, and descriptions.

Table 41 Power Meter Readings Page Description

Fields and Buttons	Description
Power Meter Readings	Data is displayed using a bar graph. Each bar represents the power usage taken over a five minute interval. Peak and average power usage are displayed by default. You can display or hide peak, average, and minimum power samples by using the appropriate checkbox. Samples are collected over a 24-hour period. Samples are not retained over a management processor or server reset. Data can be displayed in Watts or Btu/hr. To display a tool tip that indicates the power usage, power regulator mode, temperature, and timestamp, pause the mouse over the particular sample on the bar graph.
Peak	Displays the peak power reading from the server over the last 24-hour period.
Average	Displays the average power reading from the server over the last 24-hour period.
Minimum	Displays the minimum power reading from the server over the last 24-hour period.
24-hour Power History Section	The 24-hour History section displays the average, maximum, and minimum power averages. The peak and minimum samples are recorded along with the average of the averages from the 24-hour time period.
Average Power	Displays the average of the power readings from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the average of all the readings since the server was booted.
Maximum Power	Displays the maximum power reading from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the maximum of all the readings since the server was booted.
Minimum Power	Displays the minimum power reading from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the minimum of all the readings since the server was booted.
Show values in BTu/hr	Changes the displayed data from watts to BTu/hr. and from BTu/hr. to watts.
Refresh Data	Refreshes the data graph.

Power Regulator

The Power Regulator page (Figure 33) enables you to view and modify the power efficiency regulator mode of the system.

The Power Regulator feature is available on systems where support is provided by the operating system, processors, processor dependant hardware (PDH), system firmware (SFW), and iLO 2 firmware.

On Integrity servers, power regulation requires the server to have both a CPU and an operating system that is capable of power regulation. Power regulation functions are available only when the OS is booted, and the system has the required hardware, firmware, OS, and software.

The Power Regulator feature does not require the Advanced Pack license.

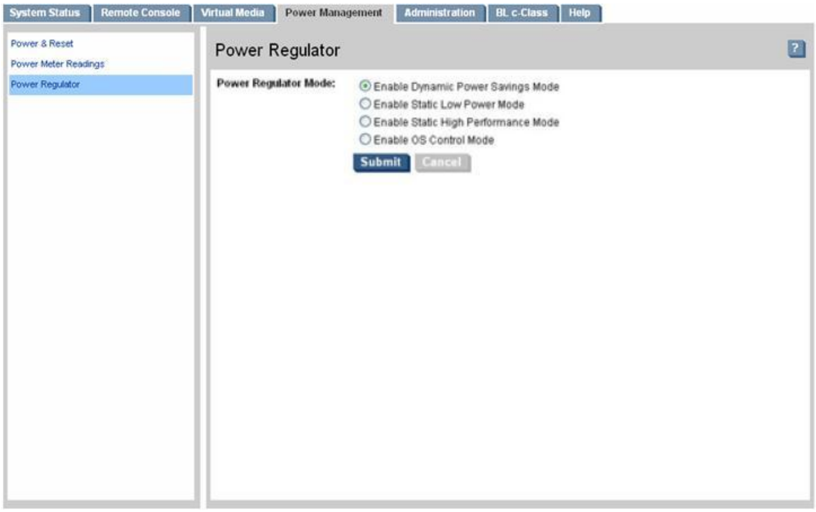
The following is required before you can use this feature:

- You must have the power control right to view and modify the power regulation modes.
- To access power and thermal history or the power regulator through IPM, requires both an IPM license and an iLO 2 (select or advanced) license.
- You must have a power-aware OS installed and running to use any mode of Power Regulation (static, dynamic, or OS control). Power Regulation on Integrity servers works in cooperation with the OS. For information on operating systems that currently support power regulation, see the HP website at:

  http://www.hp.com/go/integrityiLO.

NOTE: Depending on your server, this page might look slightly different.

Figure 33 Power Regulator Page



Power Regulator

Power Regulator Mode:
● Enable Dynamic Power Savings Mode
○ Enable Static Low Power Mode
○ Enable Static High Performance Mode
○ Enable OS Control Mode

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 42 lists the fields, buttons, and descriptions.

Table 42 Power Regulator Page Description

Fields and Buttons	Description
Power Regulator Mode	Three are four modes in which the power regulator can operate. The power regulator modes (Static Low, Static High and Dynamic) are independent of the operating system and work for any operating system. The OS Control Mode requires Microsoft Windows Server 2003 SP1 or later or Red Hat Linux 4 Update 2 or later.
Enable Dynamic Power Savings Mode	Sets the processors to the appropriate power level based on the utilization of each CPU core during the last 1/8 second. The CPU is set to the power saving processor power state if the CPU is operating at a utilization level that can be completed at the slower CPU frequency. The CPU is set to the maximum performance processor power state if the CPU is operating at a utilization level that requires the fastest CPU frequency.
Enable Static Low Power Mode	Sets the processor to the lowest supported processor state and forces the CPUs to stay in that lowest state. This mode saves the maximum amount of resources, but it might affect the system performance if processor utilization stays at or above 75% utilization.
Enable Static High Performance Mode	Sets the processor to the highest supported processor state and forces the CPUs to stay in that highest state. This mode ensures maximum performance, but it does not save any resources. This mode can be used to create a baseline of power consumption data without the power regulator.
Enable OS Control Mode	Configures the server to enable the operating system to control the processor power states. This is the necessary setting for OS power management. Moving from this state to any of the three previous states does not require a server reboot because Integrity iLO 2 power regulation works in cooperation with the OS. (This is different from ProLiant iLO power regulation).
Submit	Submits the selected function.
Cancel	Cancels the action.

The power regulation functionality is achieved through two different interfaces:

- **Power Regulation through HP SIM (using the HP IPM plug in)**

  HP Insight Power Manager (HP IPM), a plug-in to HP Systems Insight Manager (HP SIM), is an integrated power monitoring and management application that provides centralized control of server power consumption and thermal output. It extends the unified infrastructure management framework of HP SIM by providing new energy levers into the server. Leveraging HP power regulator technology, HP IPM makes policy-based power and thermal management possible. It expands the capacity of data centers by reducing the amount of power and cooling required for supported Integrity servers and the server blades.

  An Advanced Pack license is required to use the power regulation feature through the IPM.

  Information on HP IPM is available on the HP website at http://www.hp.com/go/ipm.

- **Power Regulation through the iLO 2**

  The iLO 2 reads ACPI registers to gather information and display the current power efficiency mode of the system. The available power regulator mode settings are sent to the OS through an ACPI interface. If the OS is able to respond to the settings, it sets return codes to note success or failure to reach these settings.

  You do not need an Advanced Pack license to use the power regulation feature through iLO 2.

Administration

The Administration tab enables you to access the following pages:

- Firmware Upgrade
- Licensing
- Local Accounts
- Group Accounts
- Settings
- Access Settings: LAN, Serial, and Login Options
- Directory Settings: LDAP Parameters
- Network Settings: Standard and Domain Name Server
- BL c-Class (Available only for server blade.)
- SNMP Settings
- Help

Firmware Upgrade

The Firmware Upgrade page functionality is only available to authorized HP service personnel.

The MP firmware is packaged along with system, BMC, and FPGA/PSOC firmware. To perform a firmware upgrade, you can download and upgrade the firmware package from the HP website at http://www.hp.com/go/bizsupport.

IMPORTANT: When performing a firmware upgrade that contains system programmable hardware (FPGA, EFI, PSOC, BMC), you must properly shut down any OS that is running before starting the firmware upgrade process.

Select **Download drivers and software**, select your server, and follow the directions provided.

After the upgrade, reconnect and log in as user **`Admin`** and password **`Admin`** (case sensitive).

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

Licensing

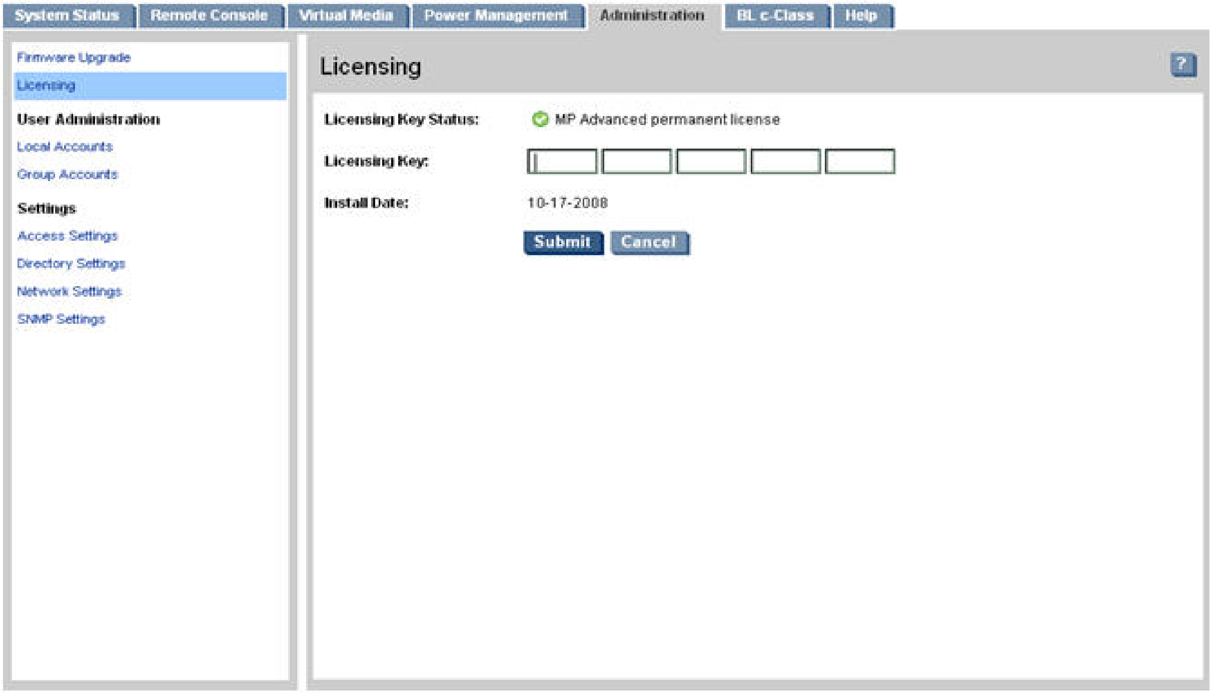
The Licensing page (Figure 34) is used to enter a license key to enable the iLO 2 Advanced Pack features.

NOTE: Licensing keys are not used with cell-based servers, the Lights-Out Advanced KVM card is used instead. For information on the Lights-Out Advanced KVM card, see Chapter 5 (page 49).

IMPORTANT: A HP ProLiant iLO 2 Advanced Pack license key will not work on an HP Integrity server, and vice versa.

NOTE: Depending on your server, this page might look slightly different.

Figure 34 Licensing Page



Licensing

Licensing Key Status: MP Advanced permanent license

Licensing Key:

Install Date: 10-17-2008

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

IMPORTANT: On HP Integrity server blades, an Advanced Pack license is standard. Remember to save the Advanced Pack license key information that was provided by HP. If you ever need to replace your server blade under warranty, you will need to transfer the key by entering the code on the replacement server blade.

Integrity iLO 2 offers some advanced features, which can be used only with the iLO 2 Advanced Pack license:

- Virtual Media
- Integrated Remote Console
- Directory-based authentication and authorization using LDAP

- LDAP schema-free integration
- Integration with Insight Power Manager

Table 43 lists the fields, buttons, and descriptions.

Table 43 Licensing Page Description

Fields and Buttons	Description
Licensing Key Status	The status of the license - inactive if no license has been installed, the type of the license (Evaluation or Permanent), and the number of days remaining if the license installed is an Evaluation license.
Licensing Key	Enter the 25-character HP Integrity license key used to enable the iLO 2 Advanced Pack features. Fields are case sensitive.
Install Date	Displays the date the license was installed.
Submit	Submits the key for activation.
Cancel	Cancels the action.

Integrity iLO provides a mechanism to install a license key which unlocks the advanced pack features. There are two types of licenses:

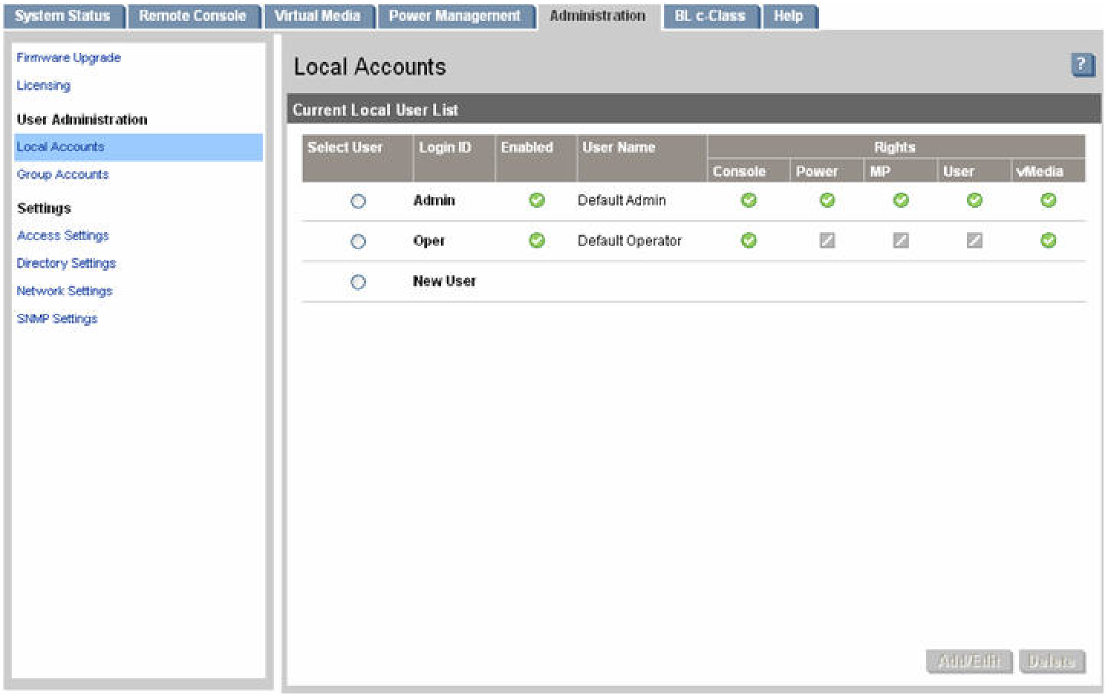
1. iLO 2 Advanced Evaluation License, a 30-day evaluation license allows usage of advanced features for 720 hours of iLO 2 uptime.
2. iLO 2 Advanced Permanent License allows perpetual use of the advanced features.

User Administration > Local Accounts

The Local Accounts page (Figure 35) displays the current list of users, their privilege rights and whether they are enabled or disabled, and the mode (CM, MA, VFP). This page enables you to modify the user configuration of iLO 2, add new users assign rights, and modify or delete existing users. You must have administration access right to use this feature.

NOTE: Depending on your server, this page might look slightly different.

Figure 35 Local Accounts Page



Local Accounts

Current Local User List

Select User	Login ID	Enabled	User Name	Rights				
				Console	Power	MP	User	vMedia
○	Admin	✓	Default Admin	✓	✓	✓	✓	✓
○	Oper	✓	Default Operator	✓	▨	▨	▨	✓
○	New User							

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

There are two default users:

1. Admin: The Admin user has all five rights (console access, power control, MP configuration, user administration, virtual media).
2. Oper: The Oper user has the login and console access rights by default.

Table 44 lists the fields and descriptions.

Table 44 Local Accounts Page Description

Field	Description
Select User	Select an existing user from the list of user names to edit or delete that account or select **New User** to add a new user.
Add/Edit	Click this button after selecting the user account to modify or to add a new account. For an existing account, you can modify any of the parameters shown, provided the user has sufficient privileges. By default, a new user is granted the login and console access right, their operating mode is set to multiple logins and the user is enabled.
Delete	Click this button after selecting the user account to delete. If you do not have the user administration access right, this button is disabled.

Group Accounts

The Group Accounts page (Figure 36) enables you to enter one or more directory groups by specifying the distinguished name of the group and privileges that should be granted to users who are members of that group.

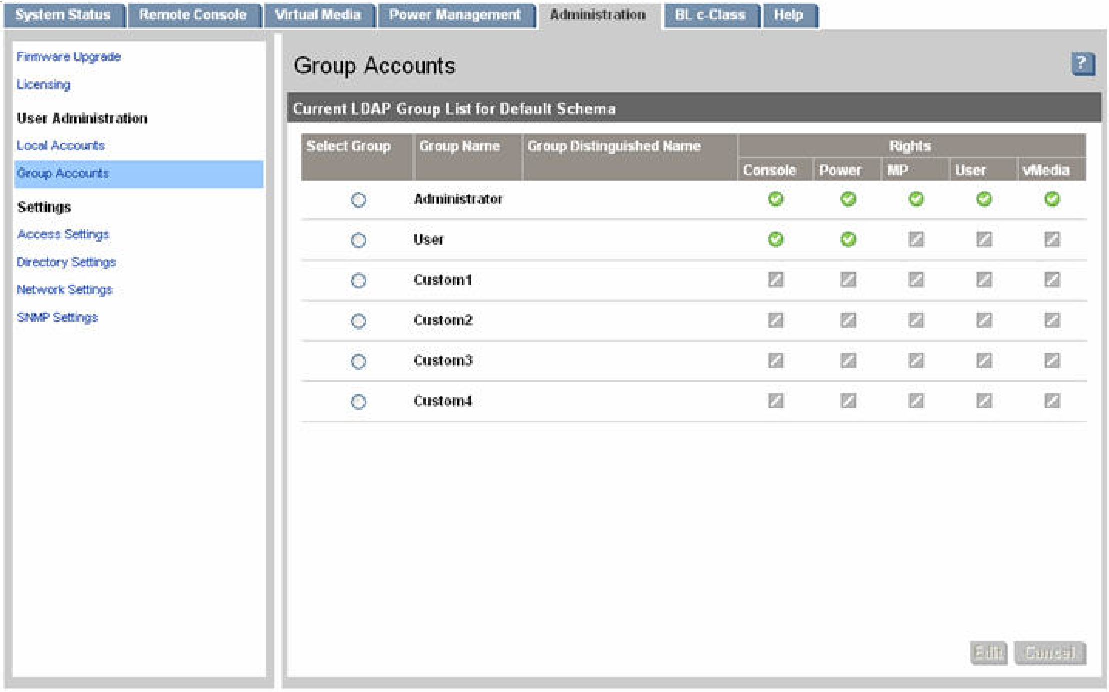
You must configure group administration information when the directory is enabled with the default schema.

When a user attempts to login into iLO 2, iLO 2 reads that user’s directory name in the directory to determine the groups the user is a member of. iLO 2 compares this information with a list of groups configured by the user. The rights of all the matched groups are combined and assigned to that user.

This feature is only available if you have the iLO 2 Advanced Pack license.

NOTE: Depending on your server, this page might look slightly different.

Figure 36 Group Accounts Page



Group Accounts

Current LDAP Group List for Default Schema

Select Group	Group Name	Group Distinguished Name	Rights				
			Console	Power	MP	User	vMedia
○	Administrator		✓	✓	✓	✓	✓
○	User		✓	✓	☒	☒	☒
○	Custom1		☒	☒	☒	☒	☒
○	Custom2		☒	☒	☒	☒	☒
○	Custom3		☒	☒	☒	☒	☒
○	Custom4		☒	☒	☒	☒	☒

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 45 lists the fields, buttons, and descriptions.

Table 45 Group Accounts Page Description

Fields and Buttons	Description
Administrator	Click **Administrator** and click **Edit** to open the Group Settings page and enter information.
User	Click **User** and click **Edit** to open the Group Settings page and enter information.
Custom (1,2,3,4)	Click **Custom 1,2,3,4** and click **Edit** to open the Group Settings page and enter information
Edit	Opens the Group Settings page.
Cancel	Cancels the action.

Access Settings

The Access Settings tab enables you to access the following pages:

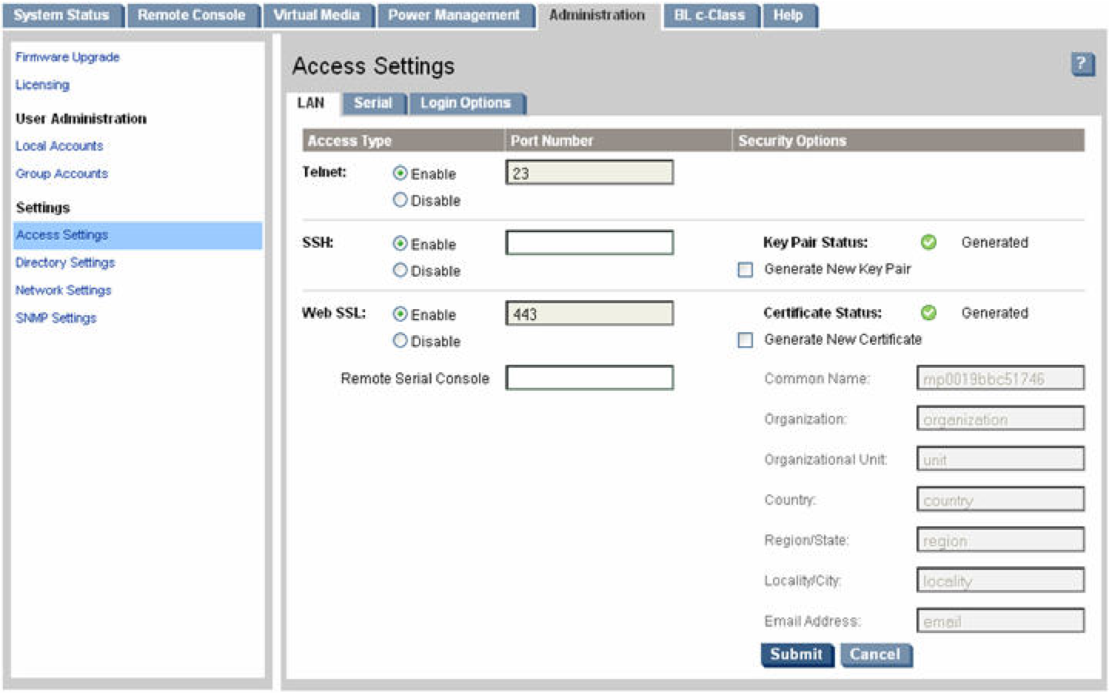
- LAN
- Serial
- Login Options

LAN

The LAN page (Figure 37) enables you to modify LAN settings. You must have iLO configuration access right to use this feature.

NOTE: Depending on your server, this page might look slightly different.

Figure 37 LAN Page



Access Settings

Access Type		Port Number	Security Options		
Telnet:	● Enable ○ Disable	23			
SSH:	● Enable ○ Disable		Key Pair Status: □ Generate New Key Pair	✓	Generated
Web SSL:	● Enable ○ Disable	443	Certificate Status: □ Generate New Certificate	✓	Generated
Remote Serial Console			Common Name:	mp0019bbc51746	
			Organization:	organization	
			Organizational Unit:	unit	
			Country:	country	
			Region/State:	region	
			Locality/City:	locality	
			Email Address:	email	

Submit Cancel

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 46 lists the fields, buttons, and descriptions.

Table 46 LAN Page Description

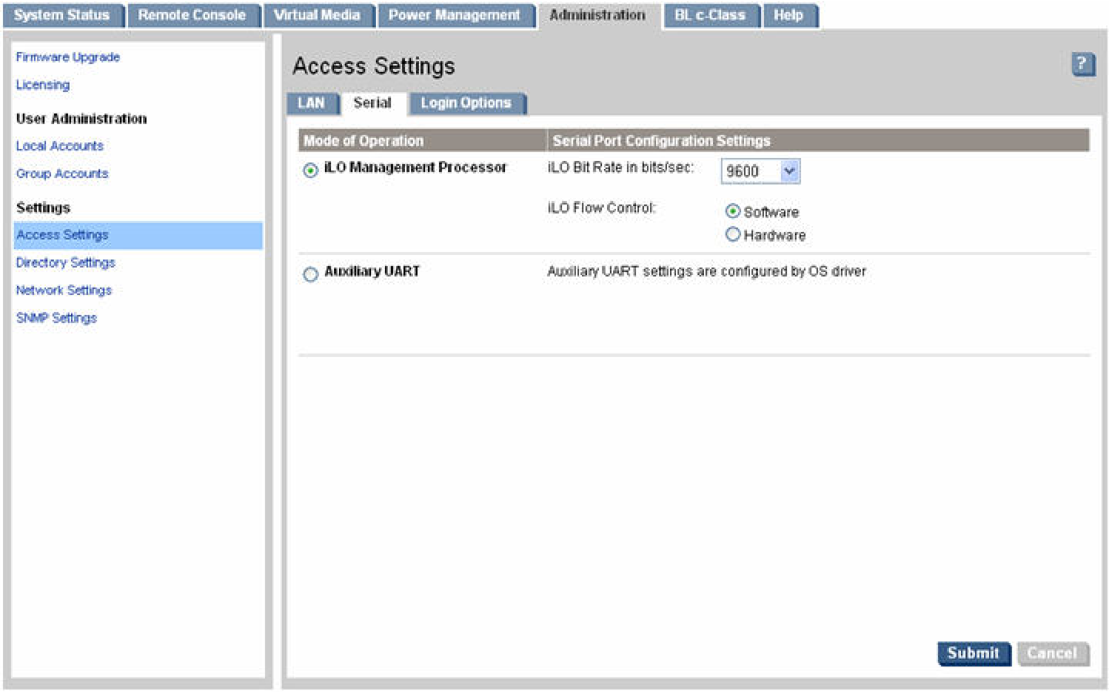
Fields and Buttons	Description
Telnet	You can enable or disable Telnet access to iLO 2 using the enable or disable option.
SSH	You can enable or disable SSH access to the iLO 2 using the enable or disable option. An industry-standard client-server connectivity protocol that provides a secure remote connection. The iLO 2 supports: • SSH2 implementation • Authentication algorithms RSA and DSA • Encryption algorithms 3DES-CBC and AES128-CBD • Integrity algorithms HMAC-SHA1 and MD5
Web SSL	You can enable or disable the web SSL access to iLO 2 using the enable or disable option. In order to make an SSL connection, you need to generate a certificate. The certificate status indicates if a certificate has been generated previously. To generate a new certificate, fill in the fields shown and check **Generate New Certificate**. The system alerts you when the certificate is about to expire or if it has already expired. You will need to generate a new certificate before you can continue. You must reset the iLO MP after you generate a new certificate.
Submit	Submits the information.
Cancel	Cancels the action.

Serial Page

The Serial page (Figure 38) enables you to set the serial port parameters. You must have iLO configuration access right to use this feature.

NOTE: Depending on your server, this page might look slightly different.

Figure 38 Serial Page



Access Settings

Mode of Operation	Serial Port Configuration Settings
● iLO Management Processor	iLO Bit Rate in bits/sec: 9600 iLO Flow Control: ● Software ○ Hardware
○ Auxiliary UART	Auxiliary UART settings are configured by OS driver

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 47 lists the fields, buttons, and descriptions.

