HP Integrity Integrated Lights-out 2 Management Processor (iLO 2 MP) Operations Guide

HP Integrity BL860c, rx2660, rx3600, and rx6600

Table of Contents

List of Figures

List of Tables

About This Document

This document provides information and instructions on how to use the Integrity Integrated Lights Out 2 (iLO 2) Management Processor.

The document printing date and part number indicate the document's current edition. The printing date changes when a new edition is printed. Minor changes may be made at reprint without changing the printing date. 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.

The latest version of this document can be found on line at:

http://www.docs.hp.com

Intended Audience

This document is intended to provide technical product and support information for authorized service providers, system administrators, and HP support personnel.

This document is not a tutorial.

New and Changed Information in This Edition

This guide is being published in accordance with the release of the HP Integrity® BL860c, rx2660, rx3600, and rx6600 servers. The following updates were included in this guide:

- Added BL860c-specific information.
- Added Onboard Administrator information.

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. The updates will consist of a complete replacement manual and pertinent on-line or CD documentation.

Table 1 Publishing History Details

Document Manufacturing Part Number	Operating Systems Supported	Supported Product Versions	Publication Date
AD217-9001A	HPUX 11.23	BL860c	February 2007
	OpenVMS 8.3	rx2660	
	Microsoft Windows Server 2003	rx3600	
	Linux Red Hat & SuSE	rx6600	
AB419–9006A	HPUX 11.23	rx2660	December 2006
	OpenVMS 8.3	rx3600	
	Microsoft Windows Server 2003	rx6600	
	Linux Red Hat & SuSE		
5971–4292	HPUX 11.23	rx3600	September 2006
	OpenVMS 8.3	rx6600	
	Microsoft Windows Server 2003		
	Linux Red Hat & SuSE		

Document Organization

This guide is divided into the following chapters.

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

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

Chapter 3   *Console Connection and Setup* Use this chapter to set up the console.

Chapter 4   *Accessing the Host Console* Use this chapter to learn how to access the host console of an HP Integrity server through the iLO 2 MP.

Chapter 5   *Configuring DHCP, DNS, LDAP, and LDAP Lite* Use this chapter to configure DHCP, DNS, LDAP extended schema, and LDAP Lite default schema.

Chapter 6   *Text User Interface* Use this chapter to learn about the TUI command menu options from which commands can be executed in the iLO 2 MP.

Chapter 7   *Web Graphical User Interface* Use this chapter to learn how to use the Web GUI interface to interact with the iLO 2 MP.

Chapter 8   *SMASH Server Management Command Line Protocol* Use this chapter to learn about SMASH and SM CLP.

Chapter 9   *Directory Services Installation and Configuration* Use this chapter to learn about directory services functions, installation, and configuration.

Chapter 10   *Integrated Remote Console and vKVM* Use this chapter to learn about IRC usage and vKVM.

Chapter 11   *Virtual Media* Use this chapter to learn how to use the virtual media devices.

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

Typographic Conventions

This document uses the following conventions.

⚠ **WARNING!**   A warning lists requirements that you must meet to avoid personal injury.

⚠ **CAUTION:**   A caution provides information required to avoid losing data or avoid losing system functionality.

🗒 **IMPORTANT:**   Important messages provide essential information to explain a concept or to complete a task.

🗒 **NOTE:**   A note highlights useful information such as restrictions, recommendations, or important details about HP product features.

💡 **TIP:**   Tips provide you with helpful hints for completing a task. A tip is not used to give essential information, but can be used, for example, to provide an alternate method for completing the task that precedes it.

Book Title	The title of a book. On the Web and on the Instant Information CD, it may be a hot link to the book itself.
KeyCap	The name of a keyboard key or graphical interface item (such as buttons, tabs, and menu items). Note that **Return** and **Enter** both refer to the same key.
Emphasis	Text that is emphasized.
Bold	Text that is strongly emphasized.
Bold	The defined use of an important word or phrase.

ComputerOut	Text displayed by the computer.
UserInput	Commands and other text that you type.
Command	A command name or qualified command phrase.
Option	An available option.
Screen Output	Example of computer screen output.
[ ]	The contents are optional in formats and command descriptions. If the contents are a list separated by a pipe (|), you must select one of the items.
{ }	The contents are required in formats and command descriptions. If the contents are a list separated by a pipe (|), you must select one of the items.
...	The preceding element can be repeated an arbitrary number of times.
⊚	Separates items in a list of choices.

Related Documents

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

Web Site for HP Technical Documentation   http://www.docs.hp.com

Server Hardware Information   http://docs.hp.com/hpux/hw/

Windows Operating System Information   You can find information about administration of the Microsoft Windows operating system at the following Web sites, among others:
- http://www.docs.hp.com/windows_nt/
- http://www.microsoft.com/technet/

Diagnostics and Event Monitoring: Hardware Support Tools   Complete information about HP's hardware support tools, including online and offline diagnostics and event monitoring tools, is at the http://www.docs.hp.com/hpux/diag/ Web site. This site has manuals, tutorials, FAQs, and other reference material.

Web Site for HP Technical Support   http://us-support2.external.hp.com/

Books about HP-UX Published by Prentice Hall   The http://www.hp.com/hpbooks/ Web site lists the HP books that Prentice Hall currently publishes, such as HP-UX books including:
- *HP-UX 11i System Administration Handbook*
  http://www.hp.com/hpbooks/prentice/ptr_0130600814.html
- *HP-UX Virtual Partitions*
  http://www.hp.com/hpbooks/prentice/ptr_0130352128.html

HP Books are available worldwide through bookstores, online booksellers, and office and computer stores.

HP Encourages Your Comments

HP encourages your comments concerning this document. We are truly committed to providing documentation that meets your needs.

Send comments to:

netinfo_feedback@cup.hp.com

Include title, manufacturing part number, and any comments, errors found, or suggestions for improvement you have concerning this document. Also, please include what we did right so we can incorporate it into other documents.

1 Introduction

The Integrated Lights-Out Management Processor (iLO MP) for entry class 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. The iLO MP 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 over the years to describe the management functionality embedded in their 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 have been designed so all administrative functions that can be performed locally on the machine, 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.

iLO 2 refers to an Integrated Lights Out 2 Management Processor (iLO 2 MP) 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 chapter addresses the following topics:

Features

iLO 2 MP functionality includes:

- 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

The iLO 2 MP 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 iLO 2 MP LAN, and packets on the iLO 2 MP LAN cannot go to the operating system. The iLO 2 MP LAN is exclusive to the iLO 2 MP and is driven by an embedded real-time operating system (RTOS) running on the iLO 2 MP.

The iLO 2 MP offers the following standard and advanced features.

Standard Features

The iLO 2 MP 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

The iLO 2 MP is active and available through the iLO 2 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, the iLO 2 MP data is protected by an on-board battery backup.

Virtual Front Panel

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

Multiple Access Methods

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

The iLO 2 MP provides strong security for remote management in IT environments such as:

- User-defined TCP/IP ports
- User accounts and access management
- LDAP-based directory services authentication and authorization (requires Advanced Pack)
- Encrypted communication using SSL and SSH

User Access Control

The iLO 2 MP 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. The iLO 2 MP supports (LDAP) directory user authentication and locally stored iLO 2 MP user accounts. iLO 2 MP 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.
- iLO 2 MP Configuration Access: Right to configure all iLO 2 MP settings (as well as 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 the iLO 2 MP. However, iLO 2 MP 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 the iLO 2 MP can support multiple simultaneous connections, to do so can impact performance. HP does not recommend running more than eight simultaneous connections.