Table 47 Serial Page Description

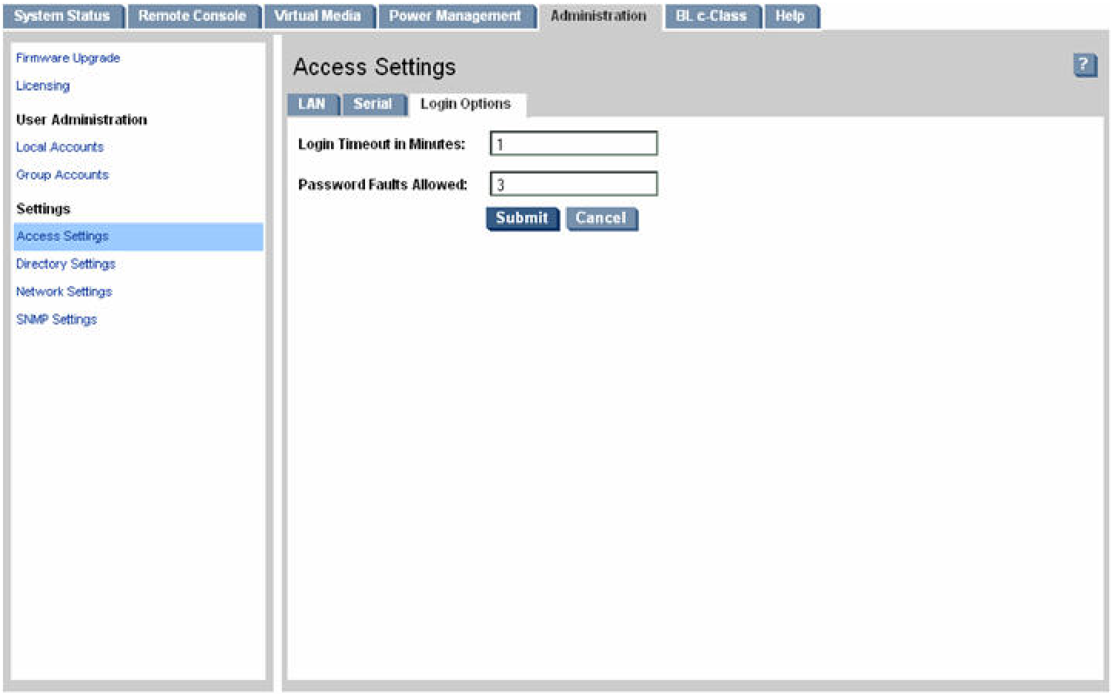
Fields and Buttons	Description
Bit Rate in Bits per Second	This option enables you to set the baud rate. Input and output data rates are the same.
Flow Control	Flow control can be through hardware or software. Hardware uses RTS/CTS; software uses Xon or Xoff.
Submit	Submits the information.
Cancel	Cancels the action.

Login Options Page

The Login Options page (Figure 39) enables you to modify the security options of iLO 2. You must have iLO configuration access right to use this feature.

NOTE: Depending on your server, this page might look slightly different.

Figure 39 Login Options Page



Access Settings

Login Timeout in Minutes: 1

Password Faults Allowed: 3

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 48 lists the fields, buttons, and descriptions.

Table 48 Login Options Page Description

Fields and Buttons	Description
Login Timeout in Minutes	The timeout value in minutes is effective on all ports, including local ports.
Password Faults Allowed	This sets a limit on the number of password faults allowed when logging in to iLO 2. The default number of password faults allowed is three.
Submit	Submits the information.
Cancel	Cancels the action.

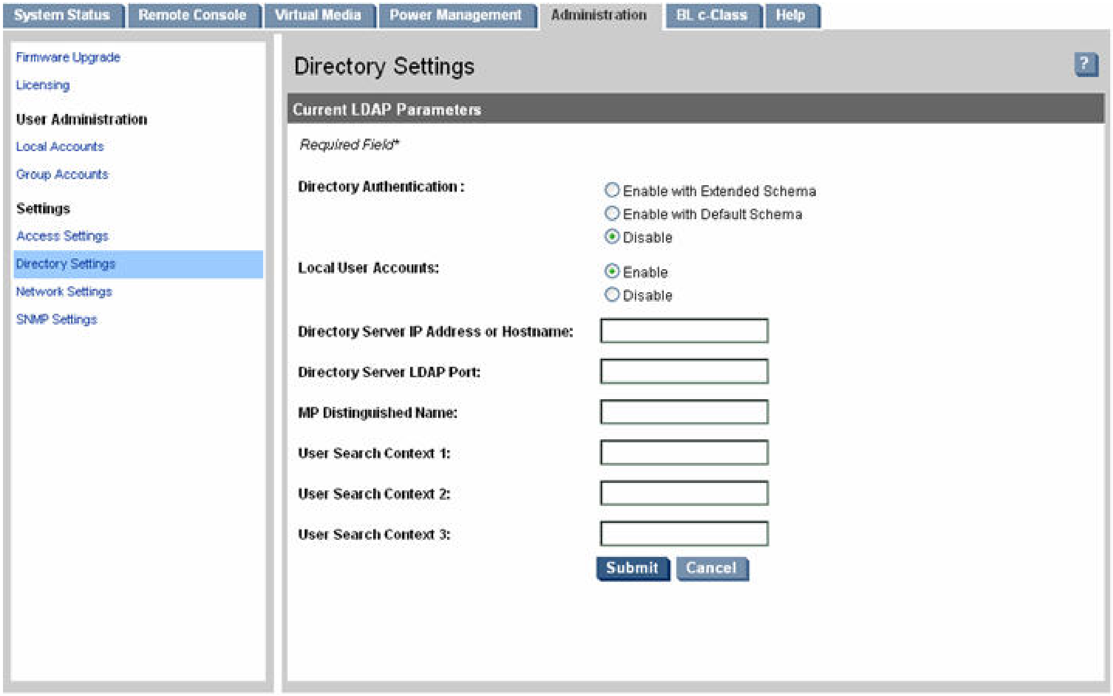
Current LDAP Parameters

The Current LDAP Parameters page (Figure 40) enables you to edit LDAP parameters. You must have iLO configuration access right to use this feature.

The LDAP feature is only available if you have the iLO 2 Advanced Pack license.

NOTE: Depending on your server, this page might look slightly different.

Figure 40 Current LDAP Parameters Page



Directory Settings

Current LDAP Parameters

*Required Field**

Directory Authentication : ○ Enable with Extended Schema ○ Enable with Default Schema ● Disable

Local User Accounts: ● Enable ○ Disable

Directory Server IP Address or Hostname:

Directory Server LDAP Port:

MP Distinguished Name:

User Search Context 1:

User Search Context 2:

User Search Context 3:

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 49 lists the fields and descriptions.

Table 49 Current LDAP Parameters Page Description

Field	Description
Directory Authentication	Choosing enable or disable, activates or deactivates directory support on iLO 2: • Enable with Extended Schema: selects directory authentication and authorization using directory objects created with HP schema. Select this option if the directory server has been extended with the HP schema. • Enable with Default Schema: selects directory authentication and authorization using user accounts in the directory which has not been extended with the HP schema. User accounts and group memberships are used to authenticate and authorize users. Data in the Group Administration page must be configured after this option is selected.
Local User Accounts	Includes or excludes access to local iLO 2 user accounts. Locally-stored user accounts can be active while LDAP directory support is enabled. If local user accounts are enabled, you may log in to the iLO 2 using locally-stored user credentials. If they are disabled, access is limited to valid directory credentials only.
Directory Server IP Address	IP address of the directory server.
Directory Server LDAP Port	Port number for the secure LDAP service on the server. The default value for this port is 636.
Distinguished Name	Distinguished Name of iLO 2, specifies where this iLO 2 instance is listed in the directory tree. Example: cn=MP Server,ou=Management Devices,o=hp
User Search Contexts (1,2,3)	User name contexts are used to locate an object in the tree structure of the directory server and applied to the login name entered to access iLO 2. **NOTE:** For instances when user authentication uses the LDAP directory server that is configured for Microsoft Active Directory, a user can log in using the username format `user@domain.hp.com`. Currently, this user credential format is only supported on Internet Explorer.

Table 49 Current LDAP Parameters Page Description *(continued)*

Field	Description
Submit	Submits the information.
Cancel	Cancels the action.

Network Settings

The Network Settings tab enables you to access the following pages:

- Standard
- Domain Name Server

IMPORTANT: If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 2 automatically resets once you confirm the change. The automatic reset occurs only after a warning displays before you commit the changes. If you enter `-nc`, no warning displays and iLO 2 reboots.

If you are connected through a serial console and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 2 alerts you to manually reset iLO 2. A warning about dropped network connections is sent prior to committing the change. The warning does not display if you enter `-nc`.

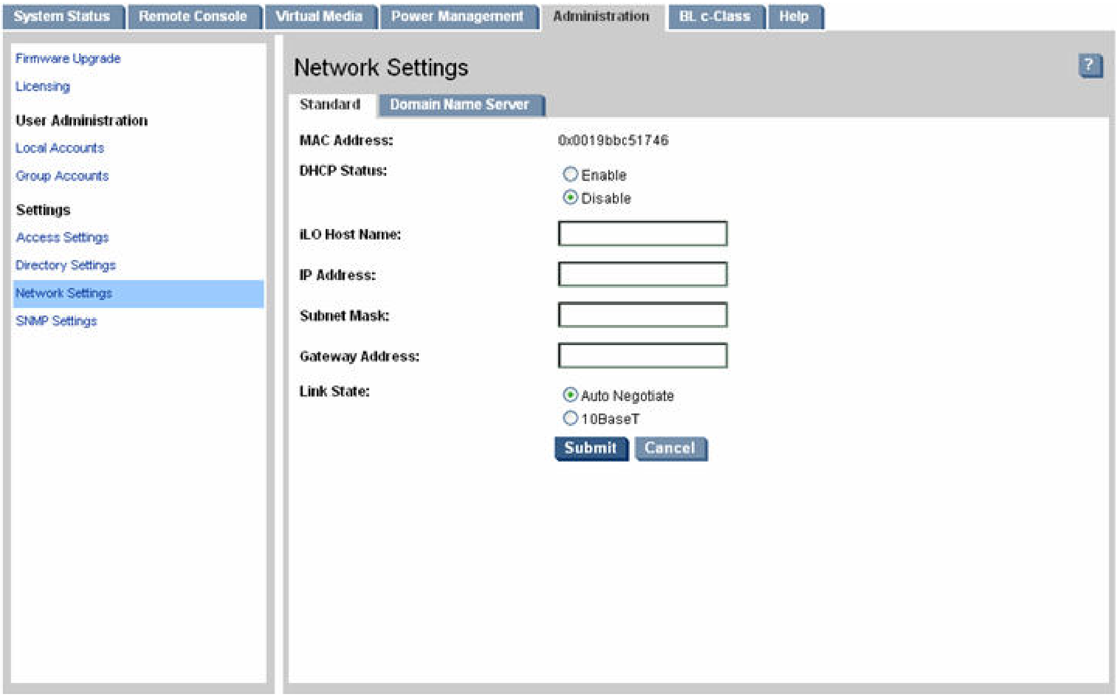
If a firmware upgrade is in progress, the commitment phase to the `LC` command fails and indicates that an upgrade or reset is in progress and changes to the `LC` parameters are not made.

Network Settings > Standard

The Standard page (Figure 41) enables you to configure the network settings and LAN configuration. You must have iLO configuration access right to configure the network settings.

NOTE: Depending on your server, this page might look slightly different.

Figure 41 Standard Page



Network Settings

MAC Address: 0x0019bbc51746

DHCP Status: ○ Enable ● Disable

iLO Host Name:

IP Address:

Subnet Mask:

Gateway Address:

Link State: ● Auto Negotiate ○ 10BaseT

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 50 lists the fields, buttons, and descriptions.

Table 50 Standard Page Description

Fields and Buttons	Description
MAC Address	The 12 digit (hexadecimal) MAC address.
DHCP Status	Enable or Disable.
iLO 2 MP Host Name	The host name set here is displayed at the iLO 2 command interface prompt.
IP Address	The iLO 2 MP IP address. If DHCP is being used, the IP address is automatically supplied.
Subnet Mask	The subnet mask for the iLO 2 IP network. If DHCP is being used, the subnet mask is automatically supplied.
Gateway Address	The IP address of the network gateway. If DHCP is being used, the gateway IP address is automatically supplied.
Link State	Auto Negotiate or 10 BaseT option.
Submit	Submits the information.
Cancel	Cancels the action.

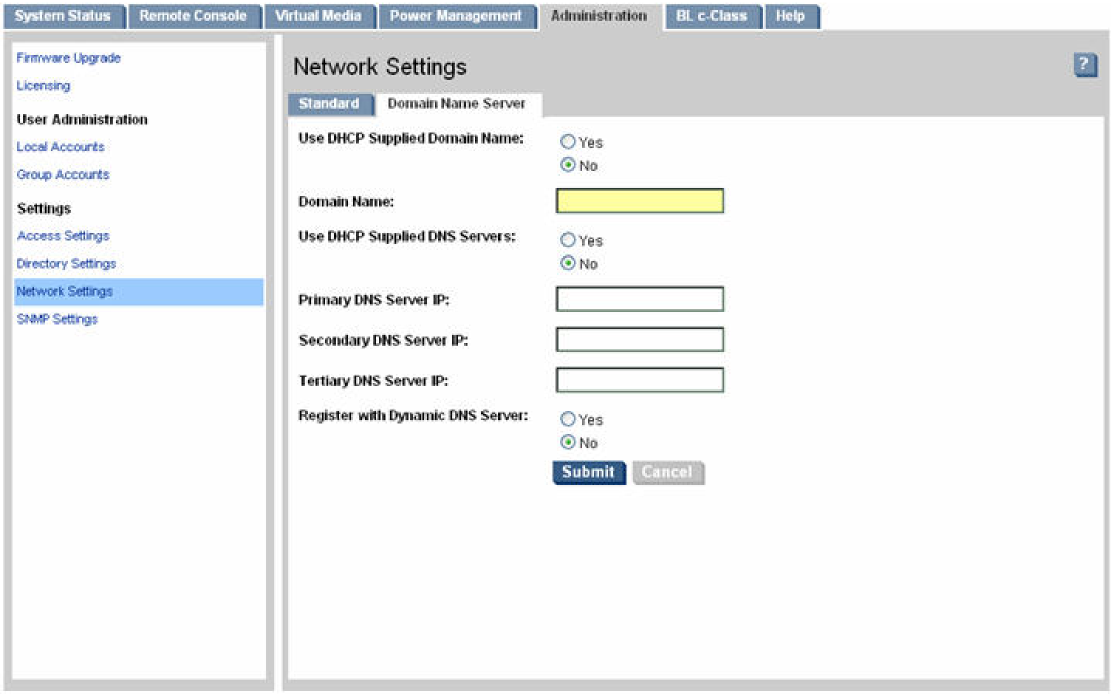
Domain Name Server

The Domain Name Server (DNS) page (Figure 42) enables you to configure the DNS server settings, domain name, and up to three DNS servers manually or automatically through DHCP. It further enables a DDNS update through the primary DNS server as long as it is authoritative for the zone. You must have iLO configuration access right to use this feature.

You can only configure the DNS server if DHCP is enabled.

NOTE: Depending on your server, this page might look slightly different.

Figure 42 Domain Name Server Page



Network Settings

Use DHCP Supplied Domain Name: ○ Yes ● No

Domain Name:

Use DHCP Supplied DNS Servers: ○ Yes ● No

Primary DNS Server IP:

Secondary DNS Server IP:

Tertiary DNS Server IP:

Register with Dynamic DNS Server: ○ Yes ● No

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 51 lists the fields, buttons, and descriptions.

Table 51 DNS Page Description

Fields and Buttons	Description
Use DHCP supplied domain name	Use the DHCP server-supplied domain name.
Domain name	This represents the factory-default DNS name of the subsystem, for example, "hp.com" in "ilo.hp.com". You can enter a new DNS name.
Use DHCP supplied DNS servers	Use the DHCP server-supplied DNS server list.
Register with Dynamic DNS	Register its name with a DDNS server.
Submit	Submits the DNS information.
Cancel	Cancels the action.

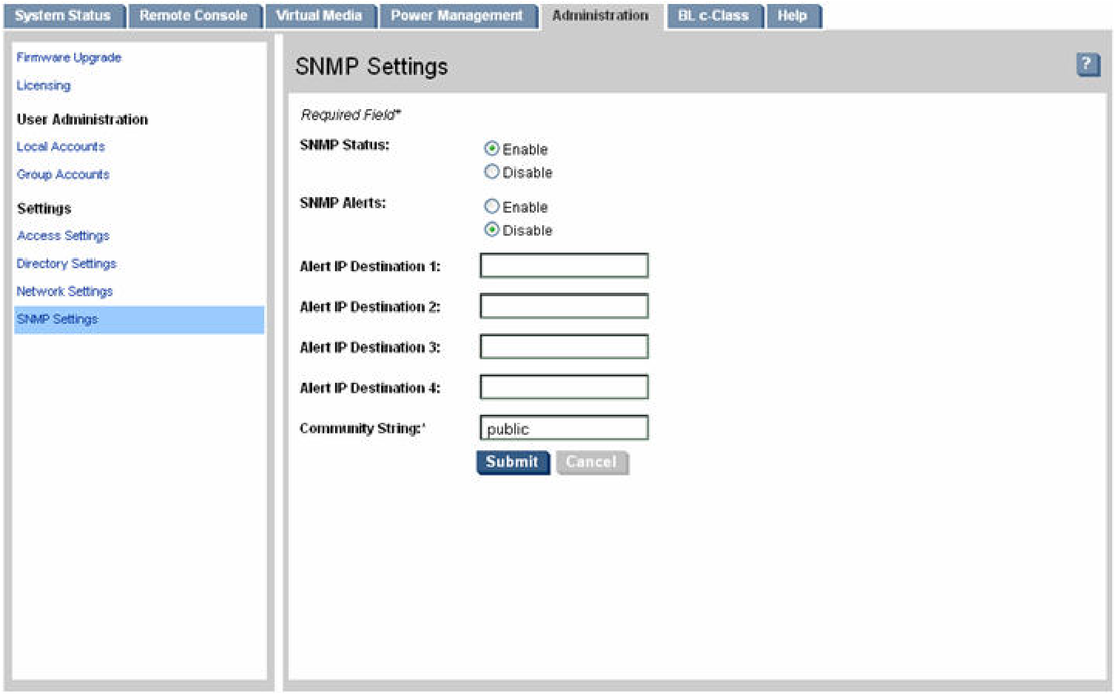
SNMP Settings

The SNMP Settings page (Figure 43) enables you edit SNMP feature settings.

You must have iLO configuration access right to use this feature.

NOTE: Depending on your server, this page might look slightly different.

Figure 43 SNMP Settings Page



SNMP Settings

*Required Field**

SNMP Status: ● Enable ○ Disable

SNMP Alerts: ○ Enable ● Disable

Alert IP Destination 1:

Alert IP Destination 2:

Alert IP Destination 3:

Alert IP Destination 4:

Community String:* public

Submit Cancel

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 52 lists the fields and descriptions.

Table 52 SNMP Settings Page Description

Field	Description
SNMP	Choosing **Enable** or **Disable**, activates or deactivates the SNMP feature support on this iLO 2.
SNMP Alerts	Enter **E** to enable or **D** to disable all SNMP alerts.

Table 52 SNMP Settings Page Description *(continued)*

Field	Description
	Enter **`1, 2, 3, 4`** to configure a destination IP address for SNMP alerts. The default is **blank** (unused).
Community String	Configure the community string to secure the access to the management information base (MIB) objects. The default is **public**.
Submit	Submits the information.
Cancel	Cancels the action.

NOTE: If SNMP was disabled earlier and then enabled, you will receive the following message:

```
Reset MP (XD command option 'R') for configuration to take effect.
```

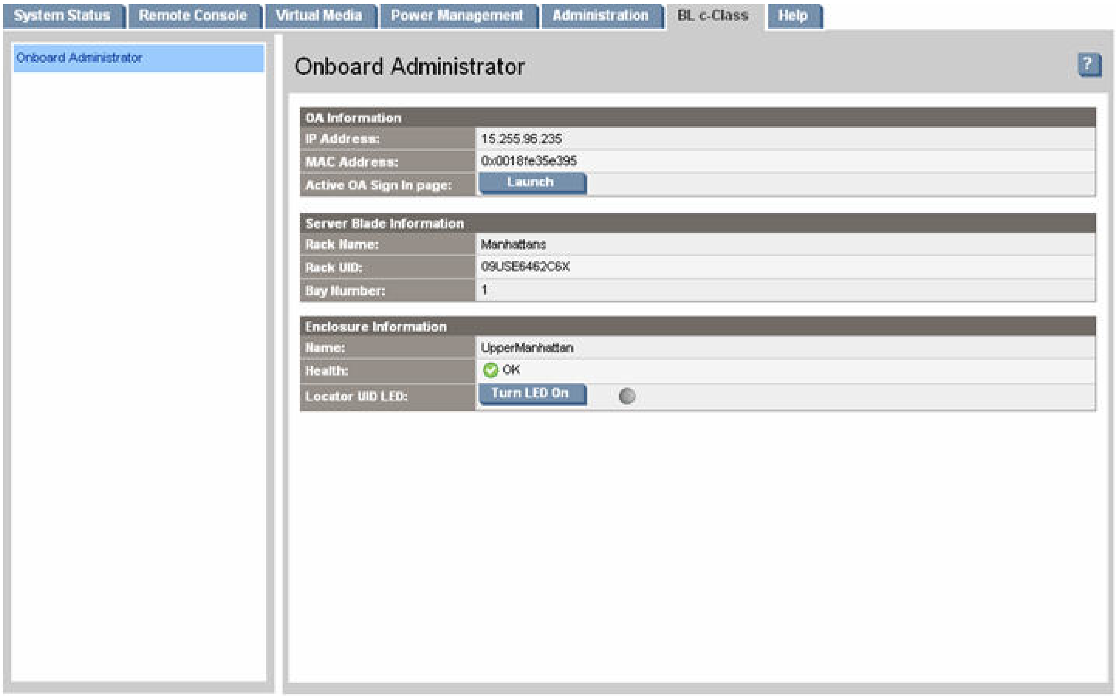
Click **OK** and reset iLO 2.

BL c-Class

The Onboard Administrator page (Figure 44) is used to facilitate the cabling and initial installation of servers blade. It also provides a quick view of the enclosure status. You must have configuration access right to turn the enclosure locator UID LED on or off.

NOTE: Depending on your server, this page might look slightly different.

Figure 44 Onboard Administrator



Onboard Administrator

OA Information	
IP Address:	15.255.96.235
MAC Address:	0x0018fe35e395
Active OA Sign In page:	Launch

Server Blade Information	
Rack Name:	Manhattans
Rack UID:	09USE6462C6X
Bay Number:	1

Enclosure Information	
Name:	UpperManhattan
Health:	✓ OK
Locator UID LED:	Turn LED On ●

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

Table 53 lists the fields and descriptions.

Table 53 Onboard Administrator Page Description

Field	Description
OA IP Address	The IP address of the OA. **IMPORTANT:** Integrity iLO 2 must have a reachable IP address as the default gateway address. Since the OA is always reachable, HP recommends using the OA IP address as the gateway address for Integrity iLO 2. If you use the Enclosure IP mode, this solution works during a failover. In the Enclosure IP mode, a static IP address is assigned to the active OA, and during a failover, the same IP address follows the active OA. If the OA IP address is assigned using DHCP, the solution does not work. In such instances, HP recommends manually changing the iLO 2 gateway address.
OA MAC Address	The MAC address of the OA.
Active OA Sign In Page	Click this button to launch the Onboard Administrator Sign In page.
Rack Name	This is used to logically group together enclosures in a rack. The rack name is shared with the other enclosures in the rack.
Rack UID	This is the rack unique identifier.
Bay Number	The enclosure can support as many as eight HP Integrity server blades. When viewed from the rack front, the bays are numbered from left to right and from 1 to 8. The bay number is used to locate and identify a server blade.
Enclosure Name	This is used to logically group together the server blades installed in the same enclosure. The enclosure name is shared with the other servers in the enclosure.
Enclosure Health	This displays the health of the enclosure.
Enclosure Locator UID LED	This allows you to turn the enclosure Locator UID LED on or off. The iLO Configuration access right is needed. If a user does not have sufficient rights, the button is disabled.

Before setting up the HP BladeSystem OA, HP recommends that you read the *HP BladeSystem Onboard Administrator User Guide* on the HP website at:

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00705292/c00705292.pdf

Reading this guide ensures that you will obtain an overall understanding of the HP BladeSystem OA and that you properly complete the initial setup to facilitate proper functioning of the OA.

The *HP BladeSystem Onboard Administrator User Guide* provides the following information in detail:

- Access Requirements
- Running the OA for the first time
- Signing in to the OA GUI
- Running the setup wizard
- Using online help
- Changing enclosure and device configurations
- Recovering the administrator password
- Flash disaster recovery

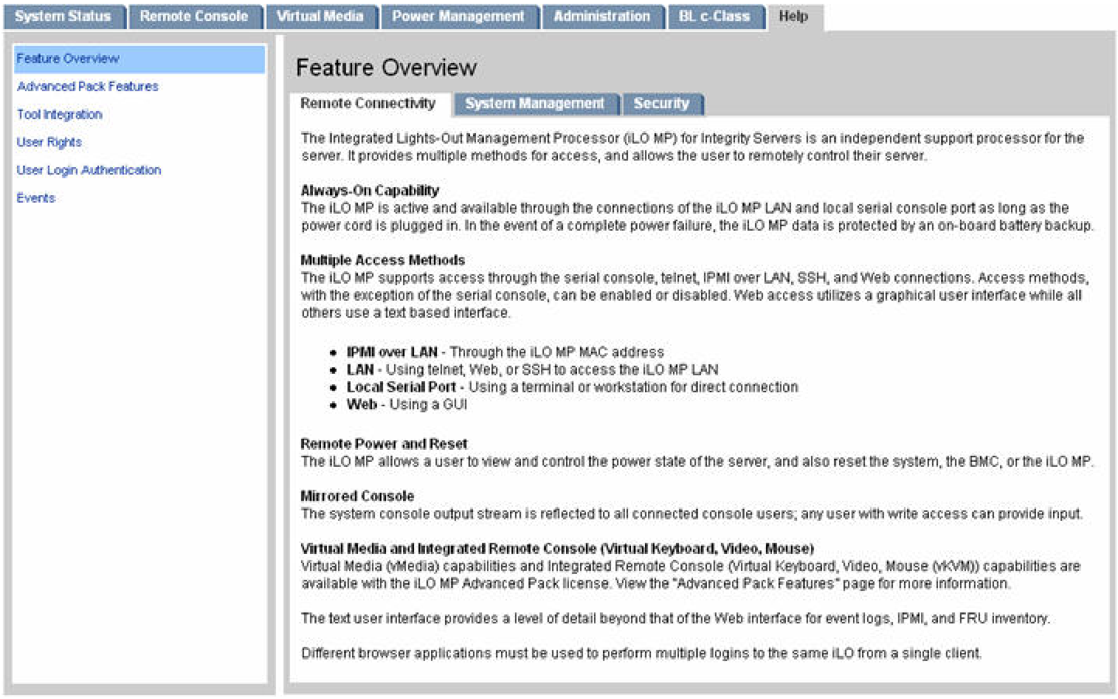
Help

The iLO 2 has a robust help system.