The iLO 2 MP supports the following connections simultaneously:

- 4 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)
- 8 SSH
- 1 local console serial port (RS-232)
- 4 IPMI over LAN
- 4 telnet
- 1 Integrated Remote Console (IRC)
- 1 vMedia

IPMI over LAN

The Intelligent Platform Management Interface (IPMI) option provides direct access from the iLO 2 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. The iLO 2 MP supports up to four simultaneous IPMI over LAN connections.

Updateable Firmware

Firmware upgrades of FPGA, EFI, PSOC, BMC firmware enhance the functionality of the iLO 2 MP.

Internal Subsystem Information

The iLO 2 MP displays information about internal subsystems:

- Field replaceable unit (FRU) information
- System power state and fan status
- Status of processors

DHCP and DNS Support

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

HPSIM

HP Systems Insight Manager Group Actions: HP Systems Insight Manager (HPSIM) is a system-level management tool that supports executing commands from HPSIM using the SSH interface. HPSIM enables the user to perform similar management activities across multiple iLO 2s (group actions) without requiring the user to access each iLO 2 MP individually. Group actions can be taken regardless of the server power state. You can find information about HPSIM at: **http://www.hp.com/go/hpsim**. You can find the user guide in the Information Library.

SNMP

The Simple Network Management Protocol (SNMP) is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suit developed to manage servers on an IP network. SNMP enables network administrators 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 (SM CLP, SM ME Addressing, SM Profiles) that address the interoperable manageability requirements of small to large-scale heterogeneous computer environments.

SM CLP

The Server Management CLP specification defines a user-friendly command line protocol that provides 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

The iLO 2 MP enables remote power cycle, power on or power off, and transfer of control (TOC). It also provides options to reset the system, the BMC, or iLO 2 MP.

Event Logging

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

Advanced Features

The iLO 2 MP 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 MP user administration with the Active Directory or eDirectory.

The advanced features require the iLO 2 MP Advanced Pack license. See "Advanced Pack License" (page 23).

IMPORTANT: On the BL860c server blade, an Advanced Pack license is bundled with the product. Although the license is bundled, the firmware does not automatically enable the advanced pack features. In order to enable the Advanced Pack features on the BL860c, you must enter the license key.

iLO 2 MP advanced features include the iLO 2 MP standard features as well as the following:

Virtual Media

Virtual Media (vMedia) enables connection of client-based USB CD/DVD devices and disk image files as virtual devices on the server and requires the virtual media right and the Java plug-in, version 1.4.2_10 and above.

Integrated Remote Console

The Integrated Remote Console (IRC) provides a remote console on Windows clients running the IE browser to Integrity-based Windows servers. It combines virtual keyboard, video, and mouse (vKVM).

Directory-based Secure Authorization Using LDAP

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

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

LDAP Lite

In Lightweight Directory Access Protocol Light (LDAP Lite) users are able to use directory authentication for logging in to the iLO 2 MP 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 MP schema-free integration provides:

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

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

In normal (for example, extended) LDAP implementation, if you want to use directory authentication for logging in to the iLO 2 MP , you have to extend the schema on the directory server itself and install directory snap-ins on client PCs. The advantage with LDAP Lite is you are spared the extra work involved in the extension of schema; and on the client's side, snap-ins need not be installed.

> **NOTE:** LDAP "Lite" and "Light" are used interchangeably.

Advanced Pack License

The iLO 2 MP Advanced Pack license features sophisticated virtual administration and security features for ultimate control of servers in the data centers and remote sites. With an iLO 2 MP Advanced license key, you can activate powerful remote management features to install, configure, monitor, update, and troubleshoot remote HP servers anywhere, anytime from a standard Web browser, command line or script.

> **IMPORTANT:** On the BL860c server blade, an Advanced Pack license is bundled with the product. Although the license is bundled, the firmware does not automatically enable the advanced pack features. In order to enable the advanced pack features on the BL860c, you must enter the license key.

Obtaining and Activating iLO 2 MP Advanced Pack Licensing (AB500A)

A free 30-day evaluation license is available for download on the HP Web site. The evaluation license activates and accesses iLO 2 MP Advanced Pack license features. You can only install one evaluation license per iLO 2. After the evaluation period, an iLO 2 MP Advanced Pack license is required to continue using the advanced features. The iLO 2 MP Advanced Pack license features automatically deactivate when the evaluation license key expires.

For more information, see the HP Web site 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.

Requirements for the iLO 2 MP Advance Pack License

To utilize iLO 2 MP Advanced Pack license features, you must have the minimum required iLO 2 MP firmware version for your server.

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

Supported Systems and Required Components and Cables

There are several ways to connect to the iLO 2 MP.

Table 1-1 lists the systems on which the iLO 2 MP is supported and the components and cables that are required to operate the iLO 2 MP.

Table 1-1 Supported Systems and Required Components Matrix

Supported Systems	Required Components	Required Cables[1]
BL860c	Front RS-232 console serial port	SUV or DB9 cable
	Rear OA/iLO network port	LAN cable
rx2660	iLO 2 MP hardware is integrated into the system board	LAN, serial, and VGA cable
rx3600 and rx6600	Core IO board without VGA; factory installed	LAN and serial cable
	Core IO board with VGA (optional) (This is only supported on Windows OS.)	LAN, serial, and VGA cable

1 Cables are not provided with the server

iLO 2 MP Supported Browsers and Operating Systems

The iLO 2 MP has an independent microprocessor. The architecture ensures that the majority of iLO 2 MP functionality is available, regardless of the host operating system.

Table 1-2 lists the operating systems and browsers that are supported on the server:

Table 1-2 iLO 2 MP Supported Browsers and Operating Systems

Browsers	Operating System					
Java Plug-in 1.4.2_10	HPUX	Windows		Linux		VMS
	11.23	WS 2003 Enterprise	XP	Red Hat Enterprise	SuSE	8.3
Mozilla 1.7.12.01.00	X					
Mozilla 1.7.13		X	X	X	X	
Internet Explorer 6.0		X	X			
HP Secure Web Browser 1.7.13		X	X			X

Security

It is important to have strong security surrounding the iLO 2 MP device. HP carefully considered security requirements of the enterprise and architected the iLO 2 MP to include:

- Authentication: iLO 2 MP incorporates authentication techniques with the use of 128-bit SSL (Secure Socket Layer) encryption; it is password-based for Web and password and key-based for SSH.
- Authorization: Using local accounts, iLO 2 MP offers administrators the ability to define up to 19 separate users and to vary the server access rights of each user. The directory services capabilities of iLO 2 MP enables administrators to maintain network user accounts and security policies in a central, scalable database that supports thousands of users, devices, and management roles.
- Integrity: iLO 2 MP incorporates a trusted Java™ applet for virtual media.
- Privacy: iLO 2 MP uses SSL for Web connections, RSL-RC4 encryption for integrated remote console and remote serial console, and SSH-DES3/DES128 2.0 recommended encryption algorithms for SSH-based connections. You can enable or disable telnet, IPMI over LAN, Web, and SSH connectivity.
- Login feature: 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.