To access iLO 2 help, click the Help tab.

NOTE: Depending on your server, this page might look slightly different.

Figure 45 Help Page



Feature Overview

The Integrated Lights-Out Management Processor (iLO MP) for Integrity Servers is an independent support processor for the server. It provides multiple methods for access, and allows the user to remotely control their server.

Always-On Capability
The iLO MP is active and available through the connections of the iLO MP LAN and local serial console port as long as the power cord is plugged in. In the event of a complete power failure, the iLO MP data is protected by an on-board battery backup.

Multiple Access Methods
The iLO MP supports access through the serial console, telnet, IPMI over LAN, SSH, and Web connections. Access methods, with the exception of the serial console, can be enabled or disabled. Web access utilizes a graphical user interface while all others use a text based interface.

- **IPMI over LAN** - Through the iLO MP MAC address
- **LAN** - Using telnet, Web, or SSH to access the iLO MP LAN
- **Local Serial Port** - Using a terminal or workstation for direct connection
- **Web** - Using a GUI

Remote Power and Reset
The iLO MP allows a user to view and control the power state of the server, and also reset the system, the BMC, or the iLO MP.

Mirrored Console
The system console output stream is reflected to all connected console users; any user with write access can provide input.

Virtual Media and Integrated Remote Console (Virtual Keyboard, Video, Mouse)
Virtual Media (vMedia) capabilities and Integrated Remote Console (Virtual Keyboard, Video, Mouse (vKVM)) capabilities are available with the iLO MP Advanced Pack license. View the "Advanced Pack Features" page for more information.

The text user interface provides a level of detail beyond that of the Web interface for event logs, IPMI, and FRU inventory.

Different browser applications must be used to perform multiple logins to the same iLO from a single client.

NOTE: The BL c-Class tab is available only on HP Integrity server blades.

You can also click the **?** at the top right corner of each page to display help about the page you are on.

Select any of the topics listed in the left navigation bar to access that particular help screen.

SMASH Server Management Command Line Protocol

The Systems Management Architecture for Server Hardware (SMASH) initiative is an effort within the Distributed Management Task Force (DMTF) to standardize commands for servers. The Server Management Command Line Protocol (SM CLP) specifies common command line syntax and message protocol semantics for server management.

IMPORTANT:

- The current DMTF CLI implementation is a prestandard release and is subject to change.
- SMASH SM CLP is not the primary text user interface (TUI) or the primary scripting interface for iLO 2.
- The HP proprietary TUI is the primary text interface of iLO 2.
- The entire text user interface of iLO 2, available on Telnet and SSH, supports all MP functionality.
- SMASH CLP does not support all iLO 2 features, and is a prototype implementation only.
- SMASH CLP is only available for entry class servers.

SM CLP Features and Functionality Overview

SM CLP includes the following features:

- Provides a user-friendly method to view and manage server information with commands in formats that facilitate scripting.
- Offered in addition to the iLO 2 existing CLI.

- Uses scripts to automate some iLO 2 tasks, especially when you are setting up many identical servers.
- Available from any TUI (serial, Telnet, and SSH).
- CLP sessions are independent from each other and nonmirrored.
- Provides a subset of MP CLI commands.
- Provides access to the MP Main Menu interface and system console interface.

SM CLP Session

Sessions between a client and an SM CLP service are established over a transport protocol. Once the session is authenticated, the client begins to submit commands using the SM CLP service.

The CLP is a command and response protocol (not a command-line interface). Each CLP command is sent over the transport protocol to iLO 2. The command is received and processed by iLO 2, which then transmits a response back to the CLP client. There are no interactive commands, so no state information is retained.

The privilege level of the logged-in user is checked against the privilege required for the command. The command is run only if a user has the privilege level required for that command.

Accessing the SM CLP Interface

When you log in to the iLO 2 MP, by default you access the MP Main Menu interface. To use the SM CLP:

1. Access the MP Main Menu.
2. At the MP Main Menu, enter **SMCLP** to access SM CLP. The screen displays the SM CLP `hpiLO->` prompt.

```
 MP MAIN MENU:

         CO: Console
        VFP: Virtual Front Panel
         CM: Command Menu
      SMCLP: Server Management Command Line Protocol
         CL: Console Log
         SL: Show Event Logs
         HE: Main Help Menu
          X: Exit Connection

[hqgstlv7] MP>
[hqgstlv7] MP> SMCLP

HP SMASH SM CLP interface.

Type "help" to display all supported commands.
Type "show" to display information about the current target.
Type "start /map1/textredirectsap1" to switch to iLO Main Menu interface.

=== SMCLP v1.0.0 Hewlett-Packard Company ===

</> hpiLO->
```

Exiting the SM CLP Interface

To terminate an SM CLP session and disconnect from iLO 2, use the `exit` command. To switch from SM CLP to the MP Main Menu interface, use the `start /map1/textredirectsap1` command.

Changing the iLO 2 Default Interface to SM CLP

The iLO 2 has a configurable setting that enables you to select your default interface, MP Main Menu or SM CLP.

To change the default interface from MP Main Menu to SM CLP:

1. At the MP Main Menu, enter **CM**.
2. From the CM prompt, enter **SA** to modify iLO 2 access configuration.
3. Use the following example as you follow the prompts on the screen to change the default interface from MP Main Menu to SM CLP.

```
MP:CM>SA

This command allows you to modify MP access configuration.

Current Set Access Configuration:
     R - Remote        : OS SESSION
     T - Telnet        : Enabled
     H - SSH           : Disabled
     W - Web SSL       : Enabled
     I - IPMI over LAN : Enabled
     C - Command Mode  : MP Menu
Enter parameter(s) to change, A to modify All, or [Q] to Quit: c
c
For each parameter, enter:
     New value, or
     <CR> to retain the current value, or
     DEFAULT to set the default value, or
     Q to Quit

Default Command Mode Configuration:
   Current -> M - MP Menu (default)
              S - SM CLP

Enter new value, or Q to Quit: s
s
    -> Default Command Mode Configuration will be updated

New Set Access Configuration (* modified values):
     R - Remote        : OS SESSION
     T - Telnet        : Enabled
     H - SSH           : Disabled
     W - Web SSL       : Enabled
     I - IPMI over LAN : Enabled
   * C - Command Mode  : SM CLP

Enter Parameter(s) to revise, Y to confirm, or [Q] to Quit: y
y
     -> Set Access Configuration has been updated.

MP:CM>
```

Using the SM CLP Interface

After initiating an SM CLP session, the iLO 2 CLP prompt appears. Each time a command is run, the CLP prompt appears as shown in the following example.

```
<current default target>hpiLO->
```

Where `<current default target>` is your current target.

Each time a CLI command runs, the output follows this general format:

```
</> hpiLO-> {CLPcommand}
status=0
status_tag=COMMAND COMPLETED
... command output returned...
</>hpiLO->
```

If you enter an invalid command, the `status` and `status_tag` values reflect the error as shown:

```
</> hpiLO-> badcommand
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND NOT RECOGNIZED

</>hpiLO->
```

If an invalid target is specified, the response differs as follows:

```
</> hpiLO-> show /badtarget1
status=3
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND SYNTAX ERROR
'/badtarget1' is an invalid target.

</>hpiLO->
```

SM CLP Syntax

The following sections provide terms, descriptions, and examples of the SM CLP syntax.

Command Line Terms

The command syntax consists of a command verb, options, target address, and properties. The general syntax of the SM CLP command is as follows:

<verb> <options> <target> <properties>

Where:

<verb> The command verb.

<options> Selections that affect the action, behavior, or output of the verb.

<target> The implicitly or explicitly-identified managed element the command is directed to.

<properties> Attributes of the target relative to the command execution.

Command Verbs

Command verbs select a management action for target.

The command verbs listed in Table 54 consist of several reserved words in the following categories:

Retrieve Information	cd, help, show, version
Configure a target	create, delete, load, set
Change target state	exit, reset, start, stop

Table 54 lists the supported command verbs.

Table 54 Supported Command Verbs

Command	Action
cd	Changes the current default target. The root of the CLP target namespace is `/`, and this is the starting point for a CLP system. By changing the current default target by running `cd <some target>`, you can shorten commands. For example, to find the current MP firmware version, run the command `show /map1/swinventory1/swid1`. However, if you run the `cd /map1/swinventory1/swid1` command, the `show` command displays the information.
create	Creates a new instance of an object.
delete	Deletes an instance of a target object.
exit	Terminates the SM CLP session.
help	Displays context-sensitive help.

Table 54 Supported Command Verbs *(continued)*

Command	Action
	`help` displays general help and all supported commands. `help <some verb>` displays help for the specified verb. `help <some target>`displays help for the specified target. `help <some property>` displays help for the specified property.
load	Moves a binary image to iLO 2 from a URI.
reset	Causes a target to cycle from enabled to disabled and back to enabled.
set	Sets a property to a specific value.
show	Displays information about managed elements (targets, their supported properties and verbs). You can also run the `show` command with an explicit or implicit target. For more information on implicit and explicit targets, see "System1 Target" (page 148), "Map1 (iLO 2) Target" (page 149), "Command Targets" (page 145) .
start	Causes a targeted object to change its state to a higher level.
stop	Causes a targeted object to change its state to a lower level.
version	Queries the version of the SM CLP implementation.

The following verbs are available for execution from any target:

- show
- help
- cd
- version
- exit

Command Targets

The command target address identifies the specific managed element or association to be affected by the command verb. All SM CLP commands have a command target, whether explicitly or implicitly identified.

For instance, the target `/map1/telnetsvc1/` can be identified in any of the following ways:

Using the target's absolute path:

```
</> hpiLO-> show /map1/telnetsvc1
```

Using the target's relative path form `map1` target:

```
</map1> hpiLO-> show telnetsvc1
```

Using implicit (current) target's with the verb **show**

```
</map1/telnetsvc1> hpiLO-> show:
```

Command Target Properties

Target properties are identifying and descriptive information related to and defined by the target. Target properties are identified by property names. Each class of target defines a set of valid property names. Property values are expressed in `name=value` format.

You can specify one or more properties on the command line. If you specify multiple properties on the same command line, they must be separated by a space.

Command Options

Command options control verb behavior.

Command options can appear immediately after the verb and must be prefaced with a dash (-).

Most command options have both a full name and a short form; for example:

`show –level all` or `show –l all`

Level Option

The level option instructs the command verb to include n number of levels in the scope of its execution. A level typically refers to the depth of containment to be processed by the verb.

Forms:

```
-level <n>
```

```
-l <n>
```

Where n is the number of levels to include in command scope.

The value of n is interpreted as follows:

n=1 Verb is interpreted for the command target only (default).

n=2 Verb acts on the command target and any directly contained Managed Elements (MEs).

n=3 Verb acts on the command target, directly contained MEs, and any MEs contained by those MEs (such as – current target and two down).

n=all Verb acts on the command target and all target MEs recursively contained in the command.

The following examples show command display option syntax:

Show information about default target and one level of contained MEs:

```
</>hpiLO-> show -l 2
```

Show all contained MEs:

```
</>hpiLO-> show -l all
```

Show information about `system1` and all contained MEs:

```
</>hpiLO-> show -l all system1
```

Display Option

The display option filters the information returned in command results.

The following examples show command display option syntax:

Display targets under `/map1` target:

```
</map1> hpiLO-> show -d targets
```

Display properties of `/map1` target:

```
</map1> hpiLO-> show -d properties
```

Display verbs of `/map1` target:

```
</map1> hpiLO-> show -d verbs
```

Display the name property of `/map1` target:

```
</>hpiLO-> show -d properties=name /map1
```

Find a target that has a property name with value of `MP Menu`:

```
</>hpiLO-> show -l all -d properties=(name==”MP Menu”)
```

Find a target that has a property name with value of `MP Menu` and display all verbs supported for that target:

`</>hpiLO-> show -l all -d properties=(name==”MP Menu”)`, verbs

Find and display all targets that have the `EnabledState` property:

```
</map1> hpiLO-> show -l all -d properties=”enabled state”
```

Find and display all `Account` targets in the system and their information:

```
</> hpiLO-> show -l all account*
```

Table 55 shows the available command options.

Table 55 Command Options

Option	Short Form	Description
-display <name>	-d	Selects the data you want to display.
-force	-f	Instructs the verb to ignore warning conditions that otherwise prevent execution.
-help	-h	Provides command-specific help.
-level <n>	-l	Instructs manageability access point (MAP) to execute the command for the specified target and for targets contained through the specified level of depth.
-source <URI>	None	Indicates the location (URI) of the source image or target.
-version	-v	Displays the version of the command.

Character Set, Delimiters, Special, and Reserved Characters

All implementations of the SM CLP must interpret the characters provided by the transport as UTF8 representation of the characters, including those in Table 56. They must interpret the characters according to the descriptions in Table 56.

Table 56 lists the SM CLP reserved characters.

Table 56 SM CLP Reserved Characters and Character Sequences

Character or Sequence	Name	Description and Uses
“ “	Space	Command line term separator.
‘	Escape character	Escape character (the backquote character). Use in front of reserved characters to instruct the command parser to use the reserved character without special meaning. When the escape character is not followed by a reserved character, it is treated as a normal character in the string that contains it.
<cr> <lf> <cr><lf>	End of line	Each of these sequences are accepted as an end-of-line indicator.
<escape character><end-of-line>	Line continuation	An escape character placed immediately before the end-of-line sequence indicates that the current line is continued to the following line. The following line is appended to the current line.
,	Comma	Delimits items in an option argument term to be interpreted as a list of option arguments. Also delimits values for an option argument.
=	Assignment operator	Separates a property name from a desired value for the property when used with verbs that modify or create an instance. It can not have a space before or after it in an expression of a property and its value.
==	Equivalence operator	Two consecutive equals signs without white space between them are used to separate a property name from a number value when filtering instances for which results must be returned.
-	Hyphen	When preceded by a space, the hyphen is the SM CLP option indicator.

Table 56 SM CLP Reserved Characters and Character Sequences *(continued)*

Character or Sequence	Name	Description and Uses
/ □	Address term separator	Separates the UFiT terms of a target address.
.	Dot	Recognized as a special target address token meaning *this container*.
..	Dot-dot	Recognized as a special target address token meaning *the container of this container*.
()	Parentheses	In a comma-separated option argument term list, delineates the values of an argument from the next option argument.
"	Double quote	Delineates a string of text that can contain the SM CLP term separator (space) so that the SM CLP command processor treats the delineated text as one string.
"->"	SM CLP PROMPT (hyphen, greater-than, space)	Literal representation of the SM CLP prompt.

System1 Target

Target: SYSTEM1

`/system1`

The `system1` target represents the root of the system namespace. Functions and information such as OS console, system power status and control, system LED status, and so on, related to the system are located under this target.

Table 57 shows `system1` target properties.

Table 57 system1 Properties

Property Name	Description	Access and Values
EnabledState	Provides information about the system power state.	Read-only Values: • Enabled: System power is off. • Disabled: System power is on.

Verbs

show Displays information about managed elements (targets, their supported properties and verbs).

help Displays context-sensitive help.

reset Resets the system.

start Turns system power on.

stop Performs graceful shutdown of the system. If used with force option, turns system power off.

System Reset Power Status and Power Control

This section describes the system reset power status and power control commands.

Resetting the System

To reset the system, apply the `reset` command to the `system1` target. For example:

```
</>hpiLO-> reset system1
status=0
```

```
status_tag=COMMAND COMPLETED
system1 has been issued a reset
```

Displaying Power Status

To display the power state of the system, query the value of the `enabledstate` property of the `system1` target. For example:

```
</>hpiLO-> show -d properties=enabledstate system1
status=0
status_tag=COMMAND COMPLETED
/system1
      Properties
      EnabledState=Enabled
```

Powering Off the System

To power off the system, apply the `stop` (graceful shutdown) or `stop-force` (power off) commands to the `system1` target. For example:

```
</system1> hpiLO-> stop -f
status=0
status_tag=COMMAND COMPLETED
System is being powered off.


</system1> hpiLO-> stop
status=0
status_tag=COMMAND COMPLETED
system has been requested graceful shutdown.
```

Powering On the System

To power on the system, apply the `start` command to the `system1` target. For example:

```
</>hpiLO-> start system1
status=0
status_tag=COMMAND COMPLETED
system1 has been powered on
```

Map1 (iLO 2) Target

Target: map1

The `map1` target (management access point) represents the root of the iLO 2 namespace. Functions and information related to iLO 2 are located under the `map1` target.

Table 58 shows `map1` target properties.

Table 58 map1 Properties

Property Name	Description	Access and Values
Dedicated	Indicates whether the computer system is a special purpose system (for example, dedicated to a particular use), or a general-purpose system.	Read-only Set to *management*.
Name	Name that identifies iLO 2.	Read-only Set to *iLO 2 Advanced, HP Integrity*.

Verbs

show	Displays information.
help	Displays context-sensitive help.
reset	Resets iLO 2.

Map1 Example

The following example displays information about map1:

```
</> hpiLO-> show map1
status=0
status_tag=COMMAND COMPLETED

/map1
   Targets
     dhcpendpt1
     dnsendpt1
     dnsserver1
     dnsserver2
     dnsserver3
     enetport1
     gateway1
     group1
     settings1
     sshsvc1
     swinstallsvc1
     swinventory1
     telnetsvc1
     textredirectsap1
     textredirectsvc1
   Properties
     Name=iLO Advanced, HP Integrity
     Dedicated=Management
   Verbs
     cd help show load reset
</> hpiLO->
```

Resetting iLO 2

To reset iLO 2, run the `reset` command to the `MAP1` target as in the following example:

```
</>hpiLO-> reset map1
status=0
status_tab=COMMAND COMPLETED
iLO was issued a reset
```

Text Console Services

This section describes targets, their properties, and supported verbs necessary to implement the console services in SM CLP.

You can invoke the system console and the MP Main Menu from SM CLP.

Any text console service is represented by a dedicated to it `textredirectsap` target.

Target `/map1/textredirectsvc1` represents iLO 2's ability to provide text console redirection service.

Opening the MP Main Menu from SM CLP

This section provides information on how to invoke the MP Main Menu from the SM CLP.

Target: map1/textredirectsap1

The textredirectsap1 target represents the MP Main Menu interface.

Table 59 shows `textredirectsap1` target properties.

Table 59 /map1/textredirectsap1 Properties

Property Name	Description	Access and Values
EnabledState	Shows whether the text redirection is enabled.	Read-only The value is set to `Enabled`.
SessionTerminateSequence	A string sequence used for terminating text redirection session and returning to SM CLP.	Read-only The value is set to `SMCLP`. Enter **`SMCLP`** at the MP Main Menu to return to the SM CLP interface.
Description	Description of this text redirection service access point.	Read-only The value is set to `MP Main Menu Interface`.
Name	Uniquely identifies this access point.	Read-only The value is set to `MP Main Menu`

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
start	Switch to MP Main Menu.

Opening the System Console Interface from SM CLP

This section provides information on how to open the system console from the SM CLP.

Target: system1/consoles1/textredirectsap1

This target represents the system text console (currently launched through the iLO 2 `CO` command). Table 60 shows `textredirectsap1` target properties.

Table 60 /system1/consoles1/textredirectsap1 Properties

Property Name	Description	Access and Values
EnabledState	Shows if the test redirection is enabled.	Read-only Set to `Enabled`.
SessionTerminateSequence	A string sequence used for terminating text redirection session and returning to SM CLP.	Read-only Set to `Esc`. Enter **Esc** at the system console to return to the SM CLP interface.
Description	Description of this text redirection service access point.	Read-only Set to `System Test Console Interface`.
Name	Uniquely identifies this access point.	Read-only Set to `System Test Console`.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
start	Switch to system text console.

Switching Between the System Console and the SM CLP

The following examples show commands used to switch between the system console and the SM CLP.

Starting a System Console Session

To start a system console session, enter the following command:

`</>hpiLO->start /system1/consoles1/textredirectsap1`

Determining the Session Termination Character Sequence for the System Console

To determine the session termination character sequence for the system console, enter the following command:

`</> hpiLO-> show -d properties=SessionTerminateSequence`

```
   /system1/consoles1/testredirectsap1
status 0
status_tag=COMMAND COMPLETED

/system1/consoles1/testredirectsap1
   Properties
      SessionTerminateSequence=Esc (
```

Exiting the System Console Session and Returning to SM CLP

To exit the system console session and return to SM CLP, enter **`Esc + (`** at the system text console.

Entering the MP Main Menu Interface From SM CLP

To enter the MP Main Menu from SM CLP, enter the following command: **`</>hpiLO->start /map1/textredirectsap1`**

Exiting the MP Main Menu Session and Returning to SM CLP

To exit the MP Main Menu interface and return to the SM CLP session, enter **`SMCLP`**

Firmware Revision Display and Upgrade

This section describes how to view firmware revisions in the system.

Each installed firmware in the system known to MP (MP FW, BMC FW, EFI FW, System FW, and so on) is represented by a `swid` target.

- `/map1/swinstallsvc1` represents iLO 2's ability to install firmware.
- `/map1/swinventory1` represents a collection of all `swids` installed in the system.

SM CLP Firmware Targets

This section describes targets, target properties, and supported verbs necessary to implement the firmware model in SM CLP.

Target: map1/swinstallsvc1

SoftwareInstallationService provides the ability to transfer images into a managed element from a source location, local or remote (such as the ability to upgrade firmware).

Table 61 shows `swinstallsvc1` target properties.

Table 61 swinstallsvc1 Properties

Property Name	Description	Access and Values
Description	Provides a textual description of the object.	Read-only The value is set to `firmware installation service`.

Verbs

cd   Changes the current default target.

help Displays context-sensitive help.
show Displays information.

Target: map1/swinventory1

SoftwareInventory is a dedicated collection for all firmware in the system known to iLO 2.

Table 62 shows `swinventory1` target properties.

Table 62 swinventory1 Properties

Property Name	Description	Access and Values
Description	Provides a textual description of the object.	Read-only The value is set to `firmware inventory`.

Verbs

cd Changes the current default target.
help Displays context-sensitive help.
show Displays information.

Target: map1/swinventory1/swid#

SoftwareIdentity represents software in the system known to iLO 2 (map1).

Table 63 shows `swid#` target properties.

Table 63 swid# Properties

Property Name	Description	Access and Values
TargetType	Identifies what type of firmware this `swid` target represents	Read-only
VersionString	Represents firmware revision string; for example, F.01.40.	Read-only

Verbs

cd Changes the current default target.
help Displays context-sensitive help.
show Displays information.
load Moves an image to iLO 2.

The following is a possible list of `swid` in the system:

- /map1/swinventory1/swid1: represents iLO 2 firmware
- /map1/swinventory1/swid2: represents BMC firmware
- /map1/swinventory1/swid3: represents EFI firmware
- /map1/swinventory1/swid4: represents System Firmware
- /map1/swinventory1/swid5: represents PDH firmware
- /map1/swinventory1/swid6: represents UCIO firmware
- /map1/swinventory1/swid7: represents PRS firmware

Displaying Firmware Revisions

This example displays only the iLO 2 firmware revision:

```
</map1/swinventory1> hpiLO-> show -d properties= `
      (TargetType=="MP FW",versionstring)
status=0
status_tag=COMMAND COMPLETED

    /map1/swid1
```

```
      Properties
         VersionString=F.01.57
```

This example displays all the firmware revisions.

```
</>hpiLO-> show /map1/swinventory1/swid*

/map1/swinventory1/swid1
 TargetType=MP FW
 VersionString=F.01.57

/map1/swcollection1/swid2
 TargetType=BMC FW
 VersionString=01.60

 /map1/swcollection1/swid3
 TargetType=EFI FW
 VersionString=ROM A 05.11, ROM B 255.255

/map1/swcollection1/swid4
 TargetType=System FW
 VersionString=ROM A 62.03, ROM B 255.255, Boot ROM B

/map1/swcollection1/swid5
 TargetType=PDH FW
 VersionString=00.0b

/map1/swcollection1/swid6
 TargetType=UCIO FW
 VersionString=03.03

/map1/swcollection1/swid7
 TargetType=PRS FW
 VersionString=00.05 UpSeqRev: 09, DownSeqRev: 07
```

or

```
</>hpiLO-> show -level all swid*
```

Firmware Upgrade

Firmware upgrades enhance the functionality of iLO 2.

The MP firmware is packaged along with system, BMC, and FPGA/PSOC firmware. You can download and upgrade the firmware package from the HP website at http://www.hp.com/go/bizsupport.

IMPORTANT: When performing a firmware upgrade that contains system programmable hardware, you must properly shut down any OS that is running before starting the firmware upgrade process.

Select **Download drivers and software**, select your server, and follow the directions provided.

After the upgrade, reconnect and log in as user **`Admin`** and password **`Admin`** (case sensitive).

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task.

Remote Access Configuration

Integrity iLO 2 supports the use of Telnet and SSH to access the iLO 2 MP command line interface.

Telnet SM CLP Targets

This section describes targets, their properties, and supported verbs necessary to enable or disable Telnet access to iLO 2.

Target: map1/telnetsvc1

The `telnetsvc1` target represents the `telnetsvc` service provided by `map1`.

Table 64 shows `telnetsvc1` target properties.

Table 64 telnetsvc1 Properties

Property Name	Description	Access and Values
EnabledState	Shows whether Telnet is enabled or disabled.	Read-only The following are valid values: Enabled, Disabled
Protocol	The protocol this service provides.	Read-only Set to `telnet`

Verbs

start	Enables iLO 2 Telnet service.
show	Displays information.
stop	Disables iLO 2 Telnet service.
help	Displays context-sensitive help.

Telnet Examples

The following examples show specific Telnet commands.

Enable Telnet Service

```
</>-> start /map1/telnetsvc1
```

Disable Telnet Service

```
</>-> stop /map1/telnetsvc1
```

SSH

This section describes targets, their properties, and supported verbs necessary to enable or disable SSH access to iLO 2.

Target: map1/sshsvc1

The `sshsvc1` target represents the SSH service provided by `map1`.

Table 65 shows `sshsvc1` target properties.

Table 65 sshsvc1 Properties

Property Name	Description	Access and Values
EnabledState	Shows whether SSH service is enabled or disabled.	Read-only The following are valid values: Enabled, Disabled
Protocol	The protocol this service provides.	Read-only Set to SSH.

Verbs

start	Enables iLO 2 SSH service.
stop	Disables iLO 2 SSH service.

show	Displays information.
help	Displays context-sensitive help.

SSH Examples

The following examples show specific SSH commands.

Enable SSH Service

```
</>-> start /map1/sshsvc1
```

Disable SSH Service

```
</>-> stop /map1/sshsvc1
```

Network Configuration

Network commands enable you to display or modify network settings.

SM CLP Network Targets, Properties, and Verbs

This section describes targets, target properties, and supported verbs necessary to implement the iLO 2 network configuration through SM CLP.

Target: map1/enetport1

The `enetport1` target represents capabilities and management of the iLO 2 MP Ethernet port.

Table 66 shows `enetport1` target information.

Table 66 enetport1 Properties

Property Name	Description	Access and Values
AutoSense	Specified if the iLO 2 AutoSense feature is enabled. If it is disabled, iLO 2 network speed is set to 10 mb/s.	Read/write Boolean values accepted.
PermanentAddress	Represents iLO 2 MP MAC address.	Read-only The iLO 2 MP MAC address is formatted as twelve hexadecimal digits (10203040506) with each pair representing one of the six octets of the MAC address.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
set	Sets a property to a specific value.

Target: map1/enetport1/lanendpt1

The `lanendpt1` target represents the iLO 2 LAN endpoint settings.

Table 67 shows `lanendpt1` target properties.

Table 67 lanedpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the iLO 2 MP LAN state.	Read-only The following are valid values:

Table 67 lanedpt1 Properties *(continued)*

Property Name	Description	Access and Values
		Enabled, Disabled
MACAddress	Represents the iLO 2 MP MAC address.	Read-only The MAC address is formatted as twelve hexadecimal digits (010203040506), with each pair representing one of the six octets of the MAC address.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.

Target: map1/enetport1/lanendpt1/ipendpt1

The `ipendpt1` target represents the iLO 2 MP IP endpoint settings.

Table 68 shows `ipendpt1` target properties.

Table 68 ipendpt1 Properties

Property Name	Description	Access and Values
IPv4Address	iLO 2 MP IP address.	Read/write The value of the property must be expressed in dotted decimal notation.
SubnetMask	iLO 2 MP subnet mask.	Read/write The value of the property must be expressed in dotted decimal notation.
AddressOrigin	Indicates the configuration method that resulted in the configuration being assigned to this `ipendpt`.	Read-only The following are valid values: Static: The iLO 2 MP IP address and subnet mask were assigned statically. DHCP: The iLO 2 MP IP address and subnet mask were acquired using DHCP.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
set	Sets a property to a specific value.

Target: map1/dhcpendpt1

The `dhcpendpt1` target represents the iLO 2 DHCP client.

Table 69 shows `dhcpendpt1` target properties.

Table 69 dhcpendpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the state of iLO 2 DHCP.	Read-only The following are valid values: Enabled: The iLO 2 DHCP client is enabled.

Table 69 dhcpendpt1 Properties *(continued)*

Property Name	Description	Access and Values
		Disabled: The iLO 2 DHCP client is disabled.
OtherTypeDescription	Textual description of this protocol endpoint.	Read-only Set to DHCP.

Verbs

cd Changes the current default target.

help Displays context-sensitive help.

show Displays information.

start Enables iLO 2 DHCP.

stop Disables iLO 2 DHCP.

Target: map1/dnsendpt1

The `dnsendpt1` target represents the iLO 2 DNS client.

Table 70 shows `dnsendpt1` target properties.

Table 70 dnsendpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the state of iLO 2 DNS.	Read only The following are valid values: Enabled: The iLO 2 DNS client is enabled. Disabled: The iLO 2 DNS client is disabled.
Hostname	Represents the host name currently assigned to iLO 2.	Read-only iLO 2 current host name.
OtherTypeDescription	Textual description of this protocol endpoint.	Read-only Set to DNS.

Verbs

cd Changes the current default target.

help Displays context-sensitive help.

show Displays information.

Target: map1/enetport1/lanendpt1/ipendpt1/gateway1

The `gateway1` target represents the gateway server.

Table 71 shows `gateway1` target properties.

Table 71 gateway1 Properties

Property Name	Description	Access and Values
AccessInfo	Represents the IP address of the gateway server.	Read/write The value of the property must be expressed in dotted decimal notation.
AccessContext	Represents access context (description) of this access point.	Read-only Set to `default gateway`.

Target: map1/dnsserver1, map1/dnsserver2, map1/dnsserver3

The `dnsserver1`, `dnsserver2`, and `dnsserver3` targets represent the iLO 2 primary, secondary, and tertiary DNS servers respectively.

Table 72 shows `dnsserver1`, `dnsserver2`, and `dnsserver3` target properties

Table 72 dnsserver1, dnsserver2, dnsserver3 Properties

Property Name	Description	Access and Values
AccessInfo	Represents the IP address of the DNS server.	Read/write The value of the property must be expressed in dotted decimal notation.
AccessContext	Represents access context (description) of this access point.	Read-only Set to `DNS server`.

Verbs

show Displays information.

help Displays context-sensitive help.

set Sets a property to a specific value.

Target: map1/settings1/dnssettings1

The `dnssettings1` target contains iLO 2 DNS settings.

Table 73 shows `dnssettings1` target properties.

Table 73 dnssettings1 Properties

Property Name	Description	Access and Values
DNSServerAddress	Contains the IP addresses of the primary, secondary, and tertiary DNS servers.	Read/write This is an array property. The value of each element of this property must be expressed in dotted decimal notation. The elements of the property are separated by commas (DNSServerAddressess=192.0.2.1, 192.0.2.2, 192.0.2.3 means that the IP addresses of the primary, secondary and tertiary DNS servers are set to 192.0.2.1, 192.0.2.2, 192.0.2.3 respectively).
DomainName	iLO 2 domain name.	Read/write
RegisterThisConnections Address	Indicates whether iLO 2 registers with the DDNS server.	Read/write. The following are valid values: Yes: register with DDNS server. No: do not register with DDNS server.
RequestedHostName	iLO 2 host name.	Read/write.

Verbs

cd Changes the current default target.

help Displays context-sensitive help.

show Displays information.

set Sets a property to a specific value.

SM CLP Network Command Examples

The following examples list specific network commands.

Determine the iLO 2 MP MAC Address

```
</>hpiLO-> show -d properties=macaddress /map1/enetport1/lanendpt1
```

or

```
</>hpiLO-> show -d properties=permanentaddress /map1/enetport1/
```

Determine current IP Address

```
</>hpiLO-> show -d properties=ipv4address /map1/enetport1/lanendpt1/ipendpt1
```

Determine Subnet Mask

```
</>hpiLO-> show -d properties=subnetmask /map1/enetport1/lanendpt1/ipendpt1
```

Set IP Address and Subnet Mask

To modify a Static IP Address and Subnet Mask, set IPv4Address and SubnetMask properties of the ipendpt1 target:

```
</>hpiLO-> set /map1/enetport1/lanendpt1/ipendpt1
ipv4address=192.0.2.1 subnetmask=255.255.255.0
```

Determine Gateway Address

```
</>hpiLO-> show -d properties=accessinfo
/map1/enetport1/lanendpt1/ipendpt1/gateway1
```

Set Gateway Address

```
</>hpiLO-> set /map1/enetport1/lanendpt1/ipendpt1/gateway1
AccessInfo=192.0.2.1
```

Determine Link State (Autosense)

```
</>hpiLO-> show -d properties=autosense /map1/enetport1
```

Set Link (Autosense)

```
</>hpiLO-> set /map1/enetport1 autosense=true
AccessInfo=192.0.2.1
```

Enable/Disable DHCP

```
</>hpiLO-> stop /map1/dhcpendpt1

</>hpiLO-> start /map1/dhcpendpt1
```

Determine all DNS settings

```
</>hpiLO-> show /map1/settings1/dnssettings1
```

Determine IP Address of the DNS Servers (primary, secondary, and tertiary)

```
</>hpiLO-> show -d properties=AccessInfo /map1/dnsserver*
```

or

```
</>hpiLO-> show -d properties=DNSServerAddresses
/map1/settings1/dnssettings1
```

Set Primary and Secondary DNS Server IPs

```
</map1/settings1/dnssettings1> set
DNSServerAddressess=192.0.2.1, 192.0.2.4
```

Set Tertiary DNS Server IP

```
</map1/settings1/dnssettings1> set DNSServerAddressess=,,192.0.2.6
```

vMedia

This section provides information on SM CLP vMedia targets, properties, and supported verbs. It also lists examples of SM CLP vMedia use cases.

The scriptable vMedia feature is supported on server blade platforms (OA version 2.0 and beyond) and on rackmounted servers as described in the following sections.

NOTE:

- Scriptable vMedia is available only if you have the iLO 2 Advanced Pack license and the vMedia user privilege.
- Only one vMedia connection is supported at a time. You cannot connect with the scriptable vMedia while the Applet vMedia is connected and vice versa.

Scriptable vMedia Supported Operating Systems

- Linux (Red Hat and SuSE)
- Windows
- HP-UX
- OpenVMS
- EFI

Setting Up IIS for Scripted vMedia

Before setting up Internet Information Services (IIS) for scripted vMedia, make sure IIS is operational. Use IIS Manager to set up a simple website and verify that it is working correctly by browsing to the site.

To configure IIS to serve diskette or ISO-9660 CD images for read only access:

1. Add a directory to your website, and place your images in the directory.
2. Verify that IIS can access the MIME type for the files you are serving. For example, if you name your diskette images with the extension .img, you must add a MIME type for that extension. Use the IIS Manager to access the Properties dialog of your website. On the HTTP Headers tab, click **`MIME Types`** to add additional MIME types.

   HP recommends you add the following types:

   .img – application/octet-stream

   .iso – application/octet-stream
3. Browse to the location of your images with a web browser, and download them to a client.

   Your web server is configured properly for serving read-only diskette and CD images.

To configure IIS to serve diskette images for read/write operations:

1. Install Perl (if necessary). Active State's ActivePerl is an installer program that also sets itself up to be a script interpreter for IIS. You can obtain it from the web at: `http://www.activestate.com/`
2. Create a directory on your web site to hold the vMedia helper script, and copy the script to that location.
3. To create an application directory, use the properties page for your directory. Under Application Settings, click **`Create`**.

   The icon for your directory in IIS Manager should change from a folder to a gear.
4. Set Execute Permissions to **`Scripts Only`**.
5. Verify that Perl is set up as a script interpreter. To view the application associations, click **`Configuration`** on the properties page. Verify that Perl is configured as follows:

   ```
   .pl c:\perl\bin\perl.exe "%s" %s GET,HEAD,POST
   ```
6. Verify your Web Service Extensions allows Perl scripts to execute. If not, click **`Web Service Extensions`**, and set Perl CGI Extension to **`Allowed`**.
7. Verify the prefix variable in the helper script is set correctly. You can set it to the same path as your document root, which can be similar to C:\inetpub\wwwroot.

vMedia Functionality on Server Blades and Rack-Mounted Servers

Administrators can easily transfer data to the managed system from the web (Apache or IIS) server containing the vMedia ISO images. On the client side, the web (Apache or IIS) server is running and the ISO images are stored so they can be accessed over HTTP.

NOTE: HTTPS is currently not supported through the SM CLP interface.

The drives (connected ISO images) on the client side appear as local drives (USB CD Read-only) on the managed server. With the help of vMedia, the server can boot from the DVD, CD, or image on the client, perform OS and applications installation on the server from the client's drives or data transfer, and so on.

To access the SM CLP interface, enter `SMCLP` at the MP Main menu after you login.

Target: map1/oemhp_vm1/cddr1

The `cddr1` target represents the virtual CD-ROM device.

Table 74 cddr1 Properties

Property Name	Description	Access and Values
oemhp_image	The image path and name for vMedia access.	Read/write The value is a URL with a maximum length of 80 characters.
oemhp_connect	Used to connect or disconnect a vMedia device and display the connection status.	Read/write The following are valid values: • Yes: Connect. • No: Disconnect.
oemhp_applet_connected	Indicates if the Java applet is connected.	Read-only Set to: • Yes • No

Verbs

set	Sets a property to a specific value.
show	Displays information.
help	Displays context-sensitive help.

Using Scriptable vMedia on Server Blades and Rack-Mounted Servers

The following examples show actions you can perform using SM CLP for vMedia on server blades and on rack-mounted servers.

Change the current context to point to the SMCLP target representing the virtual the CD drive

```
–> cd / map1 / oemhp_vm1 / cddr1
```

Display `/ map1 / oemhp_vm1 / cddr1` target properties and show the current status to verify that the media is not in use

```
–> show
```

Insert the desired image into the drive

```
–> set oemhp_image=http://<Apache server ip address>/cgi-bin/ISO/install_disk1.iso
```

Connect to the media

```
–> set / oemhp_connect=yes
```

NOTE: The `oemhp_applet_connected` has a value equal to `yes`.

If you attempt to connect when there is no valid image location set in the `oemhp_image` property, you will receive an error.

Disconnect vMedia

This command disconnects the media and clears the `oemhp_image` value.

–> set / map1 / oemhp_vm1 / cddr1 oemhp_connect=no

NOTE: If you attempt to disconnect when the drive is not connected, you will receive an error.

Using Scriptable vMedia on Server Blades Only

This section provides information on using scriptable vMedia on server blades only.

On HP Integrity server blades, all iLO 2 functions are available on the Onboard Administrator (OA).

The OA presents its bootable physical CD/DVD media as an ISO image. DVD/CD connect and disconnect sequences are initiated from the OA by the OA user. The drives (connected ISO images) on the client side appear as local drives (USB CD read-only) on the managed server. With the help of vMedia, the server can boot from the DVD/CD (or image) on the client, perform OS and applications installation on the server from the client's drives or data transfer, and so on.

The OA has two types of CD/DVD interfaces to access scriptable vMedia:

Built-in DVD Interface

The c3000 Enclosure has a built-in DVD drive you can use to connect using scriptable vMedia.

External CD/DVD Drive Interface

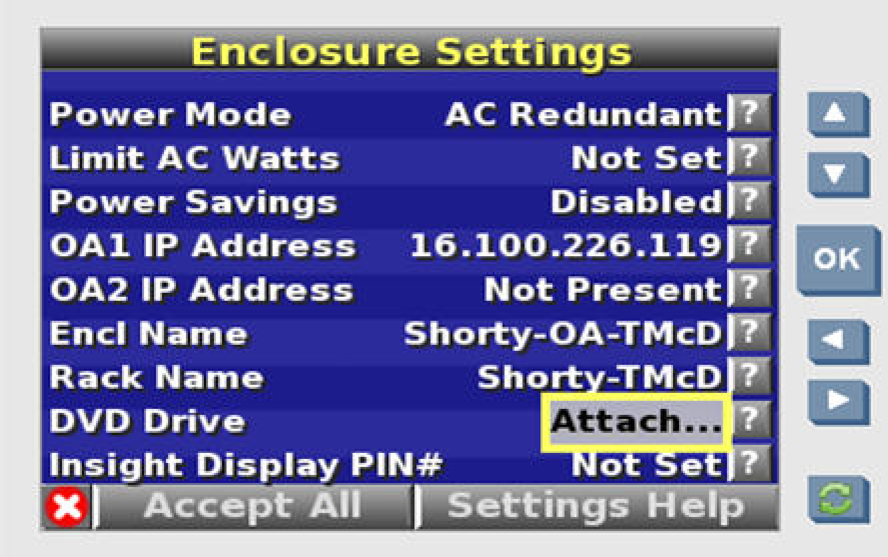
On a c7000 Enclosure, an external CD/DVD drive is connected to the additional USB port on the enclosure itself. This is used to connect using scriptable vMedia.

To connect using scriptable vMedia on server blades:

- On a c3000 enclosure, insert a DVD in the built-in DVD drive.
- On a c7000 enclosure, insert a CD/DVD in the external CD/DVD drive that is connected to the USB port.

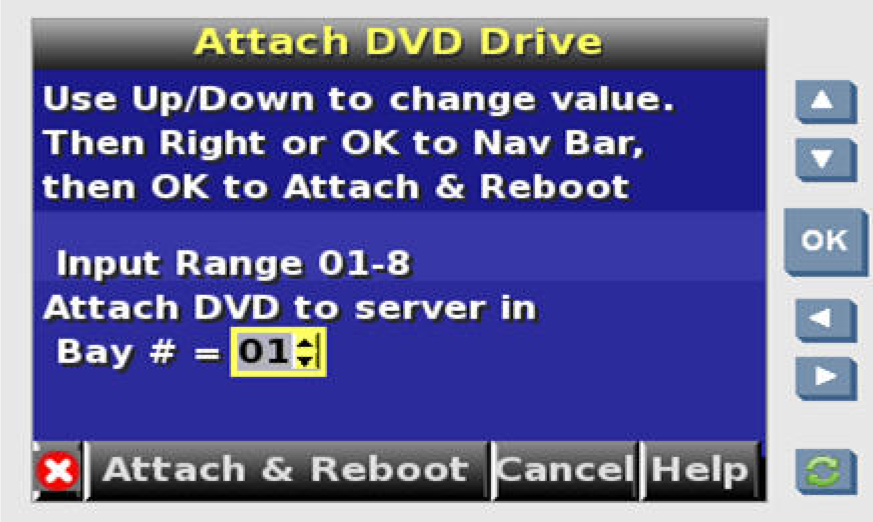
There are three methods to connect:

1. Using the LCD display on the OA enclosure, navigate to the `DVD Drive - Attach...` option.



Enclosure Settings

Power Mode AC Redundant
Limit AC Watts Not Set
Power Savings Disabled
OA1 IP Address 16.100.226.119
OA2 IP Address Not Present
Encl Name Shorty-OA-TMcD
Rack Name Shorty-TMcD
DVD Drive Attach...
Insight Display PIN# Not Set



Attach DVD Drive

Use Up/Down to change value.
Then Right or OK to Nav Bar,
then OK to Attach & Reboot

Input Range 01-8
Attach DVD to server in
Bay # = 01

2. Using the Telnet/SSH connection to the OA.

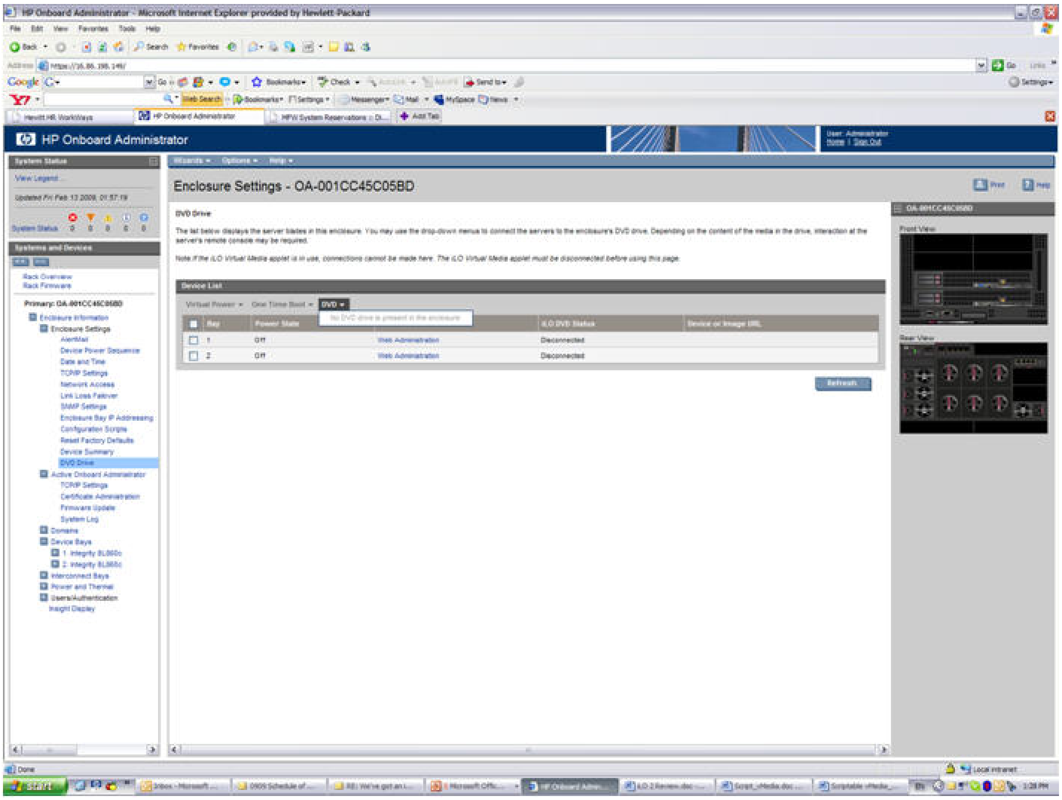
NOTE: While in the OA, you will not be entering the SM CLP vMedia commands directly in MP. Instead, you will issue the commands from the Telnet/SSH connection of the OA to connect or disconnect vMedia.

- Enter the following commands to either connect or disconnect vMedia:

  set server dvd connect <slot #> (or all to connect for all blades)

  set server dvd disconnect <slot #> (or all to disconnect for all blades)

3. Using the OA GUI, navigate to Enclosure Information/Enclosure Settings/DVD Drive.



Enclosure Settings - OA-001CC45C05BD

DVD Drive

The list below displays the server blades in this enclosure. You may use the drop-down menus to connect the servers to the enclosure's DVD drive. Depending on the content of the media in the drive, interaction at the server's remote console may be required.

Note: If the iLO Virtual Media applet is in use, connections cannot be made here. The iLO Virtual Media applet must be disconnected before using this page.

Device List

Virtual Power ▾ One Time Boot ▾ DVD ▾

No DVD drive is present in the enclosure

□	Bay	Power State		iLO DVD Status	Device or Image URL
□	1	Off	Web Administration	Disconnected	
□	2	Off	Web Administration	Disconnected	

The OA web GUI interface provides an easy-to-navigate graphical interface. Select a specific action for vMedia, such as inserting a disk, connecting, and so on.

Known Issues

- Only DVD/CD is supported at this time.
- Floppy/USB Key is currently not supported.
- Only one device is supported at a time with scriptable vMedia (either DVD/CD or Floppy/Key).
- Scriptable vMedia cannot connect while another vMedia Applet is connected and vice versa.
- Apache server cannot support large ISO images (greater than 2 GB).
- Scriptable vMedia does not currently have fully supported DNS. As a result, it does not support using the hostname in the CLI. Instead you must specify the IP address of the Apache server while specifying the image path in the command line.
- The vMedia feature is supported using the USB 1.1 protocol (since MP FW uses Philips 1181 USB device). As a result, USB 2.0 is not currently supported.
- DVD appears as the large CD.
- Currently there is no support on fully compliant DVD.

Typical Scriptable vMedia Usage

Using the scriptable vMedia feature, you can perform the following:

Deploying Operating Systems

- Installing (RHEL and SLES) Linux using ISO images
- Installing (RHEL and SLES) Linux using a set of physical CDs
- Installing Windows Server 2003 using Re-install Media using CD
- Installing Windows Server 2003 using Re-install Media using ISO image

- Installing Windows Server 2003 using Smart-setup and RTM-bit physical CDs
- Installing Windows Server 2003 using Smart-setup and RTM-bit ISO images
- Installing HP-UX using a physical CD
- Installing HP-UX using ISO images

Installing an Application

Installing MS SQL Server from an MSDN DVD

User Accounts Configuration

This section describes targets, their properties, and supported verbs used for configuring and viewing iLO 2 user accounts using SM CLP.

Target: map1/group1

The `group1` target represents a collection of user accounts on iLO 2.

Table 75 shows `group1` target information.

Table 75 group1 Properties

Property Name	Description	Access and Values
Description	Textual description of this collection target.	Read-only Set to `collection of user accounts`.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.

Target: map1/group1/account#

The `account#` target represents a user account on this iLO 2 where # is the instance number of the specific account. You can configure up to 19 user accounts on the iLO 2.

Table 76 shows `account#` target properties.

Table 76 account# Properties

Property Name	Description	Access and Values
UserID	Login name of this user account.	Read/write. Specified in ASCII characters up to 24 characters long.
UserPassword	User password.	Read/write. Specified in ASCII characters and must be least six characters long.
Name	User name of this account.	Read/write. Specified in ASCII characters up to 24 characters long.
oemhp_privileges	Privileges of this user account.	Read/write. The following are valid values: <console,power,mp,user,virtual), <all> or <none>.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
set	Sets a property to a specific value.

create Create a new user account.

delete Delete a user account.

User Account Examples

The following examples show specific user account commands.

Display all user accounts on this iLO 2

```
</> hpiLO-> show /map1/group1/account*
```

Create a new account

```
</map1/group1> hpiLO-> create account3 userid=testuser userpassword=testpass
name=”Test User” oemhp_privileges=console,power
```

Delete an account

```
</map1/group1> hpiLO-> delete account1
```

Modify account properties

```
</map1/group1/accuont3> hpiLO-> set oemhp_privileges=console name=”Console User”
```

LDAP Configuration

This section describes targets, their properties, and supported verbs used for configuring and viewing iLO 2 LDAP settings using SM CLP.

NOTE: You can only configure LDAP with extended HP schema from the SM CLP interface.

You can configure LDAP with default schema using the iLO 2 web GUI or the iLO 2 MP TUI Command menu.

Target: map1/settings1/oemhp_ldapsettings1

The **oemhp_ldapsettings1** target represents iLO 2 LDAP directory configuration settings.

Table 77 shows **oemhp_ldapsettings1** target information.

Table 77 oemhp_ldapsettings1 Properties

Property Name	Description	Access and Values
oemhp_dirauth	Represents the iLO 2 directory access setting.	Read write. Valid values are: DefaultSchema: enable directory authentication using default schema. ExtendedSchema: enable directory authentication using extended HP schema. Disabled: disable directory authentication
oemhp_localacct	Represents iLO 2 local user accounts access setting.	Read write. Valid values are: Enable: enable local iLO 2 user accounts. Disabled: disable local iLO 2 user accounts.
oemhp_dirsrvaddr	IP address or hostname of the directory server.	Read write.
oemhp_ldapport	Directory server LDAP port number.	Read write. Valid values are: 636, 2000-2400.
oemhp_dirdn	iLO 2 object distinguished name.	Read write.
oemhp_usercntxt1	Directory user search context #1.	Read write.
oemhp_usercntx2	Directory user search context #2.	Read write.
oemhp_usercntxt3	Directory user search context #3.	Read write.

Verbs

cd	Changes the current default target.
help	Displays context-sensitive help.
show	Displays information.
set	Sets a property to a specific value.

LDAP Configuration Examples

Configure LDAP parameters.

This command:

```
</map1/settings1/oemhp_ldapsettings1> hpiLO-> set oemhp_dirauth=
ExtendedSchema `oemhp_dirsrvaddr=192.0.2.1
oemhp_dirdn=cn=iLO2,ou=ManagementDevices,o=hp
oemhp_usercntxt1=cn=user,ou= engineering,o=hp
```

Applies the following LDAP settings:

- Enable LDAP authentication with extended schema.
- Set LDAP IP address.
- Set iLO 2 DN name as it is configured in the directory server. In this example it is set to `cn=iLO2,ou=ManagementDevices,o=hp`.
- Set user search context #1. In this example it is set to `cn=user,ou= engineering,o=hp`.

9 Installing and Configuring Directory Services

This chapter provides information on how to install and configure iLO 2 directory services.

You can install and configure iLO 2 directory services to leverage the benefits of a single point of administration for iLO 2 user accounts.

Directory Services

The following are benefits of directory integration:

Scalability
Leverage the directory to support thousands of users on thousands of iLO 2s.

Security
Robust user password policies are inherited from the directory. User password complexity, rotation frequency, and expiration are policy examples.