Because iLO 2 MP devices are completely autonomous and can be used to control the server, they should be treated in the same manner as other servers. For example, the administrator should include the iLO 2 MP devices in the security and network audits.

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

Protect SNMP Traffic

Because SNMP uses passwords, known as community strings, that are sent across the network in clear text, it is important to enhance the network security when using SNMP traffic. Suggestions for enhancing network security are as follows:

- 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, an administrator can allow inbound SNMP traffic into the host server only if it comes from one of the predetermined management workstations.

Telnet Security

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.

Help System

The iLO 2 MP has a robust help system.

Accessing Help Using the TUI

To access the **Help** menu if you are using the TUI, enter **HE** at the `MP>` prompt. 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,** type `Q`.

Accessing Help Using the Web GUI

To access the help screens if you are using the Web GUI, click the **Help** tab to launch iLO 2 MP help. You can also click the `?` at the top right corner of each page to display help about the page you are on.

2 Ports and LEDs

All iLO 2 MP functions are available through the server iLO 2 MP LAN and the local and remote serial ports; and the Onboard Administrator on the BL860c. This chapter describes the available iLO 2 MP ports, connectors, and LEDs on the HP Integrity BL860c server blade, and the rx2660, rx3600, and rx6600 servers.

This chapter addresses the following topics:

- "HP Integrity BL860c Server Blade Components" (page 27)
- "HP Integrity rx2660 Server Components" (page 30)
- "HP Integrity rx3600 and rx6600 Server Components" (page 30)
- "iLO 2 MP Reset Button" (page 32)
- "Console Serial Port (RS-232) and Auxiliary Serial Port" (page 32)

HP Integrity BL860c Server Blade Components

Onboard Administrator is the enclosure management processor, subsystem, and firmware base used to support the HP BladeSystem BL860c and all the managed devices contained within the enclosure. Onboard Administrator provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Utilizing this hardwired knowledge, Onboard Administrator performs initial configuration steps for the enclosure, allows for run-time management and configuration of the enclosure components, and informs you of problems within the enclosure through email, SNMP, or the Insight Display.

Before moving on to HP BladeSystem Onboard Administrator setup, HP recommends that you read the *HP BladeSystem Onboard Administrator User Guide* on the Web 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 Onboard Administrator and that you properly complete the initial setup to facilitate proper functioning of the Onboard Administrator.

The *HP BladeSystem Onboard Administrator User Guide* provides the following information in detail:

- Access Requirements
- Running Onboard Administrator for the first time
- Signing in to the Onboard Administrator GUI
- Running the setup wizard
- Using online help
- Changing enclosure and device configurations
- Recovering the administrator password
- Flash disaster recovery

You can find other Onboard Administrator docs, on the Web at:

HP BladeSystem c-Class Onboard Administrator

HP Integrity BL860c Front Panel

Figure 2-1 shows the BL860c front panel components.

Figure 2-1 HP Integrity BL860c Front Panel
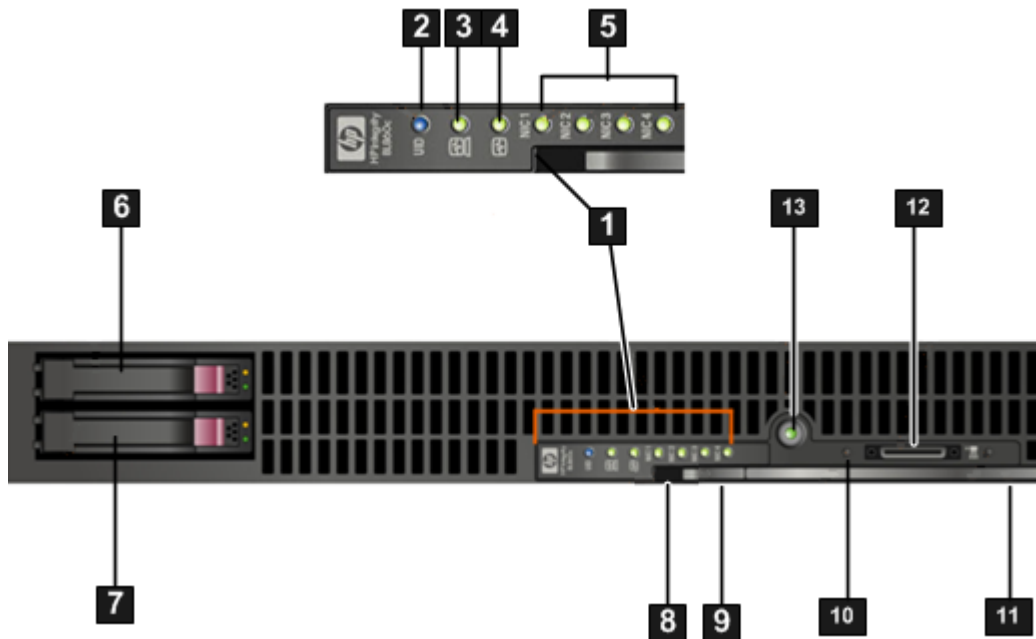
1   Front Panel LEDs

The server blade contains seven LEDs on the front panel that indicate the server blade status.

2   Unit Identification (UID)

3   System Event Health LED

4   Internal Health LED

5   NIC LEDs 1, 2, 3, 4

6   Hot-plug SAS Drive Bay 1

7   Hot-plug SAS Drive Bay 2

8   Pull Tab

The front panel of the Integrity BL860c server blade features the standard components called out above as well as a new pull tab. When you pull on this tab, it rotates out showing the server blade's model number, product number, serial number, UUID, and the default Integrity iLO 2 MP settings for user name, DNS name, and password.

9   Server Blade Release Button

Use the server blade release button to unlock the extraction handle and remove the server blade from the enclosure.

10   MP (iLO) Reset Button

Use the**MP (iLO) Reset** button to perform a hard reset of the MP to set the MP to the default shipping settings.

11   Server Blade Handle

Use the handle to pull the server blade out from the enclosure.

12   SUV Cable Port

The SUV cable port is used for server blade configuration and diagnostic procedures.

The Integrity BL860c has the addition of a video port to its SUV cable.

13   Power On / Standby Button

Setting the server blade power button to standby power removes power from most areas of the server blade. This process takes about 30 seconds, and some internal circuitry remains active.

Onboard Administrator Components

Figure 2-2 shows the Onboard Administrator OA/iLO network port and components.