Role-based administration
You can create roles (for instance, clerical, remote control of the host, complete control), and associate users or user groups with those roles. When you change a single role, the change applies to all users and the iLO 2 devices associated with that role.

Single point of administration
You can use native administrative tools, like Microsoft Management Console (MMC) and ConsoleOne, to administer the iLO 2 users.

Immediacy
A single change in the directory rolls out immediately to associated iLO 2s, eliminating the need to script this process.

Reuse of user name and password
You can use existing user accounts and passwords in the directory without having to record or remember a new set of credentials for iLO 2.

Flexibility
You can create a single role for a single user on a single iLO 2; you can create a single role for multiple users on multiple iLO 2s; or you can use a combination of roles to best fit your enterprise.

Compatibility
The iLO 2 directory integration applies to the iLO 2 products and supports the popular directories Active Directory and eDirectory.

Standards
The iLO 2 directory support builds on the LDAP 2.0 standard for secure directory access.

Features Supported by Directory Integration

The iLO 2 directory services functionality enables you to do the following:

- Authenticate users from a shared, consolidated, scalable user database.
- Control user privileges (authorization) using the directory service.
- Use roles in the directory service for group-level administration of iLO 2 and iLO 2 users.

To install directory services for the iLO 2, a schema administrator must extend the directory schema.

The local user database is retained. You can choose not to use directories, to use a combination of directories and local accounts, or to use directories exclusively for authentication.

Directory Services Installation Prerequisites

Before installing directory services, you must do the following:

- Obtain an iLO 2 Advanced Pack license.
- Configure LDAP.

TIP: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task. To make sure you have the latest supported firmware version, see the HP website at http://www.hp.com/go/bizsupport.

Installing Directory Services

To successfully enable directory-enabled management on any iLO 2, complete the following steps:

1. Plan

   Review the following sections:

   - "Directory Services" (page 169)
   - "Directory Services Schema (LDAP)" (page 201)
   - "Directory-Enabled Remote Management" (page 196)

2. Install
   a. Download the HP Lights-Out Directory Package containing the schema installer, the management snap-in installer, and the migrations utilities from the HP website (http://www.hp.com/servers/lights-out).
   b. Run the schema installer once to extend the schema. See"Schema Installer" (page 172).
   c. Run the management snap-in installer and install the appropriate snap-in for your directory service on one or more management workstations. See"Management Snap-In Installer" (page 174).

3. Update
   a. With the directory-enabled firmware, flash the ROM on iLO 2.
   b. From the Directory Settings in the iLO 2 user interface, set directory server settings and the distinguished name of the iLO 2 objects.

4. Manage
   a. Create a management device object and a role object using the snap-in. See"Directory Services Objects" (page 179).
   b. Assign rights to the role object, as necessary, and associate the role with the management device object.
   c. Add users to the role object.

   For more information about managing directory service, see "Directory-Enabled Remote Management" (page 196). Examples are available in: "Directory Services for Active Directory" (page 174) and "Directory Services for eDirectory" (page 184).

Schema Documentation

To assist with the planning and approval process, HP documents the changes made to the schema during the schema setup process. To review the changes made to your existing schema, see "Directory Services Schema (LDAP)" (page 201).

Directory Services Support

Integrity iLO 2 supports the following directory services:

- Microsoft Active Directory
- Microsoft Windows Server 2003 Active Directory
- Novell eDirectory 8.6.2
- Novell eDirectory 8.7

The iLO 2 software is designed to run within the Microsoft Active Directory Users and Computers, and Novell ConsoleOne management tools. This enables you to manage user accounts on Microsoft Active Directory or Novell eDirectory. There is no distinction made between eDirectory running on NetWare, Linux, or Windows. To spawn an eDirectory schema extension, you must have Java 1.4.2 or later for SSL authentication.

Integrity iLO 2 supports Microsoft Active Directory running on one of the following operating systems:

- Windows 2000 family
- Windows Server 2003 family

NOTE: For instances when user authentication uses the LDAP directory server that is configured for Microsoft Active Directory, a user can log in using the username format `user@domain.hp.com`. Currently, this user credential format is only supported on Internet Explorer.

Integrity iLO 2 supports eDirectory 8.6.2 and 8.7 running on one of the following operating systems:

- Windows 2000 family
- Windows Server 2003 family
- NetWare 5.x
- NetWare 6.x
- Red Hat Enterprise Linux AS 2.1
- Red Hat Linux 7.3
- Red Hat Linux 8.0

eDirectory Installation Prerequisites

Directory services for iLO 2 uses LDAP over SSL to communicate with the directory servers. iLO 2 software is designed to install in eDirectory Version 8.6.1 (and later) tree. HP does not recommend installing this product if you have eDirectory servers with a version earlier than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, read and have available the following technical information documents (available at Novell Support at: http://support.novell.com)

- TID10066591 *Novell eDirectory 8.6 or greater NDS compatibility matrix*
- TID10057565 *Unknown objects in a mixed environment*
- TID10059954 *How to test whether LDAP is working properly*
- TID10023209 *How to configure LDAP for SSL (secure) connections*
- TID10075010 *How to test LDAP authentication*

To install directory services for iLO 2, an administrator must extend the eDirectory schema.

Required Schema Software

The iLO 2 requires specific software to extend the schema and provide snap-ins to manage the iLO 2 network. An HP Smart Component that contains the schema installer and the management snap-in installer is available for download from the HP website at http://www.hp.com/go/integrityiLO.

The two components you need for Integrity iLO 2 directory integration are the Schema Extender Utility and the Snap-in Installer.

Schema Installer

One or more `.xml`files are bundled with the schema installer. These files contain the schema that is added to the directory. Typically, one of these files contains core schema that is common to all the supported directory services. Additional files contain only product-specific schema. The schema installer requires the use of the .NET Framework.

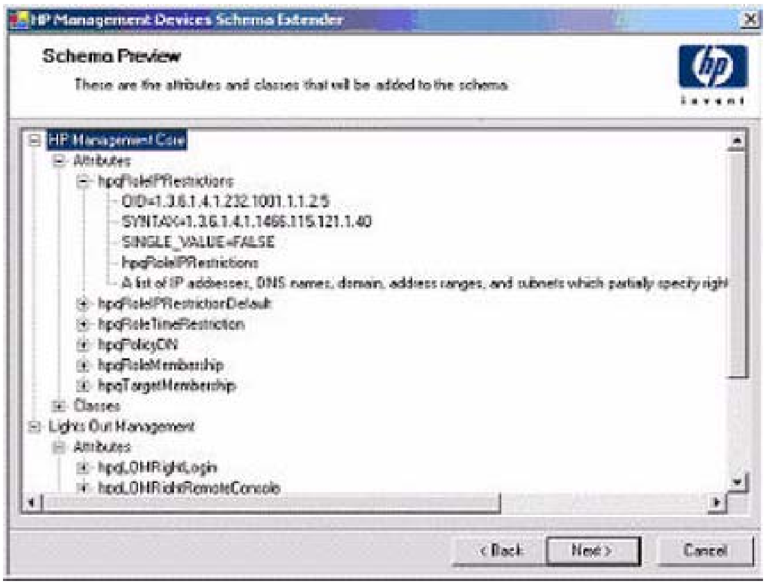
The schema installer includes three important screens:

- Schema Preview
- Setup
- Results

Schema Preview Screen

The Schema Preview screen (Figure 46) enables you to view proposed extensions to the schema. This application reads the selected schema files, parses the XML, and displays the schema on the screen in a tree view listing all of the details of the attributes and classes that are installed.

Figure 46 Schema Preview Screen



HP Management Devices Schema Extender

Schema Preview

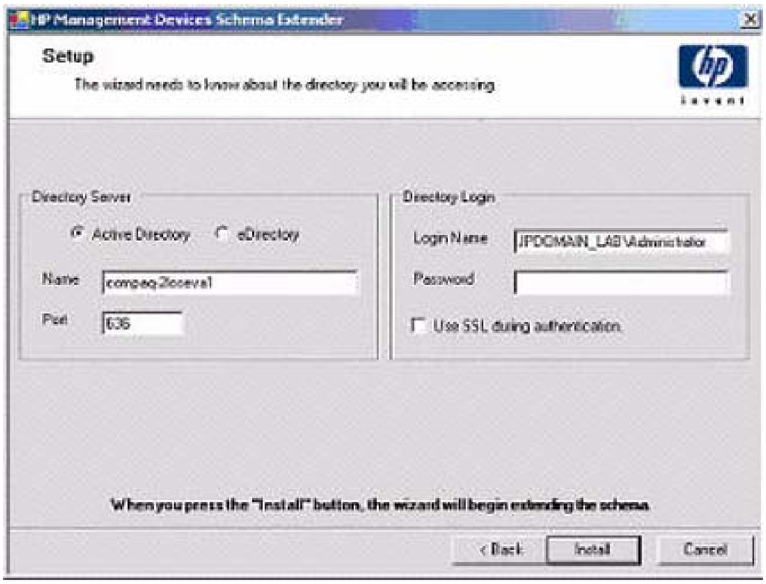
These are the attributes and classes that will be added to the schema.

```
HP Management Core
  Attributes
    hpqRoleIPRestrictions
      OID=1.3.6.1.4.1.232.1001.1.1.2.5
      SYNTAX=1.3.6.1.4.1.1466.115.121.1.40
      SINGLE_VALUE=FALSE
      hpqRoleIPRestrictions
      A list of IP addresses, DNS names, domain, address ranges, and subnets which partially specify righ
    hpqRoleIPRestrictionDefault
    hpqRoleTimeRestriction
    hpqPolicyDN
    hpqRoleMembership
    hpqTargetMembership
  Classes
Lights Out Management
  Attributes
    hpqLOMRightLogin
    hpqLOMRightRemoteConsole
```

Setup Screen

Use the Setup screen (Figure 47) to enter information before extending the schema.

Figure 47 Schema Setup Screen



HP Management Devices Schema Extender

Setup

The wizard needs to know about the directory you will be accessing

Directory Server

● Active Directory ○ eDirectory

Name: compaq-2kceval

Port: 636

Directory Login

Login Name: JPDOMAIN_LAB\Administrator

Password:

□ Use SSL during authentication

When you press the "Install" button, the wizard will begin extending the schema.

The Directory Server section of the Setup screen enables you to select whether to use Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

IMPORTANT: To extend the schema on Active Directory you must be an authenticated schema administrator, the schema must not be write protected, and the directory must be the flexible single master operation (FSMO) role owner in the tree. The installer attempts to make the target directory server the FSMO schema master.

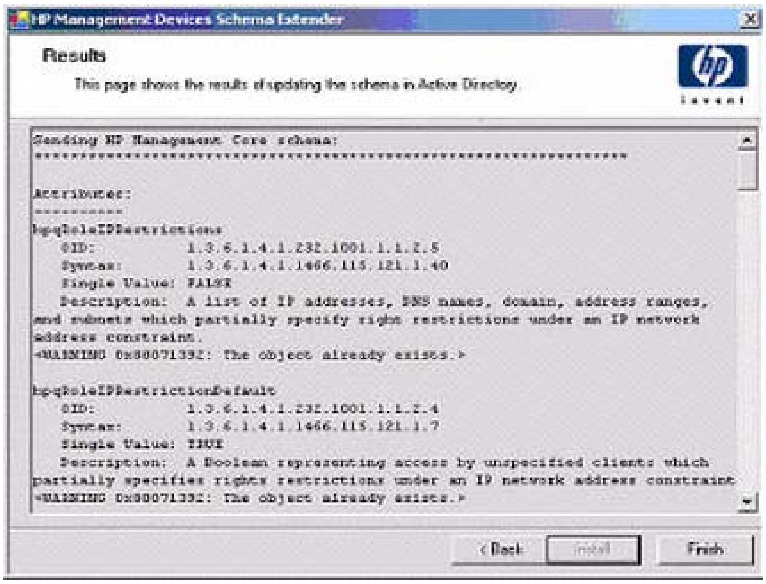
To obtain write access to the schema in Windows 2000, you must change the registry safety interlock. If you select the Active Directory option, the schema extender attempts to change the registry. The schema extender can only change the registry if the administrator who is extending the schema has the appropriate rights. Write access to the schema is automatically enabled on Windows Server 2003.

The Directory Login section of the Setup screen enables you to enter your login name and password which may be required to complete the schema extension. The Use SSL During Authentication option sets the form of secure authentication to be used. If selected, directory authentication using SSL is used. If not selected and Active Directory is selected, Windows NT® authentication is used. If not selected and eDirectory is selected, the administrator authentication and the schema extension continues using an unencrypted (clear text) connection.

Results Screen

The Results screen (Figure 48) displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Figure 48 Schema Results Screen


HP Management Devices Schema Extender
Results
This page shows the results of updating the schema in Active Directory
invent
< Back
Install
Finish

```
Sending HP Management Core schema:
**********************************************************************

Attributes:
----------
hpqRoleIPRestrictions
    OID:            1.3.6.1.4.1.232.1001.1.1.2.5
    Syntax:         1.3.6.1.4.1.1466.115.121.1.40
    Single Value:   FALSE
    Description:  A list of IP addresses, DNS names, domain, address ranges,
and subnets which partially specify right restrictions under an IP network
address constraint.
<WARNING 0x80071392: The object already exists.>

hpqRoleIPRestrictionDefault
    OID:            1.3.6.1.4.1.232.1001.1.1.2.4
    Syntax:         1.3.6.1.4.1.1466.115.121.1.7
    Single Value:   TRUE
    Description:  A Boolean representing access by unspecified clients which
partially specifies rights restrictions under an IP network address constraint
<WARNING 0x80071392: The object already exists.>
```

Management Snap-In Installer

The management snap-in installer installs the snap-ins required to manage iLO 2 objects in a Microsoft Active Directory Users and Computers directory or in a Novell ConsoleOne directory.

To create an iLO 2 directory using iLO 2 snap-ins, perform the following tasks:

1. Create and manage iLO 2 objects and role objects.
2. Make the associations between iLO 2 objects and role objects.

Directory Services for Active Directory

HP provides a utility to automate much of the directory setup process. You can download the HP Directories Support for iLO 2 on the HP website at:

http://h20000.www2.hp.com/bizsupport/TechSupport/

The following sections provide installation prerequisites, preparation, and a working example of directory services for Active Directory.

Active Directory Installation Prerequisites

The following are prerequisites for installing Active Directory:

- The Active Directory must have a digital certificate installed to enable iLO 2 to connect securely over the network.
- The Active Directory must have the schema extended to describe iLO 2 object classes and properties.
- The MP firmware must be Version F.01.57 or later.

  NOTE: Before performing certain iLO 2 functions, verify that you have the supported firmware version required to carry out the task. To make sure you have the latest supported firmware version, see the HP website at http://www.hp.com/go/bizsupport.

- The iLO 2 advanced features must be licensed.

Directory services for iLO 2 uses LDAP over SSL to communicate with the directory servers. Before installing snap-ins and schema for Active Directory, read and have available the following documentation:

IMPORTANT: To install directory services for iLO 2, an Active Directory schema administrator must extend the schema.

- Extending the schema in the Microsoft Windows 2000 Server Resource Kit, available at: http://www.microsoft.com
- Installing Active Directory in the Microsoft Windows 2000 Server Resource Kit, available at: http://www.microsoft.com
- Microsoft Knowledge Base articles:
  - 216999 “How to Install the Remote Server Administration Tools in Windows”
  - 314978 “How to Use `Adminpak.msi` to Install a Specific Server Administration Tool in Windows 2000”
  - 247078 “How to Enable SSL Communication over LDAP for Windows 2000 Domain Controllers”
  - 321051 “How to Enable LDAP over SSL with a Third-Party Certification Authority”
  - 299687 MS01-036 “Function Exposed by Using LDAP over SSL Could Enable Passwords to Be Changed”

Integrity iLO 2 requires a secure connection to communicate with the directory service. This secure connection requires the installation of the Microsoft CA. For more information, see the following Microsoft technical references:

- Securing Windows 2000, Appendix D, Configuring Digital Certificates on Domain Controllers for Secure LDAP and SMTP Replication at: http://www.microsoft.com
- Microsoft Knowledge Base Article 321051 “How to Enable LDAP over SSL with a Third-Party Certification Authority”

Preparing Directory Services for Active Directory

To set up directory services for use with iLO 2:

1. Install Active Directory. For more information, see the resource kit, Installing Active Directory in the Microsoft Windows 2000 Server.
2. Install the Microsoft Admin Pack (the `ADMINPAK.MSI` file, which is located in the i386 subdirectory of the Windows 2000 Server or Advanced Server CD). For more information, see the Microsoft Knowledge Base Article 216999.
3. In Windows 2000, the safety interlock that prevents accidental writes to the schema must be temporarily disabled. The schema extender utility can do this if the remote registry service is running and you have appropriate rights. You can also do this by setting **`HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Services NTDS Parameters Schema Update Allowed`** in the registry to a nonzero value (see the “Order of Processing When Extending the Schema” section of the Installation of Schema Extensions in the Windows 2000 Server Resource Kit), or by doing the following:

   CAUTION: Incorrectly editing the registry can severely damage your system. HP recommends creating a backup of any valued data on the computer before making changes to the registry.

   NOTE: This step is not necessary if you are using Windows Server 2003.

   a. Start the MMC.
   b. In MMC, install the Active Directory schema snap-in.
   c. Right-click **Active Directory Schema** and select **Operations Master**.
   d. Select **The Schema may be modified on this Domain Controller**.

    e. Click **OK**.

    The Active Directory schema folder may need to be expanded for the checkbox to be available.

4. Create a certificate or install Certificate Services. This step is necessary because iLO 2 uses SSL to communicate with Active Directory.
5. To specify that a certificate be issued to the server running Active Directory, do the following:
    a. Launch MMC on the server and add the default domain policy snap-in (Group policy and browse to default domain policy object).
    b. Click **Computer Configuration>Windows Settings>Security Settings>Public Key Policies**.
    c. Right-click **Automatic Certificate Requests Settings**, and select **New>Automatic Certificate Request**.
    d. Using the wizard, select the domain controller template and the certificate authority you want to use.
6. Download the Smart Component that contains the installers for the schema extender and the snap-ins. You can download the Smart Component from the HP website at http://www.hp.com/go/integrityiLO.
7. Run the schema installer application to extend the schema, which extends the directory schema with the proper HP objects.

    The schema installer associates the Active Directory snap-ins with the new schema. The snap-in installation setup utility is a Windows MSI setup script and runs anywhere MSI is supported (Windows XP, Windows 2000, Windows 98). However, some parts of the schema extension application require the .NET Framework, which you can download from the Microsoft website at http://www.microsoft.com.

Installing and Initializing Snap-Ins for Active Directory

Follow these steps to install the snap-ins and configure the directory service:

1. To install the snap-ins, run the snap-in installation application.
2. Configure the directory service with the appropriate objects and relationships for iLO 2 management:
    a. Use the management snap-ins from HP to create iLO 2 policy, admin, and user role objects.
    b. Use the management snap-ins from HP to build associations between the iLO 2 object, the policy object, and the role object.
    c. Point the iLO 2 object to the admin and user role objects (admin and user roles automatically point back to the iLO 2 object).

    For more information about iLO 2 objects, see “Directory Services Objects” (page 179).

At a minimum, create:

- One role object that contains one or more users and one or more iLO 2 objects.
- One iLO 2 object corresponding to each iLO 2 using the directory.

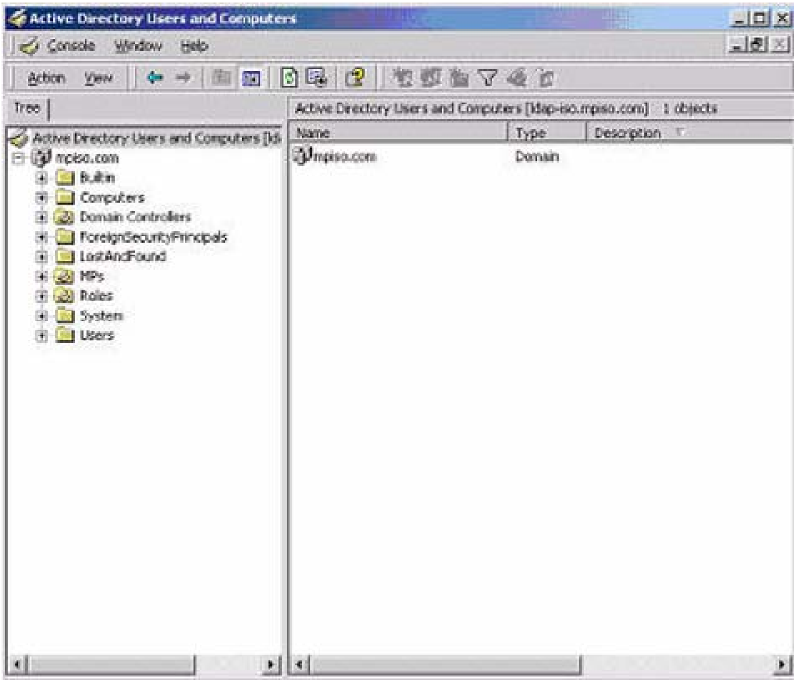
Example: Creating and Configuring Directory Objects for Use with iLO 2 in Active Directory

The following example shows how to set up roles and HP devices in an enterprise directory with the domain `mpiso.com`, which consists of two organizational units: Roles and MPs.

NOTE: Roles, such as hpqTargets and so on, are for extended schema LDAP only. They are not used in schema-free LDAP.

Assume that a company has an enterprise directory including the domain mpiso.com, arranged as shown in Figure 49.

Figure 49 Directory Example

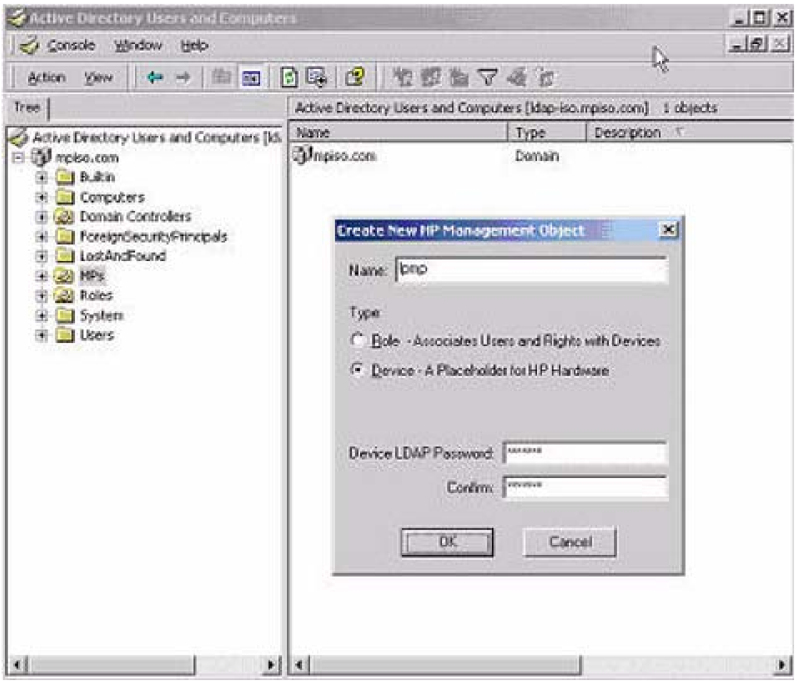


Active Directory Users and Computers [ldap-iso.mpiso.com] 1 objects

Name	Type	Description
mpiso.com	Domain	

1. Create an organizational unit to contain the iLO 2 devices managed by the domain. In this example, two organizational units are created, Roles and MPs.
2. Use the Active Directory Users and Computers snap-ins provided by HP to create iLO 2 objects for several iLO 2 devices in the MP organizational unit.
   a. In the `mpiso.com` domain, right-click the **MPs** organizational unit and select **NewHPObject**.
   b. In the Create New HP Management Object dialog box (Figure 50), select **Device** for the type.

Figure 50 Create New HP Management Object Dialog Box


Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers [ld
mpiso.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
MPs
Roles
System
Users
Create New HP Management Object
OK
Cancel

Active Directory Users and Computers [ldap-iso.mpiso.com] 1 objects

Name	Type	Description
mpiso.com	Domain	

Name: pmp

Type:

○ Role - Associates Users and Rights with Devices

● Device - A Placeholder for HP Hardware

Device LDAP Password: ******

Confirm: ******

c. In the Name field of the dialog box, enter an appropriate name In this example, the DNS host name of the iLO 2 device, `lpmp`, is used as the name of the iLO 2 object, and the surname is iLO 2.

d. Enter and confirm a password in the Device LDAP Password and Confirm fields (this is optional).

e. Click **OK**.

3. Use the HP provided Active Directory Users and Computers snap-ins to create HP role objects in the roles organizational unit.
4. Right-click the **Roles** organizational unit, select **New**, and select **Object**. The Create New HP Management Object dialog box appears.

   a. In the Type field, select **Role**.

   b. In the Name field, enter an appropriate name. In this example, the role contains users trusted for remote server administration and is named remoteAdmins.

   c. Click **OK**

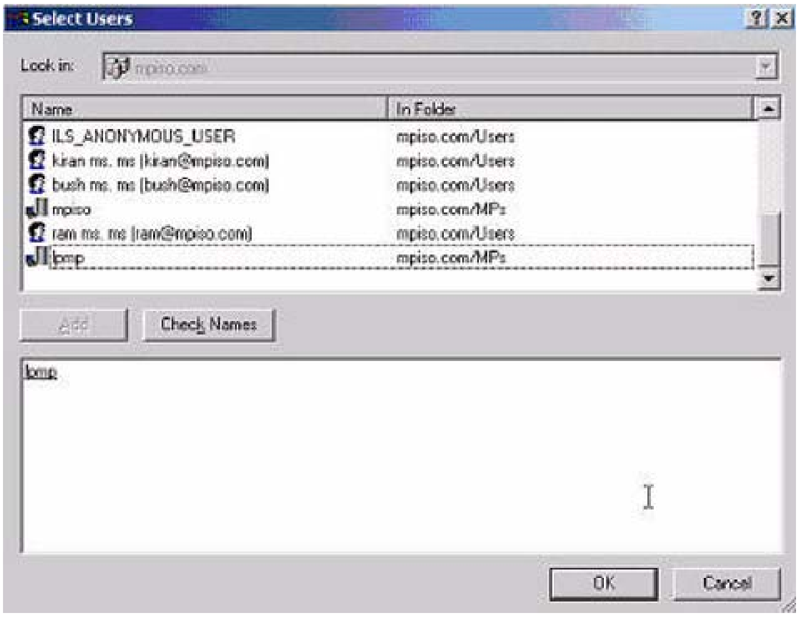
   d. Repeat the process, creating a role for remote server monitors named remoteMonitors.
5. Use the Active Directory Users and Computers snap-ins provided by HP to assign the roles rights, and associate the roles with users and devices.

   a. In the Roles organizational unit in the mpiso.com domain, right-click the **remoteAdmins** role , and select **Properties**.

   b. Select the HP Devices tab and click **Add**.

   c. From the Select Users dialog box (Figure 51), select the iLO 2 object created in step 2: (`lpmp` in folder `mpiso.com`/MPs). Click **OK**.

Figure 51 Select Users Dialog Box



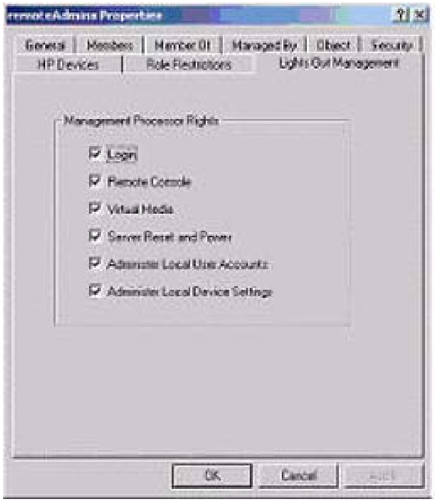
Name	In Folder
ILS_ANONYMOUS_USER	mpiso.com/Users
kiran ms. ms (kiran@mpiso.com)	mpiso.com/Users
bush ms. ms (bush@mpiso.com)	mpiso.com/Users
mpiso	mpiso.com/MPs
ram ms. ms (ram@mpiso.com)	mpiso.com/Users
lpmp	mpiso.com/MPs

lpmp

   d. To save the list, click **Apply**.

   e. To add users to the role, click the Members tab and use the **Add** button and the Select Users dialog box. Devices and users are now associated.
6. To set the rights for the role, use the Lights-Out Management tab (Figure 52). All users and groups within a role have rights assigned to the role on all of the iLO 2 devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the iLO 2 functionality. Select the appropriate rights and click **Apply**.

Figure 52 Lights-Out Management Tab



Management Processor Rights

☑ Login

☑ Remote Console

☑ Virtual Media

☑ Server Reset and Power

☑ Administer Local User Accounts

☑ Administer Local Device Settings

7. Click **OK**.
8. Using the same procedure in step 4, edit the properties of the remoteMonitors role, add the lpmp device to the Managed Devices list on the HP Devices tab, and use the Members tab to add users to the remoteMonitors role.
9. On the Lights-Out Management tab, click the **Login** checkbox.
10. Click **Apply** and **OK**. Members of the **remoteMonitors** role are able to authenticate and view the server status.

User rights to any iLO 2 are calculated as the sum of all the rights assigned by all the roles in which the user is a member and the iLO 2 is a managed device. Following the preceding examples, if a user is included in both the remoteAdmins and remoteMonitors roles, he or she has all the rights of those roles, because the remoteAdmins role also has those rights.

To configure iLO 2 and associate it with an iLO 2 object, use settings similar to the following (based on the preceding example) in the iLO 2 Directory Settings text user interface:

```
RIB Object DN = cn=lpmp,ou=MPs,dc=mpiso,dc=com
Directory User Context 1 = cn=Users,dc=mpiso,dc=com
```

For example, user Mel Moore (with the unique ID MooreM, located in the Users organizational unit within the mpiso.com domain, and a member of one of the remoteAdmins or remoteMonitors roles) would be allowed to log in to the iLO 2. To log in, he would enter `mpiso moorem`, or `moorem@mpiso.com`, or `Mel Moore`, in the Login Name field of the iLO 2 login, and use his Active Directory password in the Password field.

Directory Services Objects

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization enables the administrator to build relationships between a managed device and user or groups already contained within the directory service. The iLO 2 user management requires the following basic objects in the directory service:

- iLO 2
- Role
- User

Each object represents a device, user, or relationship that is required for directory-based management.

NOTE: After you install the snap-ins, restart ConsoleOne and MMC to display the new entries.

After the snap-in is installed, you can create iLO 2 objects and roles in the directory. Using the Users and Computers tool, you can:

- Create iLO 2 objects and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

Active Directory Snap-Ins

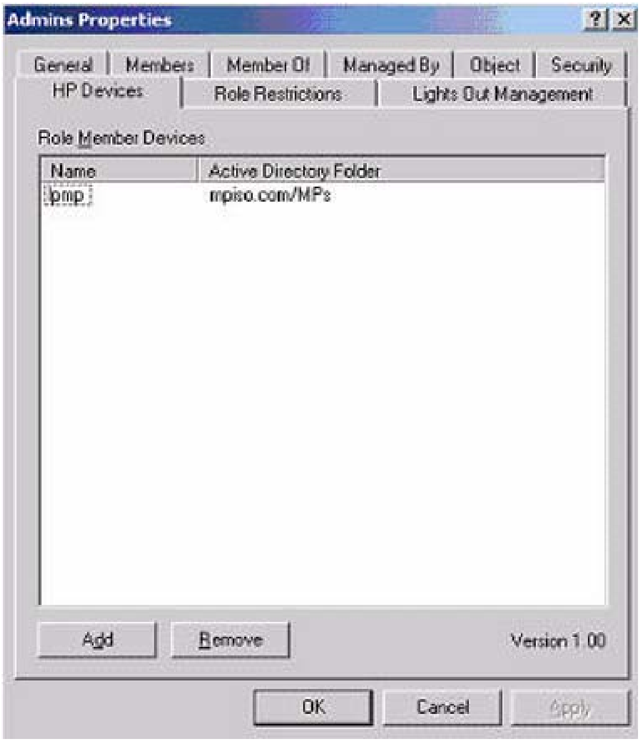
The following sections discuss the additional management options available in Active Directory Users and Computers after you have installed the HP snap-ins.

Managing HP Devices In a Role

To add HP devices to be managed in a role, use the HP Devices tab (Figure 53).

- To browse to a specific HP device and add it to the list of member devices, click **Add**.
- To browse to a specific HP device and remove it from the list of member devices, click **Remove**.

Figure 53 HP Devices Tab



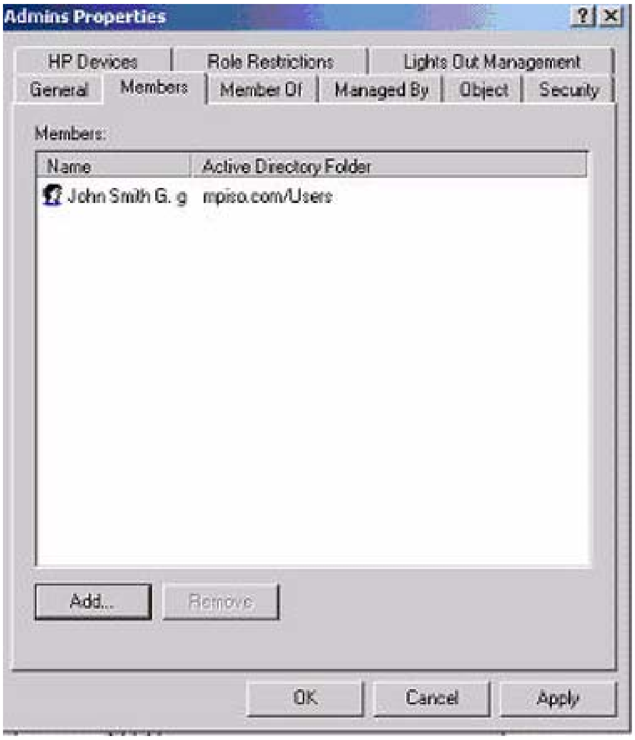
Name	Active Directory Folder
pmp	mpiso.com/MPs

Managing Users In a Role

After user objects are created, use the Members tab (Figure 54) to manage the users within the role.

- To add a user, browse to the specific user you want to add, and click **Add**.
- To remove a user from the list of valid members, highlight an existing user and click **Remove**.

Figure 54 Members Tab



Members:

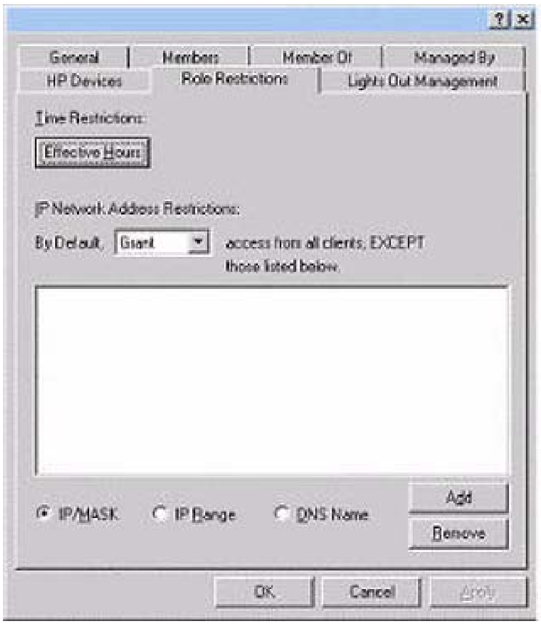
Name	Active Directory Folder
John Smith G. g	mpiso.com/Users

Setting Login Restrictions

The Role Restrictions tab (Figure 55) enables you to set login restrictions for a role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
  - DNS Name

Figure 55 Role Restrictions Tab



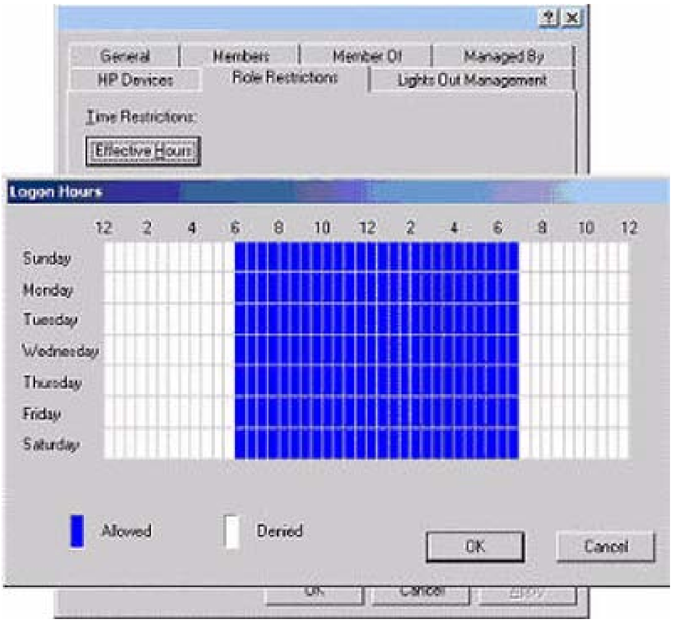
By Default, Grant access from all clients, EXCEPT those listed below.

● IP/MASK ○ IP Range ○ DNS Name

Setting Time Restrictions

- To manage the hours available for login by members of the role, click the Effective Hours button. The Logon Hours screen appears (Figure 56).
- To select the times available for login each day of the week in half-hour increments, use the Logon Hours screen. You can change a single square by clicking it, or you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button.
- Use the default setting to allow access at all times.

Figure 56 Logon Hours Screen



Defining Client IP Address or DNS Name Access

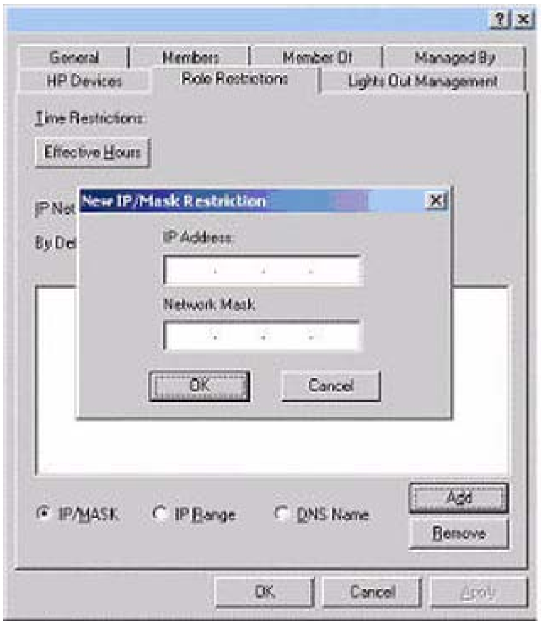
From the Role Restrictions tab you can grant or deny access to an IP address, IP address range, or DNS names.

In the By Default list, select whether to grant or deny access from all addresses except for specified IP addresses, IP address ranges, and DNS names.

To restrict an IP address:

1. From the Role Restrictions tab, select **IP/MASK** and click **Add**. The New IP/Mask Restriction dialog box appears (Figure 57).

Figure 57 New IP/Mask Dialog Box



2. In the New IP/Mask Restriction dialog box, enter the information and click **OK**.
3. To restrict access based on a DNS, select **DNS Name** and click **Add**. The New DNS Name Restriction dialog box appears. The DNS Name option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com.
4. Enter the information and click **OK.**
5. To save the changes, click **OK**.

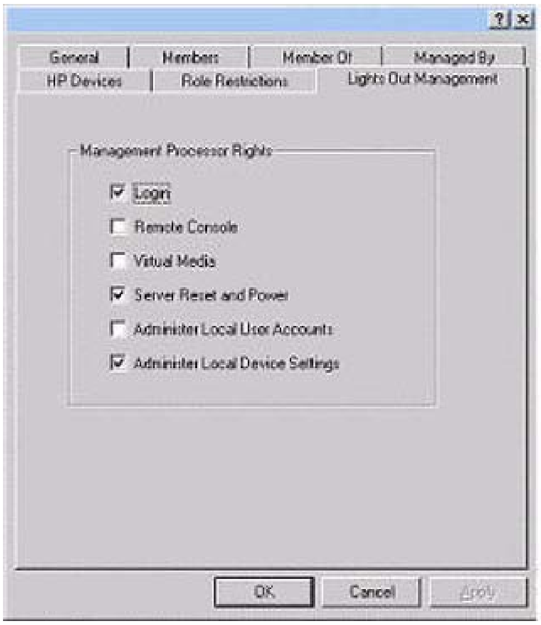
To remove any of the entries, highlight the entry in the display list and click **Remove**.

Setting User or Group Role Rights

After you create a role, you can select rights for that role. You can enable users and group objects to be members of the role, giving each the rights granted by the role.

Use the Lights-Out Management tab (Figure 58) to manage rights.

Figure 58 Lights-Out Management Tab



Management Processor Rights

☑ Login

☐ Remote Console

☐ Virtual Media

☑ Server Reset and Power

☐ Administer Local User Accounts

☑ Administer Local Device Settings

Table 78 lists the available Lights-Out Management rights.

Table 78 Lights-Out Management Rights

MP Rights	Description
Login	This option controls whether users can log in to the associated devices and execute `Status` or `Read-only` commands (view event logs and console logs, check system status, power status, and so on) but not execute any commands that would alter the state of iLO 2 or the system.
Remote Console	This option enables users to access the system console (the host OS).
Virtual Media	This option enables users to connect devices through the network such as CD, DVD, and network drives as virtual devices.
Server Reset and Power	This option enables users to execute iLO 2 power operations to remotely power on, power off, or reset the host platform, as well as configure the system's power restore policy.
Administer Local User Accounts	This option enables users to administer local iLO 2 user accounts.
Administer Local Device Settings	This option enables users to configure all iLO 2 settings, as well as reboot LO 2.

Directory Services for eDirectory

The following sections provide installation prerequisites, preparation, and a working example of directory services for eDirectory.

NOTE: Schema-Free LDAP is not supported with eDirectory.

Installing and Initializing Snap-In for eDirectory

For instructions on using the snap-in installation application, see "Installing and Initializing Snap-Ins for Active Directory" (page 176).

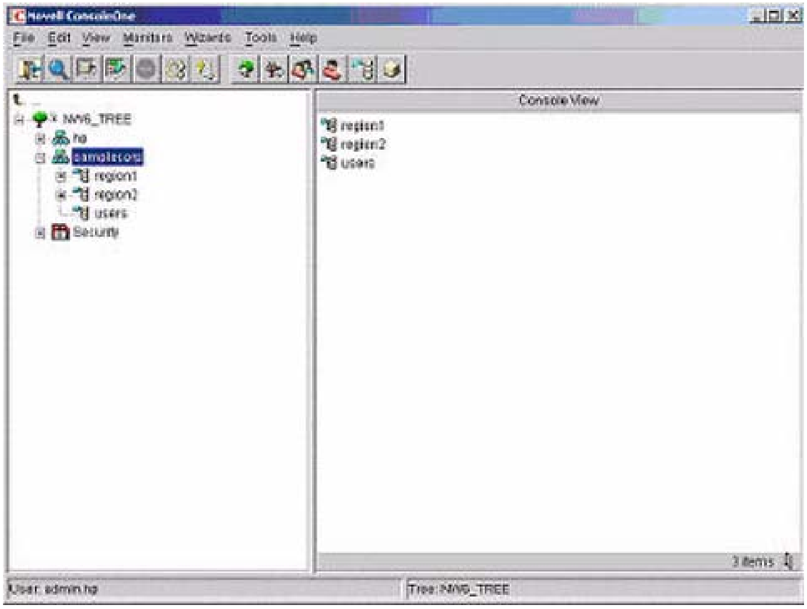
NOTE: After you install snap-ins, restart ConsoleOne and MMC to show the new entries.

Example: Creating and Configuring Directory Objects for Use with iLO 2 Devices in eDirectory

The following example demonstrates how to set up roles and HP devices in a company called samplecorp, which consists of two regions: region1 and region2.

Assume that samplecorp has an enterprise directory arranged according to that in Figure 59.

Figure 59 Roles and Devices Example



Begin by creating organizational units in each region to contain iLO 2 devices and roles specific to that region. In this example, two organizational units are created, roles and HP devices, in each organizational unit (region1 and region2).

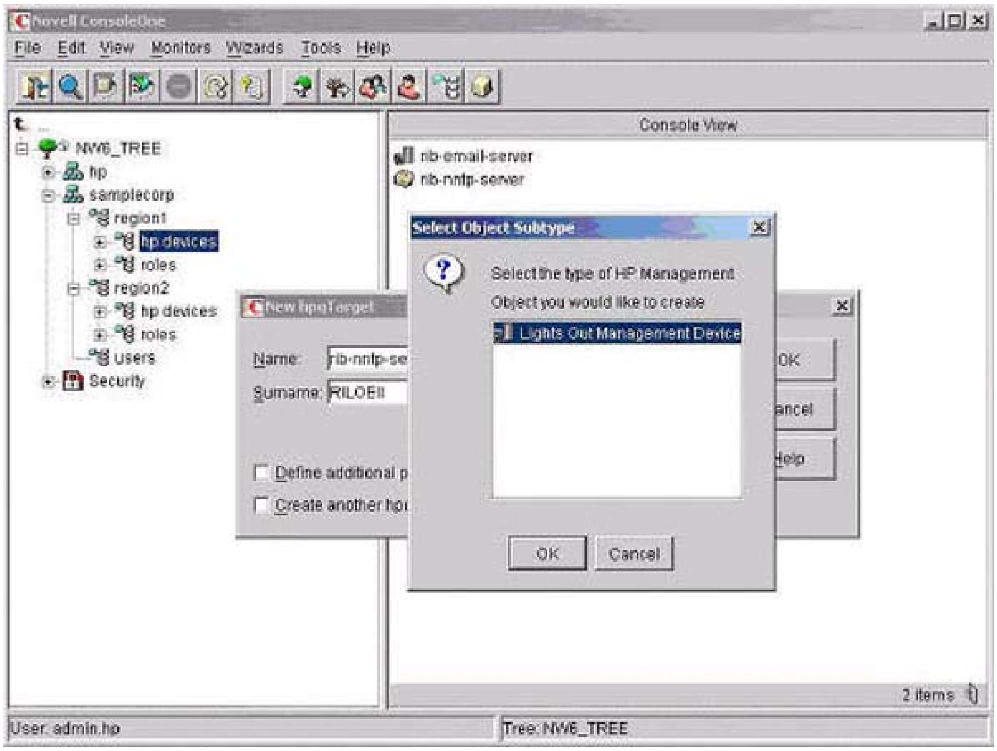
Creating Objects

To create iLO 2 objects:

1. Use the ConsoleOne snap-ins provided by HP to create iLO 2 objects in the HP devices organizational unit for several iLO 2 devices.

2. From in the region1 organizational unit, right-click the **HP devices** organizational unit. Select **New**, and select **Object**.
   a. Select **hpqTarget** from the list of classes, and click **OK**.
   b. Enter an appropriate name and surname in the New hpqTarget dialog box. In this example, the DNS host name of the iLO 2 device, rib-email-server, is used as the name of the iLO 2 object, and the surname is RILOEII (iLO 2). Click **OK**. The Select Object Subtype dialog box (Figure 60) appears.

Figure 60 Select Object Subtype Dialog Box



Select the type of HP Management Object you would like to create

Name: rib-nntp-se

Surname: RILOEII

   c. Select **Lights-Out Management Device** from the list, and click **OK**.
   d. Repeat the process for several more iLO 2 devices with the DNS names rib-nntp-server and rib-file-server-users1 in HP devices under region1, and rib-file-server-users2 and rib-app-server in HP devices under region2.

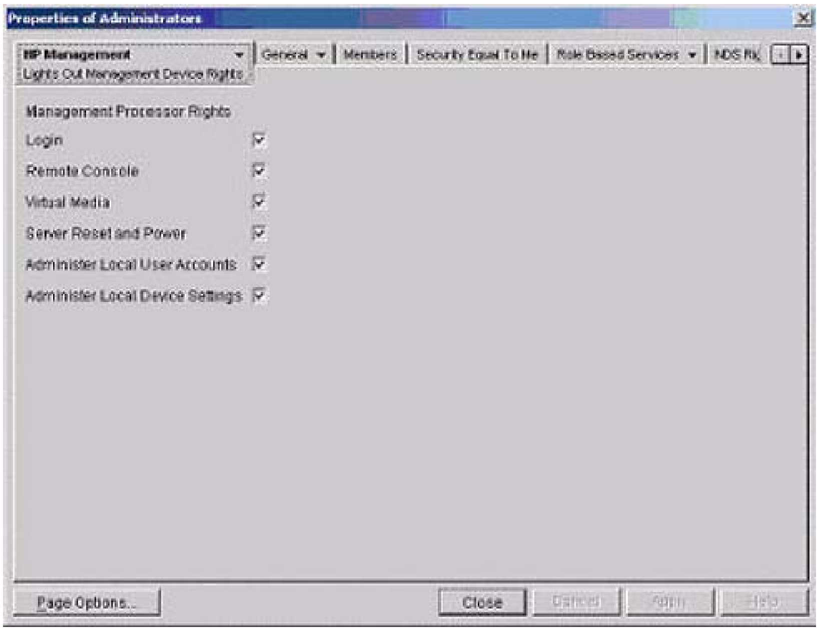
Creating Roles

To create roles:

1. Use the ConsoleOne snap-ins provided by HP to create HP role objects in the roles organizational units.
   a. From the region2 organizational unit, right-click the **roles** organizational unit. Select **New**, and select **Object**.
   b. Select **hpqRole** from the list of classes, and click **OK**.
   c. Enter an appropriate name in the New hpqRole dialog box. In this example, the role contains users trusted for remote server administration and is named remoteAdmins.
   d. Click **OK**. The Select Object Subtype dialog box appears.
   e. Select **Lights-Out Management Devices** from the list, and click **OK**.
2. Repeat the process, creating a role for remote server monitors named remoteMonitors in region1 roles, and a remoteAdmins and remoteMonitors role in region2.
3. Use the ConsoleOne snap-ins provided by HP to assign rights to the role and associate the roles with users and devices.

    a. Right-click the **remoteAdmins** role in the roles organizational unit in the region1 organizational unit, and select **Properties**.
    b. Select the Role Managed Devices subtab of the HP Management tab, and click **Add**.
    c. Using the Select Objects dialog box, browse to the HP devices organizational unit in the region1 organizational unit. Select the three iLO 2 objects created in step 2. Click **OK** and click **Apply**.
    d. Add users to the role. Click the Members tab, and add users using **Add** and the Select Objects dialog box. The devices and users are now associated.
    e. To set the rights for the role, use the Lights-Out Management Device Rights subtab of the HP Management tab (Figure 61).

Figure 61 Setting Role Rights



Management Processor Rights

Login ☑

Remote Console ☑

Virtual Media ☑

Server Reset and Power ☑

Administer Local User Accounts ☑

Administer Local Device Settings ☑

All users within a role will have rights assigned to the role on all he iLO 2 devices managed by the role. In this example, users in the remoteAdmins role are given full access to iLO 2 functionality. Select the boxes next to each right, and click **Apply**.

    f. To close the property sheet, click **Close**.

4. Using the same procedure as in step 3, edit the properties of the remoteMonitors role:
    a. Add the three iLO 2 devices within HP devices under region1 to the Managed Devices list on the Role Managed Devices subtab of the HP Management tab.
    b. Add users to the remoteMonitors role using the Members tab.
    c. Using the Lights-Out Management Device Rights subtab of the HP Management tab, click the **Login** checkbox, and click **Apply** and **Close**. Members of the remoteMonitors role are now able to authenticate and view the server status.

User rights to any iLO 2 device are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and in which the iLO 2 device is a managed device. Using the preceding examples, if a user is in both the remoteAdmins and remoteMonitors roles, he or she has all rights, because the remoteAdmins role has those rights.

To configure an iLO 2 device from the previous example and associate it with an iLO 2 object, use settings similar to the following on the iLO 2 directory settings TUI.