Figure 2-2 OA/iLO Network Port and Components
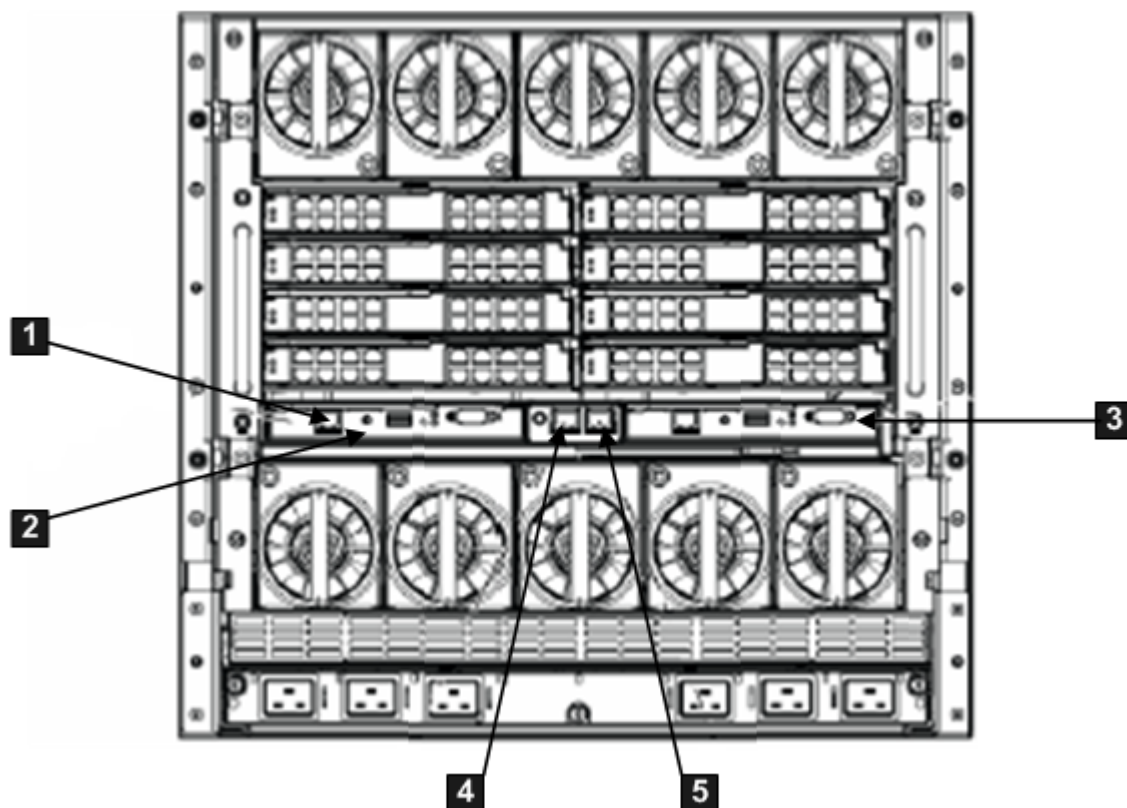
1	OA/iLO Network Port	**4**	Enclosure Link-up Port
2	Onboard Administrator Bay 1	**5**	Enclosure Link-down Port
3	Onboard Administrator Bay 2 (redundant if used)		

Figure 2-3 shows the Onboard Administrator LEDs and buttons.

Figure 2-3 Onboard Administrator LEDs and Buttons
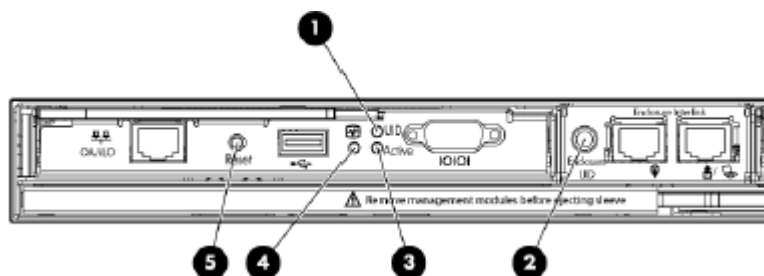
1	Onboard Administrator UID LED	**4**	Onboard Administrator Health LED
2	Enclosure UID LED	**5**	Onboard Administrator Reset Button
3	Onboard Administrator Active LED		

HP Integrity rx2660 Server Components

Figure 2-4 shows the controls, ports, and LEDs on the rear of the HP Integrity rx2660 server.

Figure 2-4 HP Integrity rx2660 Server Rear Ports and LEDs
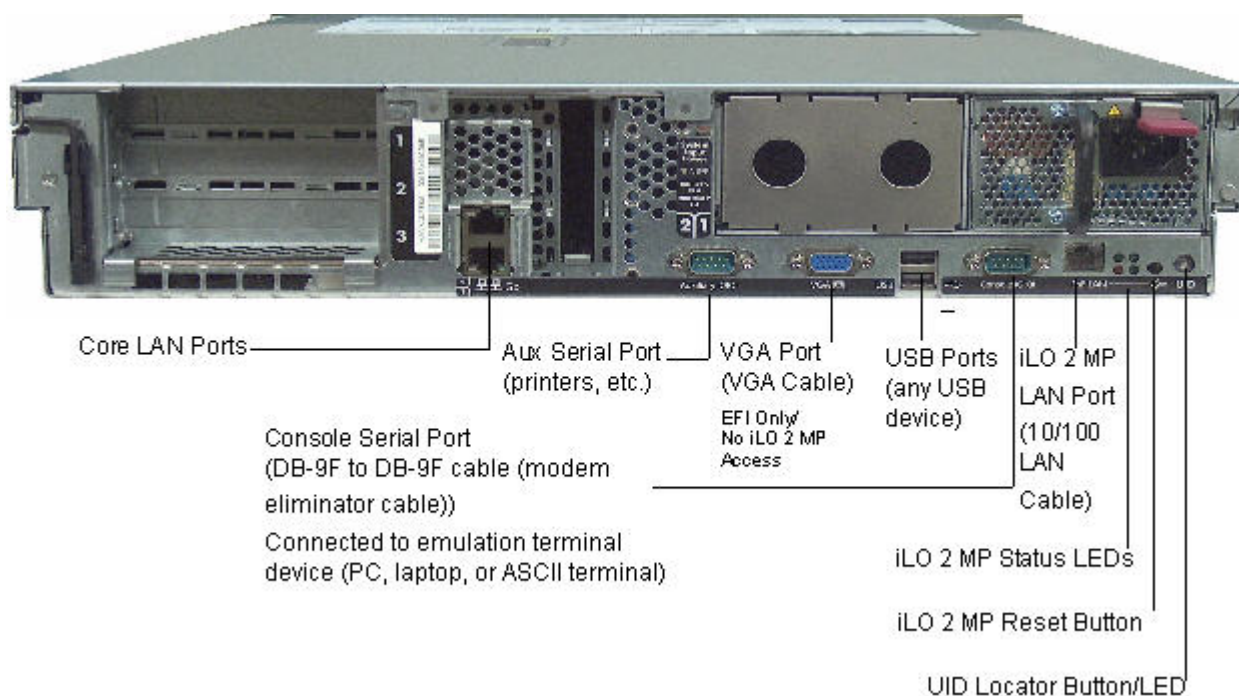
HP Integrity rx2660 System Board Ports

Table 2-1 lists a description of the system board LAN ports shown in Figure 2-4. The system LAN functionality is integrated into the system board.

Table 2-1 HP Integrity rx2660 System Board LAN Ports

Port	Description
Two – RJ–45 style 10 Base-T/100 Base-T/1000 Base-T system LAN	LAN ports dedicated for remote access to the iLO 2 MP.
Auxiliary serial	Local serial port.
Console serial (iLO 2 MP)	Local serial port that provides a console connection to the server.
USB	Two public USB 2.0 ports used primarily to connect to a keyboard and mouse for console input functions (Windows and Linux operating systems only).
VGA	VGA port used primarily to connect to a monitor that displays console output (Windows and Linux operating systems only).

HP Integrity rx3600 and rx6600 Server Components

Figure 2-5 shows the controls, ports, and LEDs on the rear of the HP Integrity rx3600 and rx6600 servers.

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

Figure 2-5 HP Integrity rx3600 and rx6600 Server Rear Ports and LEDs
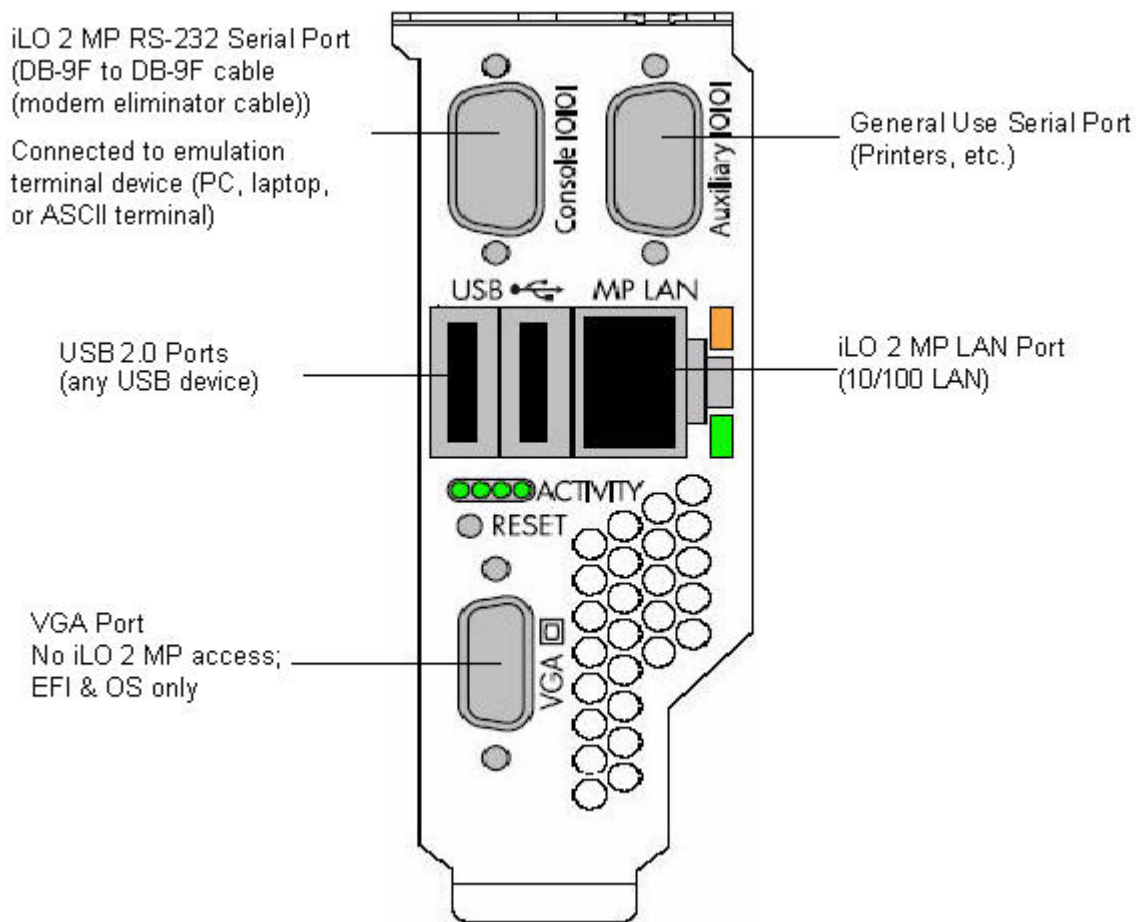
HP Integrity rx3600 and rx6600 Core I/O Board Ports

Table 2-2 lists a description of the core I/O board ports shown in Figure 2-5.

Table 2-2 HP Integrity rx3600 and rx6600 Core I/O Board Ports

Port	Description
10 Base-T/100 Base-T LAN	LAN port dedicated for remote access to the iLO 2 MP.
Auxiliary serial	Local serial port.
Console serial (iLO 2 MP)	Local serial port that provides a console connection to the server.
USB	Two public USB 2.0 ports used primarily to connect to a keyboard and mouse for console input functions (Windows and Linux operating systems only).
VGA (optional)	VGA port used primarily to connect to a monitor that displays console output (Windows and Linux operating systems only).

iLO 2 MP Status LEDs

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

Table 2-3 iLO 2 MP Status LEDs

iLO 2 MP Status LED	LED State
Standby power	Solid green.
iLO 2 MP selftest	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 selftest; the LED then 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 the iLO 2 MP, and reset the user-specific values to factory default values. A momentary press causes a soft reset of the iLO 2 MP when the button is released. A greater than four second press causes a soft reset of the iLO 2 MP 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 MP user passwords have been lost, or iLO 2 MP local user accounts have been 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 rest local user accounts and passwords to their default values.

To reset local user accounts and passwords to default values, follow these steps:

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

Console Serial Port (RS-232) and Auxiliary Serial Port

Figure 2-6 shows the console serial port connector with numbered labels for each pin on each port.

Figure 2-6 Console Serial Port (RS-232) Connector
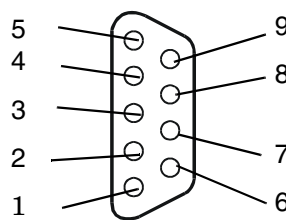
Table 2-4 maps the console serial port connector pin number to its signal description on each port.

Table 2-4 Console Serial Port Pinouts

Pin Number	Signal Description
1	Not applicable
2	Receive data
3	Transmit data

Table 2-4 Console Serial Port Pinouts *(continued)*

Pin Number	Signal Description
4	Not applicable
5	Ground
6	Not applicable
7	Request to send
8	Clear to send
9	Not applicable

iLO 2 MP LAN Port

Figure 2-7 shows the iLO 2 MP LAN port connector pins and LEDs.

Figure 2-7 iLO 2 MP LAN Port
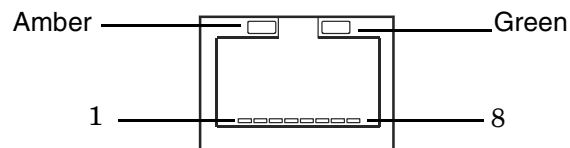
Table 2-5 maps the iLO 2 MP LAN port connector pin number to its signal description.

Table 2-5 iLO 2 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

iLO 2 MP LAN LEDs

Table 2-6 lists the iLO 2 MP LAN link status LEDs and states.

Table 2-6 iLO 2 MP LAN Link Status LEDs

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

Table 2-7 lists the iLO 2 MP LAN link speed LEDs and states.