NOTE: In LDAP Distinguished Names, use commas, not periods, to separate each component.

```
RIB Object DN = cn=rib-email-server,ou=hp
```

```
devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

For example, user CSmith (located in the users organizational unit within the samplecorp organization, who is also a member of one of the remoteAdmins or remoteMonitors roles) would be allowed to log in to iLO 2. He would type **`csmith`** (case insensitive) in the Login Name field of the iLO 2 login, and use his eDirectory password in the Password field to gain access.

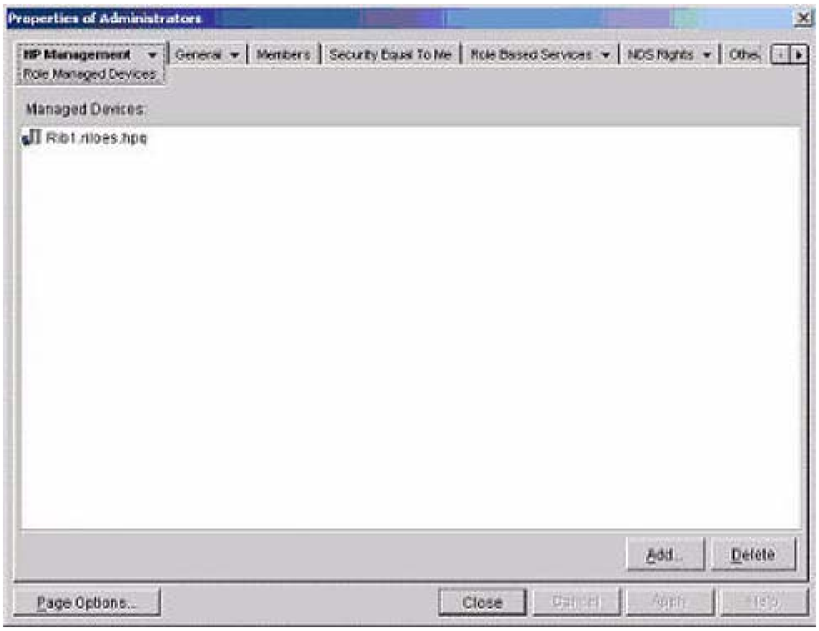
Directory Services Objects for eDirectory

Directory services objects enable virtualization of managed devices and the relationships between a managed device and a user or groups already contained within the directory service.

Adding Role Managed Devices

Use the Role Managed Devices subtab under the HP Management tab (Figure 62) to add HP devices to be managed within a role.

Figure 62 Role Managed Devices Subtab

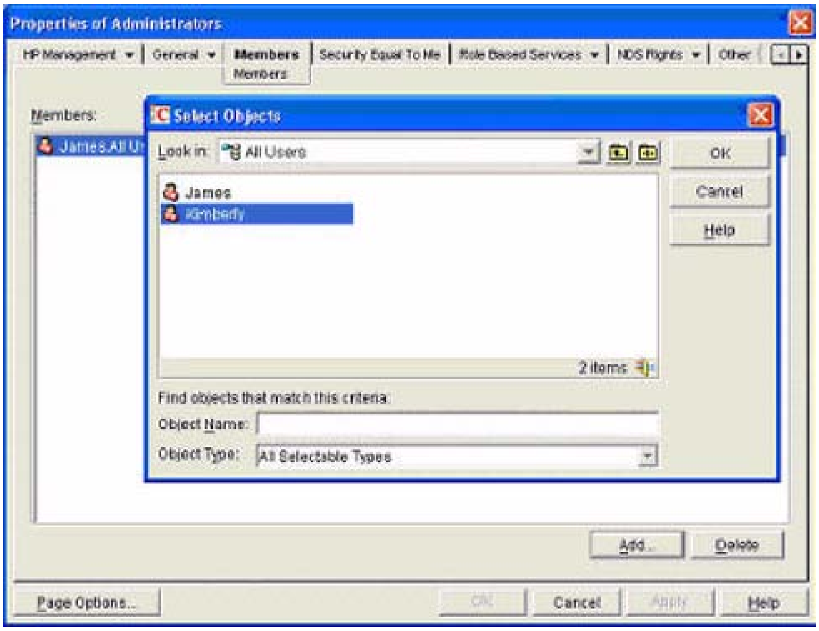


To browse to the specific HP device and add it as a managed device, click **Add**.

Adding Members

After you create user objects, use the Members tab (Figure 63) to manage users within a role.

Figure 63 Members Tab (eDirectory)



Look in: All Users

Object Name:

Object Type: All Selectable Types

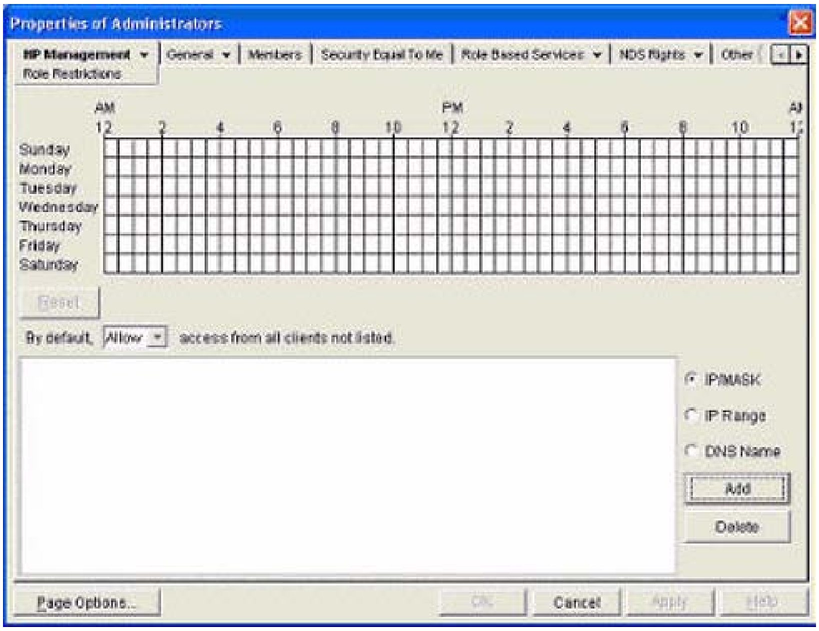
To browse to the specific user you want to add, click **Add**.

To remove a user from the list of valid members, highlight the user name and click **Delete**.

Setting Role Restrictions

The Role Restrictions subtab (Figure 64) enables you to set login restrictions for a role.

Figure 64 Role Restrictions Subtab (eDirectory)



By default, Allow access from all clients not listed.

● IP/MASK

These restrictions include the following:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
- DNS Name

Setting Time Restrictions

You can manage the hours available for login by members of a role using the time grid displayed in the Role Restrictions subtab (Figure 64). You can select the times available for login for each day of the week in half-hour increments. You can change a single square by clicking it or change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

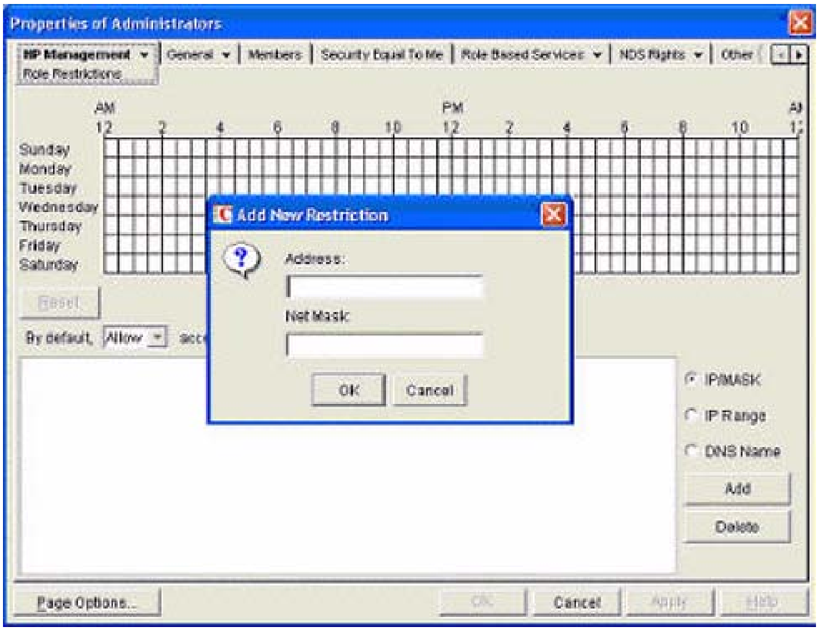
Defining Client IP Address or DNS Name Access

You can grant or deny access to an IP address, IP address range, or DNS names.

Using the By Default list, select whether to allow or deny access from all addresses except the specified IP addresses, IP address ranges, and DNS names.

1. To restrict an IP address, select **IP/MASK** in the Role Restrictions subtab and click **Add**. The Add New Restriction dialog box for the IP/Mask option appears.
2. In the Add New Restriction dialog box (Figure 65), enter the information, and click **OK**.

Figure 65 Add New Restriction Dialog Box



By default, Allow acc

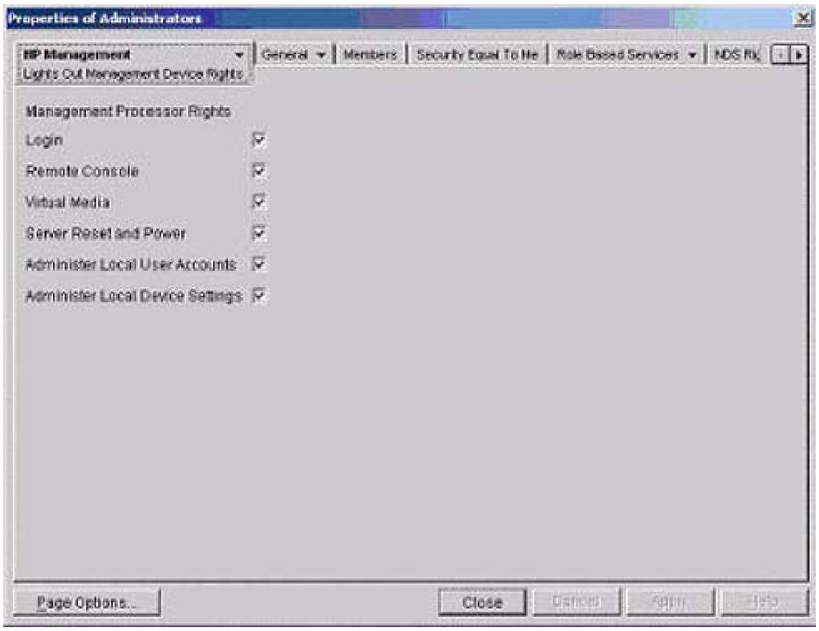
3. In the Role Restrictions subtab, select **DNS Name** and click **Add**. The DNS Name option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com. The New DNS Name Restriction dialog box appears.
4. Enter the information and click **OK**.
5. To save the changes, click **Apply**.

To remove any of the entries, highlight the entry in the display field and click **Delete**.

Setting Lights-Out Management Device Rights

After you create a role, you can select rights for the role and make users and group objects members of the role, which gives users or groups of users the rights granted by that role. Use the Lights-Out Management Device Rights subtab of the HP Management tab (Figure 66) to manage rights.

Figure 66 Lights-Out Management Device Rights Tab



Management Processor Rights

Login ☑

Remote Console ☑

Virtual Media ☑

Server Reset and Power ☑

Administer Local User Accounts ☑

Administer Local Device Settings ☑

Table 79 lists the available management device rights.

Table 79 Management Device Rights

Option	Description
Login	This option controls whether users can log in to the associated devices and execute `status` or `read-only` commands (view event logs and console logs, check system status, power status, and so on) but not execute any commands that would alter the state of iLO 2 or the system.
Remote Console	This option enables users to access the system console (the host OS).
Virtual Media	This option enables users to connect devices through the network such as CD, DVD, and network drives as virtual devices.
Server Reset and Power	This option enables users to execute iLO 2 power operations to remotely power on, power off, or reset the host platform, as well as configure the system's power restore policy.
Administer Local User Accounts	This option enables users to administer local iLO 2 user accounts.
Administer Local Device Settings	This option enables users to configure all iLO 2 settings, as well as reboot iLO 2.

Installing Snap-Ins and Extending Schema for eDirectory on a Linux Platform

This section describes a method that does not require a Windows client to install snap-ins and extend schema for eDirectory on a Linux platform.

Schema extension is the addition of new classes to existing classes. You can use these classes to create objects to support a specific utility. New classes are added, such as hpqTarget, hpqPolicy and hpq role. HP has created objects using these classes to support iLO 2 devices (created using the hpqTarget class), and iLO 2 admins and monitors (created using the hpqRole class). These objects support the Login Authentication utility to the iLO 2 device and enable iLO 2 users to execute commands based on their assigned roles.

Installing the Java Runtime Environment

As a prerequisite for extending schema, you must have Java Runtime Environment (JRE) 1.4.2 installed.

To ensure you have the correct version of JRE installed on your system:

1. To determine the Java version, execute the following command:

   ```
   # java -version
   ```

   The Java version installed on your system is displayed.

2. If Java is not installed on your system, execute the following command:

   ```
   # rpm –iv j2re-1_4_2_04-linux-i586.rpm
   ```

   NOTE: You can download this `rpm` file from the Java website.

3. Execute the following command if:

   - Java is installed and the version is older than 1.4.2.
   - You want to upgrade the Java version and uninstall an older version.

   ```
   # rpm –Uv j2re-1_4_2_04-linux-i586.rpm
   ```

4. Add the entry **`/usr/java/j2re1.4.2_04/bin`** to the `.bash_profile` file.

Installing Snap-Ins

Create the HP directory under the `/usr/ConsoleOne/snapins/` directory, and copy the two `.jar` snap-in files, `hpqLOMv100.jar` and `hpqMgmtCore.jar`, to the HP directory. When the `hpdsse.sh` file is executed, the HP directory is automatically created and the two `.jar` files are copied to it.

NOTE: The `hpdsse.sh` file is obtained when the `Schema.tar` tar file is extracted. This process is explained in the Schema Extension section. You can download schema extensions from the HP website at: http://h18013.www1.hp.com/products/servers/management/directorysupp/index.html

Select Software and Drivers, and the operating system for the schema extension you want to install.

Extending Schema

To obtain the `hpdsse.sh` file:

1. Download the tar file to the Linux system where eDirectory is installed.
2. Extract the tar file to obtain the `hpdsse.sh` file by executing the following command:

   ```
   # tar –xvf Schema. tar
   ```

3. Run this file by executing the following command:

   ```
   # ./hpdsse.sh
   ```

   This command displays instructions. As indicated in the instructions to extend the schema, provide the server name, admin DN, and admin password as command line arguments.

4. To see the results, view the `schema.log` file, (created after the schema extension is complete).

   The log file lists the created classes and attributes. In addition, it shows the result as “Succeeded”. If the objects already exist, the message “Already Exists” appears in the log file.

The **Already Exists** message appears only when you try to run the same `.sh` file after the schema extension is complete.

The SSL port (636) is used during the schema extension. You can verify this by running the `netstat -nt    grep :636` command while the `hpdsse.sh` file is being executed.

Verifying Snap-In Installation and Schema Extension

To verify the installation of snap-ins and schema extension:

1. Run ConsoleOne and log on to the tree.
2. Verify the new classes by opening the **Schema Manager** from the Tools list.

   All the classes related to the HP directory services must be present in the classes list. The classes are hpqRole, hpqTarget, hpqPolicy, and hpqLOMv100.

Using the LDAP Command to Configure Directory Settings in iLO 2

Use the LDAP Command Menu in the iLO 2 MP TUI to configure iLO 2 LDAP directory settings.

The following is an example of the **LDAP** command output:

```
[mp1] MP:CM> LDAP

Current LDAP Directory Configuration:
L – LDAP Directory Authentication : Disabled
M – Local MP User database        : Enabled
I - Directory Server IP Address   : 192.0.2.1
P - Directory Server LDAP Port    : 636
D - Distinguished Name (DN)      : cn=mp,o=demo
1 - User Search Context 1        : o=mp
2 - User Search Context 2        : o=demo
3 - User Search Context 3        : o=test
Enter parameter(s) to change, A to modify All, or [Q] to Quit: a

  For each parameter, enter:
  New value, or
  <CR> to retain the current value, or
  DEFAULT to set the default value, or
 Q to Quit

LDAP Directory Authentication:
          E – Enabled
Current > D – Disabled (default)

Enter new value, or Q to Quit: e
 > LDAP Directory Authentication will be updated

Local MP User Accounts:
          D - Disabled  (default)
Current > E - Enabled

Enter new value, or Q to Quit: <CR>
   -> Current Local MP User Accounts has been retained

Directory Server IP Address:
   Current -> 127.0.0.1 (default)

Enter new value, or Q to Quit: 192.0.2.1
 -> Directory Server IP Address will be updated

Directory Server LDAP Port:
   Current -> 636 (default)

Enter new value, or Q to Quit: <CR>
 -> Current Directory Server LDAP Port has been retained

Distinguished Name (DN):
   Current -> cn=mp,o=demo
```

```
Enter new value, or Q to Quit: <CR>
   -> Current Distinguished Name has been retained

User Search Context 1:
   Current -> o=mp

Enter new value, or Q to Quit: <CR>
    -> Current User Search Context 1 has been retained

User Search Context 2:
   Current -> o=demo

Enter new value, or Q to Quit: <CR>
    -> Current User Search Context 2 has been retained

User Search Context 3:
   Current -> o=test

Enter new value, or Q to Quit: <CR>
    -> Current User Search Context 3 has been retained

New Directory Configuration (* modified values):
*L – LDAP Directory Authentication: Enabled
 M – Local MP User database       : Enabled
*I - Directory Server IP Address  : 192.0.2.1
 P - Directory Server LDAP Port   : 636
 D - Distinguished Name (DN)      : cn=mp,o=demo
 1 - User Search Context 1        : o=mp
 2 - User Search Context 2        : o=demo
 3 - User Search Context 3        : o=test