Table 2-7 iLO 2 MP LAN Link Speed LEDs

Link Speed	LED State
100Mb	Solid amber
10Mb	Off

3 Console Connection and Setup

Setting up the console involves the following:

1. Determining the physical access method to connect cables. There are two physical connections to the Integrity iLO 2 MP:
   - Console serial port (RS-232)
   - iLO 2 MP LAN port

2. Configuring the Integrity iLO 2 MP and assigning an IP address if necessary. Though there are several methods to configuring the LAN, DHCP with DNS is the preferred one. DHCP with DNS comes preconfigured with default factory settings, including a default user account and password. Other options include:
   - ARP-Ping
   - Console serial port (RS-232)

This chapter addresses the following topics:

Setup Checklist

Use the checklist in Table 3-1 to assist you with the Integrity iLO 2 MP setup process.

Table 3-1 Setup Checklist

Step		Action	X
Standard and Advanced			
1	Preparation	1. Determine access method to select and connect cables. 2. Determine LAN configuration method and assign IP address if necessary.	
2	Configure the iLO 2 MP LAN	There are three methods to configure the LAN for iLO 2 MP access: • DHCP with DNS • ARP Ping • Console serial port (RS-232)	
3	Log on to the iLO 2 MP	Log in to the iLO 2 MP from a supported Web browser or command line using the default user name and password.	
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 using the local accounts feature.	
6	Set up security access	Set up the security access settings.	
6	Access the host console	Access the host console using method of choice.	

Table 3-1 Setup Checklist *(continued)*

Step	Action	X
Advanced		
Activate Advanced Pack Features	Activate advanced features by entering a license key.	

Setup Flowchart

Use this console setup flowchart as a guide to assist in the Integrity iLO 2 MP setup process.

Figure 3-1 Setup Flowchart
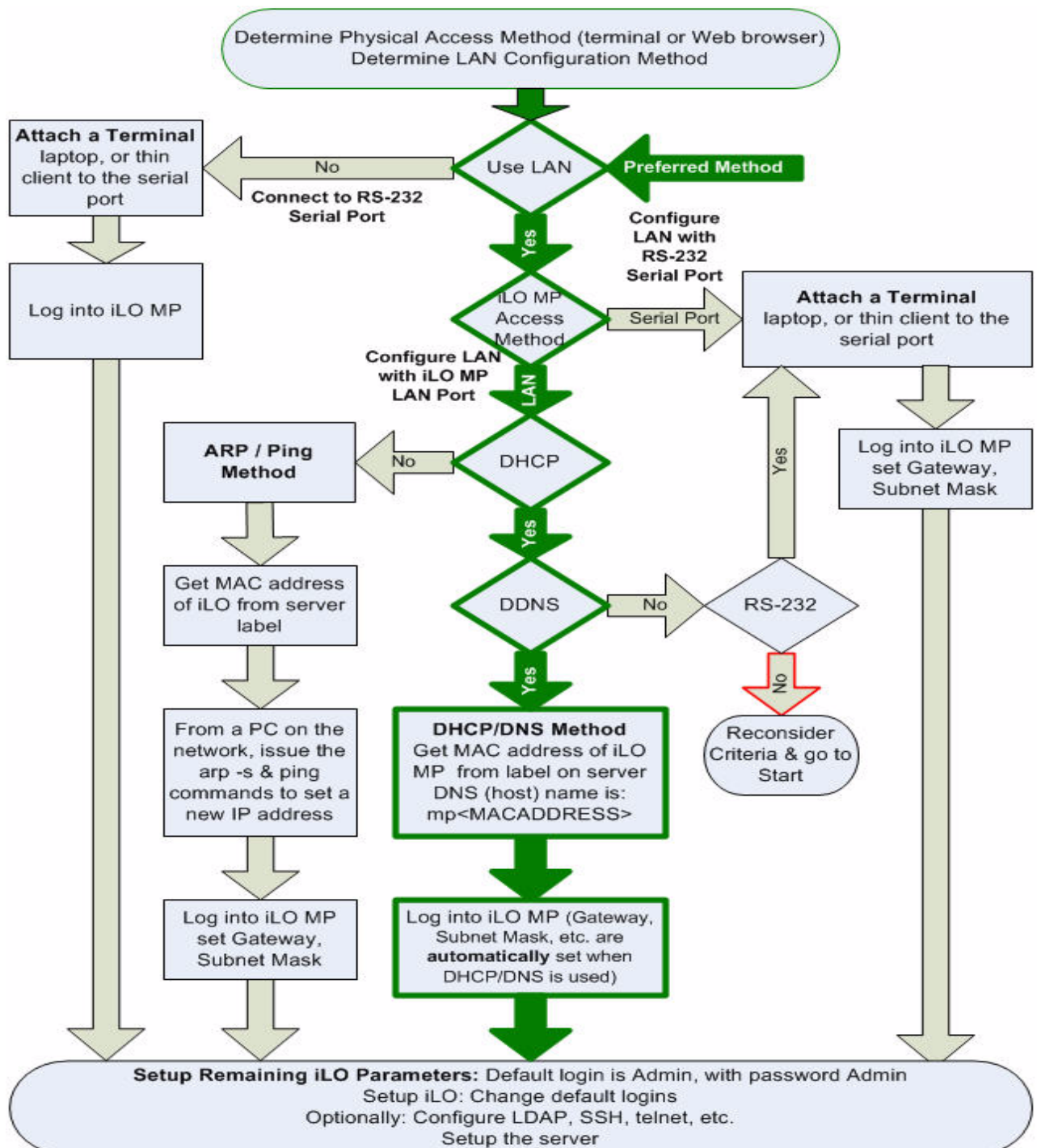
Preparation

There are several tasks to perform before you can 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.

Determining the Physical iLO 2 MP Access Method

Before you can access the iLO 2 MP, you must first determine the correct physical connection method. The iLO 2 MP 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 port used by the operating system. See Figure 2-4 and Figure 2-5 (page 31) and use Table 3-2 to determine your physical connection method.

Table 3-2 lists the appropriate connection method, required connection components, and connectors to the host console.

Table 3-2 Physical Connection Matrix

Connection Method	Required Connection Components
Console serial port (RS-232)	1. Host console 2. Console serial port (RS-232) DB-9F to DB-9F cable (modem eliminator cable) 3. Emulation terminal device (for example, a PC, laptop, or ASCII terminal)
LAN port	10/100 LAN cable

Determining the iLO 2 MP LAN Configuration Method

To access the iLO 2 MP through the iLO 2 MP LAN, the iLO 2 MP must acquire an IP address. The way the iLO 2 MP 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 3-3 for possible scenarios.)

Once you have determined the iLO 2 MP access, you must determine how you will configure the iLO 2 MP LAN in order to acquire an IP address. There are three methods available.
- DHCP/DNS
- ARP Ping
- Console serial port (RS-232)

Table 3-3 provides all the possible scenarios to consider. Use this table to help you select the appropriate LAN configuration method to obtain an IP address.

Table 3-3 LAN Configuration Methods

DHCP	DNS	Console Serial Port (RS-232) MP (LC command)	LAN Configuration Method
Yes	Yes	No	DHCP
Yes	Yes	Yes	DHCP or console serial port (RS-232)
No	No	No	ARP Ping
No	Yes	No	ARP Ping
No	Yes	Yes	ARP Ping or RS-232
Yes	No	Yes	Console serial port (RS-232)
No	No	Yes	Console serial port (RS-232) or ARP Ping
Yes	No	No	Cannot set up the LAN. Reconsider your criteria.

Once you have determined how you will configure the iLO 2 MP LAN in order to acquire an IP address, you must configure the iLO 2 MP LAN using the selected method.

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 the iLO 2 MP are shipped from the factory with DHCP enabled.

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

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.

When you use DHCP and DNS, you can connect to the iLO 2 MP by typing the default host 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 has been configured through the DHCP server.

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

To configure the iLO 2 MP using DHCP and DNS, follow these steps:

1. Obtain the factory-set host name from the iLO 2 MP Media Access Protocol (MAC) address label on the server. The default host name is 14 characters long, consisting of the letters **mp** followed by the 12 characters of the MAC address.

   MAC address 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.

   IMPORTANT: Make sure you obtain the MAC address to the system board and not the MAC address to the server core LAN card.

2. Connect the iLO 2 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 default host name. The default host name is the letters **mp** followed by the 12 characters of the MAC address. The **iLO 2 MP Log In** window opens.
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 the iLO 2 MP until you change the default user name and password.

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

Configuring the iLO 2 MP LAN Using ARP Ping

📝 **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 the iLO 2 MP which will negate the DHCP/DDNS 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, or subnet, as the computer 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.

📝 **NOTE:** ARP Ping 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 for three minutes after the iLO 2 MP is booted. This applies to every subsequent boot of the iLO 2 MP until an IP address is obtained by DHCP or has been assigned by using the LC command.
- Upon successfully assigning an IP address using ARP Ping, DHCP is automatically disabled.

There are two 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 3-4 lists the ARP Ping commands.

Table 3-4 ARP Ping Commands

ARP Command	Description
arp -s	This command assign 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	This command tests network connections. It verifies the iLO 2 MP LAN port is configured with the appropriate IP address.

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, follow these steps:

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 iLO 2 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.

   Syntax

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

   Example from Windows

   arp -s 192.0.2.1 00-00-0c-07-ac-00

6. At the DOS command prompt, enter **ping** followed by the IP address to verify that the iLO 2 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.

   Syntax

   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 the iLO 2 MP from a host on the local subnet and complete the rest of the LAN parameter (gateway, subnet).

Configuring the iLO 2 MP LAN Using the Console Serial Port (RS-232)

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

> **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 an 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 and use the LC command.

To assign a static IP address using the LC command, follow these steps:

1. Ensure the emulation software device is properly configured. 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 ensure the emulation software is correctly configured, follow these steps:
   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. Supported terminal types are:
      - hpterm
      - vt100
      - vt100+
      - vt-utf8

   IMPORTANT: Do not mix hpterm and vt100 terminal types at the same time.

   There are many different emulation software applications. Consult the help section of the emulation software application for instructions on how to configure the software options.

2. Use Table 3-2 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 the iLO 2 MP. See "Logging In to the iLO 2 MP" (page 41).
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. You may need the information for future troubleshooting.
8. Use the `LC` command to disable DHCP.
   a. From the `LC` command menu, type `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 the iLO 2 MP.
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 the iLO 2 MP.
11. After the iLO 2 MP resets, log in to the iLO 2 MP again and enter `CM` at the `MP>` prompt.
12. Enter `LS` to confirm that DHCP is disabled and display a list of updated LAN configuration settings.

Logging In to the iLO 2 MP

To log in to the iLO 2 MP, follow these steps:

1. Access the iLO 2 MP using the LAN, console serial port (RS-232), telnet, SSH, or Web method. The iLO 2 MP login prompt displays.
2. Log in using the default the iLO 2 MP 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 Password" (page 45).