Enter Parameter(s) to revise, Y to confirm, or [Q] to Quit: y
 -> LDAP Configuration has been updated
```

User Login Using Directory Services

The MP Login Name field accepts all of the following:

- Directory users
- LDAP Fully Distinguished Names

  Example: CN=John Smith,CN=Users,DC=HP,DC=COM, or @HP.com

  The short form of the login name by itself does not identify which domain you are trying to access. To identify the domain, provide the domain name or use the LDAP Distinguished Name of your account.
- Domain\user name form (Active Directory only)

  Example: HP\jsmith
- username@domain form (Active Directory only)

  Directory users that are specified with the @ searchable form can be located in one of three searchable contexts that are configured within Directory Settings.

  Example: jsmith@hp.com
- User name form

  Example: John Smith

Directory users that are specified with the user name form can be located in one of three searchable contexts that are configured within Directory Settings.

- Local users - Login ID

  For the iLO 2 login, the maximum length of the Login Name is 25 characters for local users. For directory services users, the maximum length of the Login Name is 256 characters.

Certificate Services

The following sections provide instructions for installing Certificate Services, verifying directory services, and configuring automatic certificate requests.

Installing Certificate Services

To install Certificate Services:

1. **Select Start>Settings>Control Panel**.
2. Double-click **Add/Remove Programs**.
3. Click **Add/Remove Windows Components** to start the Windows Components wizard.
4. Select **Certificate Services** and click **Next**.
5. At the warning that the server cannot be renamed, click **OK**. The Enterprise root CA option is selected because there is no CA registered in the Active Directory.
6. Enter the information appropriate for your site and organization. Accept the default time period of two years in the Valid for field and click **Next**.
7. Accept the default locations of the certificate database and the database log. Click **Next**.
8. Browse to the `c: I386` folder when prompted for the Windows 2000 Advanced Server CD.
9. Click **Finish** to close the wizard.

Verifying Directory Services

Because iLO 2 communicates with Active Directory using SSL, you must create a certificate or install Certificate Services. Install an enterprise CA because you are issuing certificates to objects within your organizational domain.

To verify that certificate services is installed, select **Start>Programs>Administrative Tools>Certification Authority**. If **Certificate Services** is not installed, an error message appears.

Configuring an Automatic Certificate Request

To request that a certificate be issued to the server:

1. Select **Start>Run**, and enter **`mmc`**.
2. Click **Add**.
3. Select **Group Policy**, and click **Add** to add the snap-in to the MMC.
4. Click **Browse**, and select the **Default Domain Policy** object. Click **OK**.
5. Select **Finish>Close>OK**.
6. **Expand Computer Configuration>Windows Settings>Security Settings>Public Key Policies**.
7. Right-click **Automatic Certificate Requests Settings**, and select **New>Automatic Certificate Request**.
8. When the Automatic Certificate Request Setup wizard starts, click **Next**.
9. Select the **Domain Controller** template, and click **Next**.
10. Select the certificate authority listed. (the same CA defined during the Certificate Services installation). Click **Next**.
11. Click **Finish** to close the wizard.

Directory-Enabled Remote Management

This section is for administrators who are familiar with directory services and with the iLO 2 product. To familiarize yourself with the product and services, see "Directory Services" (page 169). Be sure you understand the examples and are comfortable with setting up the product.

In general, you can use the HP provided snap-ins to create objects. It is useful to give the iLO 2 device objects meaningful names, such as the device's network address, DNS name, host server name, or serial number.

Directory-enabled remote management enables you to:

- Create iLO 2 objects:

  Each device object created represents each device that will use the directory service to authenticate and authorize users. For more information, see the following sections:

  "Directory Services for Active Directory" (page 174)

  "Directory Services for eDirectory" (page 184)

- Configure iLO 2 devices:

  Every iLO 2 device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. For details about the specific directory settings, see "Using the LDAP Command to Configure Directory Settings in iLO 2" (page 193). In general, each device is configured with the appropriate directory server address, iLO 2 object distinguished name, and any user contexts. The server address is either the IP address or DNS name of a local directory server, or, for more redundancy, a multihost DNS name.

Using Existing Groups

Many organizations arrange users and administrators into groups. In many cases, it is convenient to use existing groups and associate these groups with one or more iLO 2 role objects. When the devices are associated with role objects, you can control access to the iLO 2 devices associated with the role by adding or deleting members from the groups.

When using Microsoft Active Directory, you can place one group within another, or create nested groups. Role objects are considered groups and can include other groups directly. To include other groups directly, add the existing nested group directly to the role and assign the appropriate rights and restrictions. Add new users to either the existing group or to the role.

Novell™ eDirectory does not allow nested groups. In eDirectory, any user who can read a role is considered a member of that role. When adding an existing group, organizational unit, or organization to a role, add the object as a read trustee of the role. All the members of the object are considered members of the role. Add new users to either the existing object or to the role.

When you use trustee or directory rights assignments to extend role membership, users must be able to read the iLO 2 object representing the iLO 2 device. Some environments require the trustees of a role to also be read trustees of the iLO 2 object to successfully authenticate users.

Using Multiple Roles

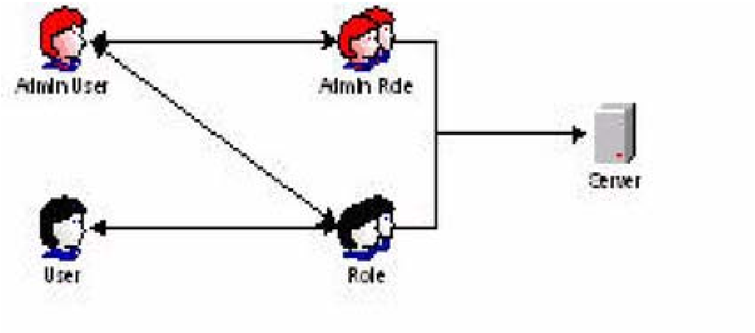
Most deployments do not require that the same user be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When building multiple-role relationships, users receive all the rights assigned by every applicable role. Roles only grant rights, not revoke them. If one role grants a user a right, the user has the right, even if the user is in another role that does not grant that right.

Typically, a directory administrator creates a base role with the minimum number of rights assigned and then creates additional roles to add additional rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization might have two types of users: administrators of the iLO 2 device or host server, and users of the iLO 2 device. In this situation, it makes sense to create two roles, one for the administrators and one for the users. Both roles include some of the same devices, but grant different rights. Sometimes, it is useful to assign generic rights to the lesser role, and include the iLO 2 administrators in that role, and the administrative role.

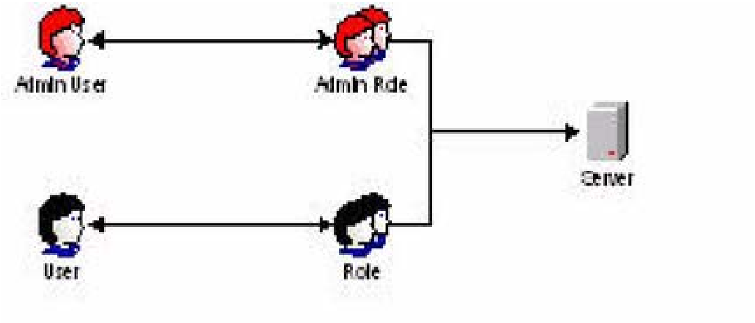
Figure 67 shows one way that an administrative user gains admin role right. The admin user's initial login right is granted through the regular user role. After the initial login, more advanced rights are assigned to the admin user through the admin role such as server reset and remote console.

Figure 67 Admin User Gaining Admin Role Right, Example 1



In Figure 68, the admin user gains the admin role right in a different way. The admin user initially logs in through the admin role and is immediately assigned admin rights (server reset, remote console, and login).

Figure 68 Admin User Gaining Admin Role Right, Example 2



Creating Roles that Follow Organizational Structure

Often, administrators within an organization are placed into a hierarchy in which subordinate administrators must assign rights independently of ranking administrators. In this case, it is useful to have one role that represents the rights assigned by higher-level administrators, and to allow subordinate administrators to create and manage their own roles.

Restricting Roles

Restrictions enable you to limit the scope of a role. A role only grants rights to those users who satisfy the role's restrictions. Using restricted roles creates users with dynamic rights that change based on the time of day or network address of the client.

For step-by-step instructions on how to create network and time restrictions for a role, see "Setting Role Restrictions" (page 189) or "Setting Time Restrictions" (page 190).

Role Time Restrictions

You can place time restrictions on iLO 2 roles. Users are only granted rights that are specified for the iLO 2 devices listed in the role if they are members of the role and meet the time restrictions for that role.

The iLO 2 devices use local host time to enforce time restrictions. If the iLO 2 device clock is not set, the role time restriction fails (unless no time restrictions are specified on the role).

Role-based time restrictions can only be enforced if the time is set on the iLO 2 device. The time is normally set when the host is booted and is maintained by running the agents in the host operating system, which enables iLO 2 device to compensate for leap years and minimize clock drift with respect to the host. Events such as unexpected power loss or the flashing of MP firmware can cause the iLO 2 device clock not to be set. Also, the host time must be correct for the iLO 2 device to preserve time across firmware flashes.

IP Address Range Restrictions

IP address range restrictions enable you to specify network addresses that are granted or denied access by the restriction. The address range is typically specified in a low-to-high range format. You can specify an address range to grant or deny access to a single address. Addresses that fall within the low-to-high IP address range meet the IP address restriction.

IP Address and Subnet Mask Restrictions

IP address and subnet mask restrictions enable you to specify a range of addresses that are granted or denied access by the restriction. This format has similar capabilities to those in an IP address range but can be more native to your networking environment. An IP address and subnet mask range is typically specified using a subnet address and address bit mask that identifies addresses on the same logical network.

In binary math, if the bits of a client machine address are added to the bits of the subnet mask, and these bits match the restriction subnet address, the client machine meets the restriction.

DNS-Based Restrictions

DNS-based restrictions use the network naming service to examine the logical name of the client machine by looking up machine names assigned to the client IP addresses. DNS restrictions require a functional name server. If the name service fails or cannot be reached, DNS restrictions cannot be matched and will fail.

DNS-based restrictions can limit access to a single, specific machine name or to machines sharing a common domain suffix. For example, the DNS restriction www.hp.com matches hosts that are assigned the domain name www.hp.com. However, the DNS restriction *.hp.com matches any machine originating from HP.

DNS restrictions can cause some ambiguity because a host can be multi-homed. DNS restrictions do not necessarily match one-to-one with a single system.

Using DNS-based restrictions can create some security complications. Name service protocols are insecure. Any individual with malicious intent and access to the network can place a rogue DNS service on the network, creating fake address restriction criteria. Organizational security policies should be taken into consideration when implementing DNS-based address restrictions.

Role Address Restrictions

Role address restrictions are enforced by the MP firmware, based on the client's IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

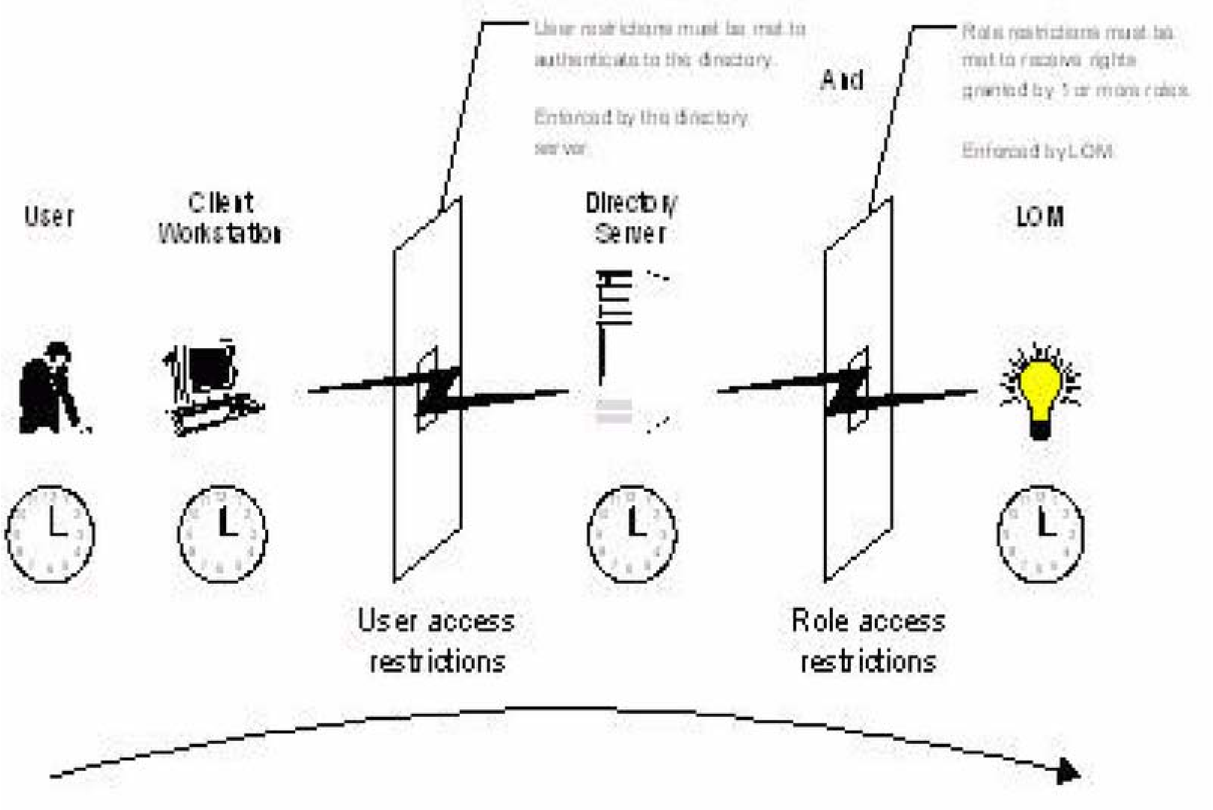
Address restrictions can be difficult to manage if access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

Enforcing Directory Login Restrictions

The following figure shows how two sets of restrictions potentially limit a directory user's access to iLO 2 devices. User access restrictions limit a user's access to authenticate to the directory. Role access restrictions limit an authenticated user's ability to receive iLO 2 privileges based on rights specified in one or more roles.

Figure 69 shows the user and role access restrictions.

Figure 69 User and Role Access Restrictions


User restrictions must be met to authenticate to the directory.
Enforced by the directory server.
And
Role restrictions must be met to receive rights granted by 1 or more roles.
Enforced by LOM
User
Client Workstation
Directory Server
LOM
User access restrictions
Role access restrictions

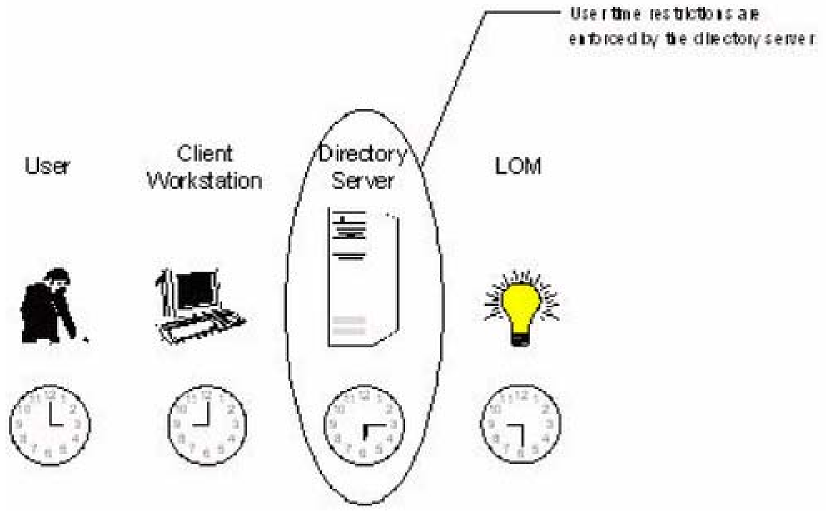
Enforcing User Time Restrictions

You can place a time restriction on directory user accounts. Time restrictions limit the ability of the user to log in (authenticate) to the directory. Typically, time restrictions are enforced using the time on the directory server, but if the directory server is located in a different time zones or a replica in a different time zone is accessed, time zone information from the managed object can be used to adjust for relative time.

While directory server evaluates user time restrictions, the determination can be complicated by time zone changes or by the authentication mechanism.

Figure 70 shows the user time restrictions.

Figure 70 User Time Restrictions



User Address Restrictions

You can place network address restrictions on a directory user account, and the directory server enforces these restrictions. See the directory service documentation for information about the enforcement of address restrictions on LDAP clients, such as a user logging in to an iLO 2 device.

Network address restrictions placed on the user in the directory may not be enforced in the expected manner if the directory user logs in through a proxy server. When a user logs in to an iLO 2 device as a directory user, the iLO 2 device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when accessing the iLO 2 device. However, because the user is proxied at the iLO 2 device, the network address of the authentication attempt is that of the iLO 2 device, not that of the client workstation.

Creating Multiple Restrictions and Roles

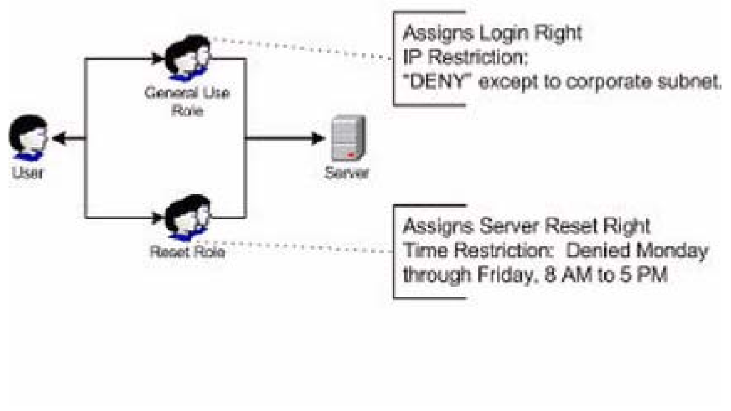
The most useful application of multiple roles includes restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables you to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which iLO 2 administrators are allowed to use the iLO 2 device from within the corporate network but are only able to reset the server outside of regular business hours.

Directory administrators may be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to an after-hours application might allow administrators outside the corporate network, to reset the server, which is contrary to most security policies.

Figure 71 shows how security policy dictates that general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.

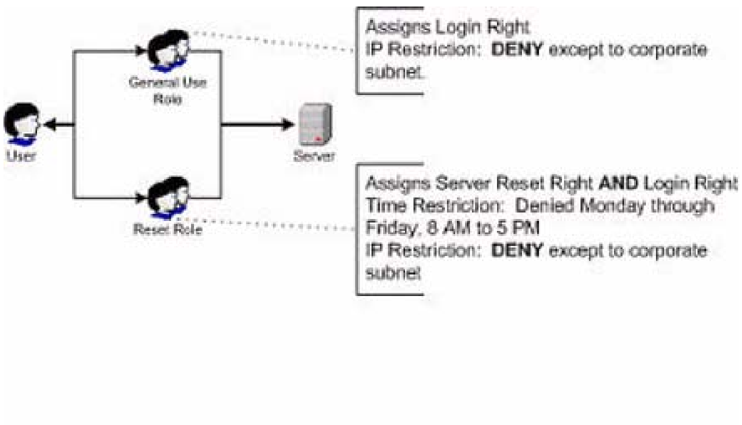
Figure 71 Restricting General Use


General Use Role
User
Server
Reset Role
Assigns Login Right
IP Restriction:
"DENY" except to corporate subnet.
Assigns Server Reset Right
Time Restriction: Denied Monday through Friday, 8 AM to 5 PM

Alternatively, the directory administrator could create a role that grants the login right and restrict it to the corporate network, create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration can create another role that grants users from addresses outside the corporate network the login right, which could unintentionally grant the iLO 2 administrators in the server reset role the ability to reset the server from anywhere, provided they satisfy the time constraints of that role.

The previous configuration satisfies corporate security policy. However, adding another role that grants the login right can inadvertently grant server reset privileges from outside the corporate subnet after hours. A more manageable solution would be to restrict the reset role, as well as the general use role.

Figure 72 Restricting the Reset Role


General Use Role
User
Server
Reset Role
Assigns Login Right
IP Restriction: DENY except to corporate subnet.
Assigns Server Reset Right AND Login Right
Time Restriction: Denied Monday through Friday, 8 AM to 5 PM
IP Restriction: DENY except to corporate subnet

Directory Services Schema (LDAP)

A directory schema specifies the types of objects that a directory can have and the mandatory and optional attributes of each object type. The following sections describe both the HP management core, and the LDAP object identifier classes and attributes that are specific to iLO 2.

HP Management Core LDAP Object Identifier Classes and Attributes

Object identifiers (OIDs) are unique numbers that are used by LDAP to identify object class, attribute, syntaxes (data types), matching rules, protocol mechanisms, controls, extended operation and supported features.

Changes made to the schema during the schema setup process include changes to the following:

- Core classes
- Core attributes

NOTE: Roles such as hpqTargets, and so on, are for extended schema LDAP only. They are not used in schema-free LDAP.

Core Classes

Table 80 lists the core LDAP OID classes.

Table 80 Core Classes

Class Name	Assigned OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Core Attributes

Table 81 lists the core LDAP OID attributes.

Table 81 Core Attributes

Attribute Name	Assigned OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core Class Definitions

Table 82, Table 83, and Table 84 define the HP management core classes.

hpqTarget

Table 82 hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Description	This class defines target objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	User
Attributes	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2
Remarks	None

hpqRole

Table 83 hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	This class defines role objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	Group
Attributes	hpqRoleIPRestrictions—1.3.6.1.4.1.232.1001.1.1.2.5hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Remarks	None

hpqPolicy

Table 84 hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	This class defines policy objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	Top
Attributes	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1
Remarks	None

Core Attribute Definitions

Table 85 through Table 90 define the HP management core class attributes.

hpqPolicyDN

Table 85 hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	This attribute provides the Distinguished Name of the policy that controls the general configuration of this target.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Single Valued
Remarks	None

hpqRoleMembership

Table 86 hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	This attribute provides a list of hpqTarget objects to which this object belongs.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Multi Valued
Remarks	None

hpqTargetMembership

Table 87 hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	This attribute provides a list of hpqTarget objects that belong to this object.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Multi Valued
Remarks	None

hpqRoleIPRestrictionDefault

Table 88 hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	This attribute is a Boolean expression representing access by unspecified clients, which partially specifies rights restrictions under an IP network address constraint.
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single Valued
Remarks	If this attribute is TRUE, IP restrictions are satisfied for unexceptional network clients. If this attribute is FALSE, IP restrictions are unsatisfied for unexceptional network clients.

hpqRoleIPRestrictions

Table 89 hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	This attribute provides a list of IP addresses, DNS names, domain, address ranges, and subnets, which partially specify right restrictions under an IP network address constraint.
Syntax	Octet String-1.3.6.1.4.1.1466.115.121.1.40
Options	Multi Valued
Remarks	This attribute is only used on role objects. The IP restrictions are satisfied when the address matches and general access is denied, and unsatisfied when the address matches and general access is allowed. Values are an identifier byte followed by a type-specific number of bytes specifying a network address. For IP subnets, the identifier is <0x01>, followed by the IP network address in network order, followed by the IP network subnet mask in network order. For example, the IP subnet 127.0.0.1/255.0.0.0 would be represented as <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. For IP ranges, the identifier is <0x02>, followed by the lower bound IP address, followed by the upper bound IP address. Both are inclusive and in network order. For example, the IP range 10.0.0.1 to 10.0.10.255 is represented as <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. For DNS names or domains, the identifier is <0x03>, followed by the ASCII encoded DNS name. DNS names can be prefixed with a * (ASCII 0x2A), to indicate they should match all names that end with the specified string. For example, the DNS domain *.acme.com is represented as <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. General access is allowed.

hpqRoleTimeRestriction

Table 90 hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	This attribute represents a 7-day time grid, with 30-minute resolution, which specifies rights restrictions under a time constraint.
Syntax	Octet String {42}-1.3.6.1.4.1.1466.115.121.1.40

Table 90 hpqRoleTimeRestriction *(continued)*

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Options	Single Valued
Remarks	This attribute is only used on role objects. Time restrictions are satisfied when the bit corresponding to the current local side real time of the device is 1, and unsatisfied when the bit is 0. The least significant bit of the first byte corresponds to Sunday, from 12 midnight, to Sunday 12:30 AM. Each more significant bit and sequential byte corresponds to the next consecutive half-hour blocks within the week. The most significant (8th) bit of the 42nd byte corresponds to Saturday at 11:30 PM, to Sunday at 12 midnight.

iLO 2-Specific LDAP OID Classes and Attributes

The schema attributes and classes in Table 91 and Table 92 might depend on attributes or classes defined in the HP management core classes and attributes.

iLO 2 Classes

Table 91 iLO 2 Classes

Class Name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

iLO 2 Attributes

Table 92 iLO 2 Attributes

Class Name	Assigned OID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

iLO 2 Class Definitions

hpqLOMv100

Table 93 hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	This class defines the rights and settings used with HP iLO 2 products.
Class Type	Auxiliary
SuperClasses	None
Attributes	hpqLOMRightConfigureSettings-1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin-1.3.6.1.4.1.232.1001.1. 8.2.2 hpqLOMRightLogin-1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole-1.3.6.1.4.1.232.1001.1.8.2.4 hpq LOMRightServerReset-1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia-1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

iLO 2 Attribute Definitions

Table 94 through Table 99 define the iLO 2 core class attributes.

hpqLOMRightLogin

Table 94 hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Login right for HP iLO 2 products.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single Valued
Remarks	The attribute is meaningful only on role objects. If TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

Table 95 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Remote console right for iLO 2 products. Meaningful only on role objects.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

Table 96 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Virtual media right for HP iLO 2 products.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightServerReset

Table 97 hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Remote server reset and power button right for HP iLO 2 products.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightLocalUserAdmin

Table 98 hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Local user database administration right for HP iLO 2 products.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightConfigureSettings

Table 99 hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Configure devices settings right for HP iLO 2 products.
Syntax	Boolean-1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

Glossary

A

Address In networking, a unique code that identifies a node in the network. Names such as **host1.hp.com** are translated to dott-quad addresses such as **168.124.3.4** by the Domain Name Service (DNS).

Address Path An address path is one in which each term has the appropriate intervening addressing association.

Administrator A person managing a system through interaction with management clients, transport clients, and other policies and procedures.

ARP Address Resolution Protocol. A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions: a server authenticates a client to make access control decisions, and the client can also authenticate the server. With Secure Sockets Layer (SSL), the client always authenticates the server.

Authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

B

Bind In the Lightweight Directory Access Protocol (LDAP), refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS Basic Input/Output System. System software that controls the loading of the operating system and testing of hardware when the system is powered on. The BIOS is stored in read-only memory (ROM).

BMC Baseboard Management Controller. A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) for which it provides an interface. The BMC also provides an interface to the SEL. Typical functions of the BMC are measuring processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.

C

CIM See Common Information Model.

Client A client is a logical component that manages a system through a manageability access point (MAP). A client can run on a management station or other system. A client is responsible for:

- Providing an interface to the functionality provided by the MAP in a form consistent with the SM architecture
- Accessing a MAP using one of the SM CLP architecture defined management protocol specifications. This involves interacting with the MAP through the following actions:
    - Initiating a session with a MAP
    - Transmitting protocol-specific messages to the MAP
    - Receiving protocol-specific output messages from the MAP

Command Line Interface (CLI) A text-based interface that enables users to enter executable instructions at a command prompt.

Command Line Protocol (CLP) The CLP defines the form and content of messages transmitted from and responses received by a client within the context of a text-based session between that client and the CLP service for a Manageability Access Point (MAP).

The CLP consists of a set of command verbs that manipulate command targets representing Managed Elements (ME) that are within the scope of access by a MAP. Each CLP interaction consists of a command line transmitted to the CLP service and a subsequent response transmitted back to the client. Each command transmitted generates only one response data transmission to the client.

The CLP allows for extensibility through different mechanisms: verbs, targets, target properties, and option names, and option arguments. The conventions allow for implementers to extend the interface in a non-conflicting mechanism that allows for differentiation and experimentation without encroaching upon the standard CLP syntax and semantics.

Common Information Model (CIM) An industry standard that was developed by the DMTF. CIM describes data about applications and devices so that administrators and software management programs can control applications and devices on different platforms in the same way, ensuring interoperability across a network.

CIM provides a common definition of management information for systems, components, networks, applications, and services, and it allows for vendor extensions. CIM common definitions enable vendors to exchange management information between systems.

Using techniques of object-oriented programming, CIM provides a consistent definition and structure of data, including expressions for elements such as object classes, properties, associations, and methods.

For example, if an enterprise purchases four different servers from four different vendors and networks them together, using CIM, the administrator can view the same information about each of the devices, such as manufacturer and serial number, the device's model number, its location on the network, its storage capacity, and its relationship to the applications that run throughout the network.

Console The interface between iLO 2 and the server that controls basic functionality. Also known as *host console*.

D

DDNS Dynamic Domain Name System. DDNS is how iLO 2 automatically registers its name with the Domain Name System so that when iLO 2 receives its new IP address from DHCP, users can connect to the new iLO 2 using the host name, rather than the new IP address.

DHCP Dynamic Host Configuration Protocol. A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network. Without DHCP, IP addresses must be entered manually at each computer, and when computers are moved to another location on another part of the network, a new IP address must be entered.

Directory Server In the Lightweight Directory Access Protocol (LDAP), a server which stores and provides information about people and resources within an organization from a logically centralized location.

Distinguished Name (DN) In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

DMTF Distributed Management Task Force. The industry organization that authors and promotes management standards and integration technology for enterprise and Internet environments to further the ability to remotely manage computer systems.

DNS Domain Name Server. The server that typically manages host names in a domain. DNS servers translate host names, such as **www.example.com**, into Internet Protocol (IP) addresses, such as **030.120.000.168**.

Domain Name Service. The data query service that searches domains until a specified host name is found.

Domain Name System. A distributed, name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as **00.120.000.168**, with host names, such as **www.hp.com**. Machines typically acquire this information from a DNS server.

Domain A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address.

Domain Name The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix. Domain names are interpreted from right to left.

E

Ethernet An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, which all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.

Event A change in the state of a managed object. The event-handling subsystem can provide a notification, to which a software system must respond when it occurs, but which the software did not solicit or control.

Extended Schema A platform-specific schema derived from the common model. An example is the Win32 schema.

F

Firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

FPGA Field Programmable Gate Array. A semiconductor device containing programmable logic components and programmable interconnects.

FTP File Transfer Protocol. A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.

G

Gateway A computer or program that interconnects two networks and passes data packets between the networks. A gateway has more than one network interface.

Gateway Address Where the packet needs to be sent. This can be the local network card or a gateway (router) on the local subnet.

GUI Graphical User Interface. An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

H

Host A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

Host Console The interface between iLO 2 and the server that controls basic functionality. Also known as *console*.

Host ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network. Host ID is also known as *DNS Name* or *Host Name*.

Host Name The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

HTTP Hypertext Transfer Protocol. The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server, and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

I

In-band System Management A server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

Integrated Lights-Out (iLO) The iLO functionality offers remote server management through an independent management processor (MP). iLO was introduced into most HP Integrity entry class servers in late 2004. Prior to that, embedded remote server management was referred to as *MP functionality*. All legacy MP functionality has been carried forward and combined with new features, all under the heading of "iLO". Therefore, "iLO" and "MP" mean the same thing for entry class servers.

IP Internet Protocol. IP specifies the format of packets and the packet addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. TCP/IP establishes a connection between two hosts so that they can send messages back and forth for a period of time. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255; for example, 1.160.10.240. Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates.

IP Address An identifier for a computer or device on a TCP/IP network.

IPMI Intelligent Platform Management Interface. A hardware-level interface specification designed primarily for the out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors, enabling a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes inventory reporting, system monitoring, logging, system recovery (including local and remote system resets, and power on and power off capabilities), and alerting.

K

Kernel The core of the operating system (OS) that manages the hardware and provides fundamental services that the hardware does not provide, such as filing and resource allocation.

KVM Switch Keyboard, Video, Mouse. A hardware device that allows a user, or multiple users, to control multiple computers from a single keyboard, video monitor and mouse.

L

LDAP Lightweight Directory Access Protocol. A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) across multiple platforms.

Lights-Out Advanced KVM card The HP Lights-Out Advanced KVM card is a PCI-X card that you install into any sx2000-based mid-range or high-end HP Integrity server such as rx7640, rx8640, and Superdome sx2000.

The Lights-Out Advanced KVM card enables the Lights-Out Advanced IRC and vMedia features of iLO 2.

The Lights-Out Advanced KVM card is also a KVM card that offers physical video functionality for servers running Windows, and USB functionality for servers running HP-UX, Windows, and OpenVMS.

M

Managed Object The actual item in the system environment that is accessed by the provider. For example, a Network Interface Card (NIC).

Management Information Base (MIB) The MIB defines the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each definition written in the MIB. MIB is not the actual database itself and is implementation dependant.

Management Processor (MP) The component that provides a LAN interface to the system console and system management. Prior to iLO 2, embedded remote server management was referred to as MP functionality. All legacy MP functionality has been carried forward and combined with new features, all under the heading of "iLO 2". Therefore, "iLO 2" and "MP" mean the same thing for entry class servers.

MAP Manageability Access Point. A network-accessible interface for managing a computer system. A MAP can be initiated by a management process, a management processor, a service processor, or a service process.

MAP Address Space This is the hierarchical graph of the UFiTs contained in the MAP's AdminDomain. Each instance starting at the AdminDomain is a node in the graph. Each supported association forms a link in the graph to another instance node, and so on, until a terminating instance node is encountered.

Media Access Control (MAC) Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture. In the Ethernet standard, every network connection must support a unique MAC value.

N

Network Interface Card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

Network mask A number used by software to separate a local subnet address from the rest of an Internet Protocol (IP) address.

Node An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

O

Onboard Administrator The Onboard Administrator (OA) is the enclosure management processor, subsystem, and firmware base used to support HP Integrity server blades and all the managed devices contained within the enclosure. The OA provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Utilizing this hard-wired information, the OA performs initial configuration steps for the enclosure, allows for run-time management and configuration of enclosure components, and informs administrators about problems within the enclosure through email, SNMP, or the Insight Display.

Options Used in the SMASH SM CLP. Options control verb behavior.

Out-of-band System Management Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

P

Port The location (socket) where Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

Port Number A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

POST Power-On Self-Test. The series of steps that the host system CPU performs following power-on. Steps include testing memory, initializing peripherals, and executing option ROMs. Following POST, the host ROM passes control to the installed operating system.

Properties Properties are attributes that are relevant to a target that are passed as parameters to the command. Property keywords map to properties of CIM class.

Protocol A set of rules that describes how systems or devices on a network exchange information.

Proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

R

Rackmount Electronic equipment and devices designed to fit industry-standard-sized computer racks and cabinets (19" wide). Rackmount devices are also standard 1.75 inch units.

Remote System A system other than the one on which the user is working.

S

Schema Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results. Schemas come in many forms, such as a text file, information in a repository, or diagrams.

Serial Console A terminal connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

Server Blade A single circuit board populated with components such as processors, memory, and network connections that are usually found on multiple boards.

SM CLP Server Management Command Line Protocol (SM CLP). SM CLP specification defines a user-friendly command line protocol to manipulate CIM instances defined by the SM profiles specification.

SMASH System Management Architecture for Server Hardware (SMASH). An initiative by the Distributed Management Task Force (DMTF) that encompasses specifications (SM CLP, SM ME Addressing, SM Profiles) that address the interoperable manageability requirements of small-to large-scale heterogeneous computer environments.

SNMP Simple Network Management Protocol. A set of protocols for managing complex networks.

SSH Secure Shell. A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.

SSL Secure Sockets Layer. A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

Subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

Subnet Mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long, and selects the network portion of the Internet address and one or more bits of the local portion. Also called an *address mask*.

System Event Log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

Target A target is the implicitly or explicitly identified managed element that a command is directed toward. Command targets specify managed elements in the system. Targets follow the SM addressing specification.

Target Address The target addressing scheme provides an easy-to-use method to accurately address CIM objects. The target address term of the CLP syntax in this architecture is extensible. The addressing scheme provides a unique target for CLP commands. The scheme is finite for parsing target names, and unique for unambiguous access to associated instance information needed to support association traversal rooted at the MAP AdminDomain instance.

Target Address Scheme Resolution Service This entity is responsible for discovering and enumerating the managed elements within the local domain, for maintaining the addressing and naming structure of the local domain, and coordinating this information with the operation invocation engine.

Telnet A telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system.

U

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 450 Mb/s (USB 2.0). A USB port connects devices such as mouse pointers, keyboards, and printers, to the computer system.

User The CLP User represents an instance of a client which transmits and receives CLP-compliant messages. The CLP is part of the SM CLP architecture. It is intended to either be a person or a script interacting with a terminal service such as Telnet or SSHv2.

User Account A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Friendly class Tag (UFcT) A short, user-friendly synonym for a CIM class name. It has the same properties and methods as the CIM class it represents.

User Friendly instance Path (UFiP) A unique path to an instance formed by concatenating the UFiTs of each instance from the root instance to the terminating instance. The intervening '/' between each UFiT represents an address association.

User Friendly instance Tag (UFiT) A unique instance tag within the scope of the target instance's containment class. A UFiT is created by adding an nonzero positive-integer suffix to the target instance's UFcT.

User Friendly Tag (UFT) A short, user-friendly tag for a CIM class name or instance. There are two types of UFTs; UFcT and UFiT.

User Name A combination of letters, and possibly numbers, that identifies a user to the system.

UTF-8 Unicode Transformation Format (8-bit). A variable-length character encoding for Unicode.

V

Verb Used with SMASH SM CLP. The verb selects a management action for a target.

vKVM Virtual keyboard, video, mouse. The iLO 2 graphical IRC provides virtual keyboard, video (monitor), and mouse (vKVM) capabilities with KVM-over-IP performance.

VPN Virtual private network. A network that is constructed using public wires (the Internet) to connect nodes. These systems use encryption and other security mechanisms to ensure only authorized users can access the network and that the data cannot be intercepted.

Index