Following is the **MP Main Menu**:

```
iLO 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 Chapter 6: "Text User Interface" (page 57) for information on the iLO 2 MP menus and commands.

When logging in using the local or remote RS-232 console serial ports, the login prompt may not display if another user is logged in through these ports. Use **Ctrl-B** to access the **MP Main Menu** and the MP> prompt.

Physically Connecting the BL860c to the iLO 2 MP

There are two methods you can use to connect to the iLO 2 MP.

- Connecting to the iLO 2 MP with DHCP Enabled. Use the Onboard Administrator iLO (OA/iLO) network port on the rear of the enclosure. If the OA /iLO network port on the enclosure is connected to the local nework 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.
- Connecting to the iLO 2 MP with No Network Connection. Use the RS-232 port on the SUV cable. If the enclosure is not connected to any network, you must configure your server through the RS-232 serial console port 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 the iLO 2 MP. The USB provides keyboard and mouse to the operating system on the Integrity BL860c. 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 Integrity BL860c. In addition, there is no LAN (Ethernet connection) to the front of the server blade.

Connecting the BL860c to the iLO 2 MP 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.

To connect to the iLO 2 MP using the Onboard Administrator, follow these steps:

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 press **OK**.

4. Select the appropriate server blade from the options on the screen and press **OK**. The screen displays the iLO 2MP IP address.

5. Write down the iLO 2 MP IP address and access the iLO 2 MP through telnet, SSH, or the Web using the assigned DHCP iLO 2 MP IP address.

NOTE: For the BL860c server blade, you can use the Onboard Administrator to set the IP addresses for all the iLO 2 MPs. You can also find the iLO 2 MP address so you can log in.

Connecting the BL860c to the iLO 2 MP Using the RS-232 Serial Console Port

If the enclosure is not connected to any network, you must configure your server through the RS-232 serial console port on the SUV cable. Use this procedure to configure the RS-232 port to enable iLO 2 MP 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 Integrity BL860c you have access to two serial ports through the RS-232 connector. The default setting is for the iLO 2 MP interface, the other is for an AUX UART that is directly connected to the host operating system and can be used for any serial device (terminal, debug port, etc.) The AUX UART is recommended for server blade setup or debug purposes only.

In most situations you can use a command to toggle between the two ports. However, if access to the iLO 2 MP UI is not possible through telnet and if the port mode of operation is set to the AUX UART, perform a hard reset of the iLO 2 MP to set it to the default shipping settings by pushing the recessed **MP (iLO) Reset** button.

TIP: It is not necessary to physically connect to the iLO 2 MP through the RS-232 serial console port to perform any management task. The intention is that you should use the OA/iLO 2 LAN port to communicate with any iLO 2 MP in the enclosure, as well as the Onboard Administrator. You can use the LCD panel and the Onboard Administrator to configure and determine the iLO 2 MP LAN address.

Connecting the SUV Cable to the BL860c

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

CAUTION: Disconnect the SUV cable from the port when not in use. The port and connector are not intended to provide a permanent connection.

On the SUV cable, locking buttons are located on the sides of the server blade connector. Always be sure to 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, and it will need to be replaced.

To establish a connection from the server blade to the terminal emulator, follow these steps:

1. Insert the SUV cable into the SUV port on the rear of the server blade. See Figure 3-2 and Figure 3-3

2. Connect a standard DB9f to DB9f modem eliminator cable to the RS-232 port on the SUV cable.

3. Connect the other end of the DB9f to DB9f modem eliminator cable to the terminal emulator.

4. Verify the parameters for RS-232 serial 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. Click **OK** to set the parameters.
6. If running an emulator, launch it now.

Figure 3-2 SUV Cable

1	Server Blade Connector	**5**	USB
2	2–port USB		Label
3	VGA	**6**	USB-1
	The VGA connection provides no access to the iLO 2 MP	**7**	USB-0
4	9–pin RS-232 Port		

Figure 3-3 Connecting the SUV Cable to the Server Blade

Additional Setup

This section provides additional information to setup the iLO 2 MP.

Modifying User Accounts and Default Password

The iLO 2 MP 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 MP user interfaces.

To modify default account configuration settings, follow these steps:

1. Log in as the administrator. You must log in as the administrator in order 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 setup 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 generally recommends that iLO 2 MP management traffic be on a separate dedicated management network 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 administrators to physically control which workstations are connected to the network.

HP also strongly recommends you modify the default settings during the initial logon session and determine the security access required and what user accounts and privileges are needed. Create local accounts or use directory services to control user access. See "Modifying User Accounts and Default Password" (page 45).

Security Access Settings

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

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

⚠ **CAUTION:** When DHCP is enabled, the system is vulnerable to security risks because anyone can access the iLO 2 MP 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 MP access. This is ideal for small environments such as labs and small-to-medium sized businesses.
- Use directory services. Use the corporate directory to manage iLO 2 MP 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.

📝 **NOTE:** See Chapter 9: "Directory Services Installation and Configuration" (page 137) for more information on how to create local accounts and use directory services.

---

4 Accessing the Host Console

There are several ways to access the host console of an HP Integrity server.

This chapter addresses the following topics:

Accessing the iLO 2 MP With the Web Browser

Web browser access is an embedded feature of the iLO 2 MP.

The iLO 2 MP 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 port used by the operating system.

IMPORTANT: Make sure you use the MAC address to the iLO 2 MP LAN and not the MAC address to the server core LAN. The iLO 2 MP MAC address is located on a label on the server.

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

- IP address for the iLO 2 MP LAN
- Host name (this is used when messages are logged or printed)

To interact with the iLO 2 MP through the Web GUI, follow these steps:

1. Open a Web browser and enter the host 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 4-1).

Figure 4-1 Web Login Page

NOTE: The iLO 2 MP Web interface session has a five minute timeout 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 4-2) displays after login.

Figure 4-2 Status Summary Page
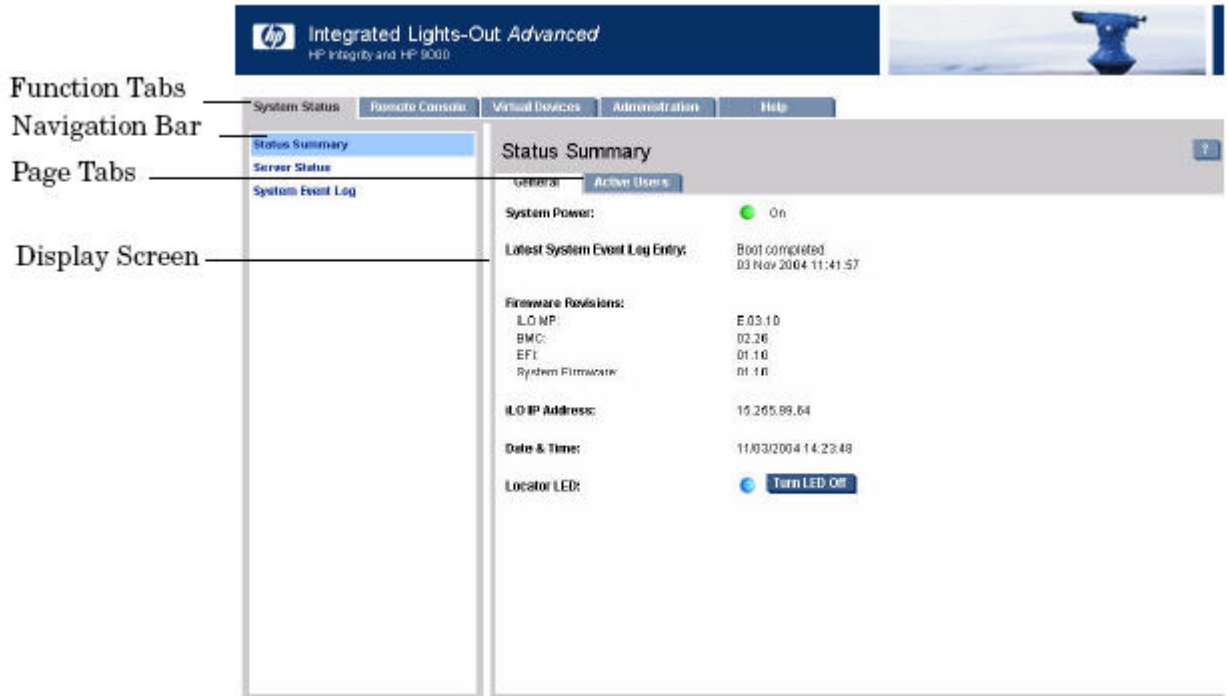
1. Select the Web interface functions by clicking the **Function** tabs at the top of the page. Each function lists options in the **Navigation Bar** on the left side of the page.
2. Click an option link to display data in the **Display** screen; and click **Refresh** to update the display.
3. Click the **Remote Console** tab. The remote console provides the following options to access the console:
   • A serial console that behaves similarly to the TUI of the following section
   • The virtual KVM console

Help

The iLO 2 MP Web interface has a robust help system. To launch iLO 2 MP help, click the **Help** tab in the **Display** screen or click the **?** at the top right corner of each page to display help about that page.

Accessing the Host Console With the TUI - CO Command

This section provides the steps to access the host console using the text user interface (TUI).

To access the host console through the iLO 2 MP, follow these steps:

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

Accessing the Host Console With vKVM - 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 177).

Accessing the 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 114).

Accessing iLO 2 MP Using Onboard Administrator

NOTE: The HP BladeSystem Onboard Administrator is only available on the HP Integrity BL860c server blade.

To access the iLO 2 MP using the onboard administrator, follow these steps:

1. Establish a network connection through the OA/iLO network port.
2. Enter the iLO MP IP address you obtained previously through the OA/iLO port in the appropriate screen. You now have access to the iLO 2 MP functionality through the telnet session.
3. Ensure you have an MP prompt.

To log into the iLO 2 MP, enter the following default values for the login ID and password (case sensitive):

- Login: **Admin**
- Password: **Admin**

The **MP Main Menu** screen displays.

Accessing the Graphic Console Using VGA

VGA is a method you can use to access the graphic console.

NOTE: You cannot access the iLO 2 MP using VGA.

This method requires three elements:

- Monitor (VGA connector)
- Keyboard (USB connector)
- Mouse (USB connector)

The graphic console output displays on the monitor screen.

IMPORTANT: The server console output does not display on the console device screen until the server boots to the EFI Shell. Start a console session using the console serial port (RS-232) method to view console output prior to booting to the EFI Shell or to access the iLO 2 MP. See"Configuring the iLO 2 MP LAN Using the Console Serial Port (RS-232)" (page 40).

To access the graphic console with VGA, follow these steps:

1. Perform preparation tasks.
2. Connect the cables. See Figure 2-4 and Figure 2-5 (page 31) for specific port information.
   a. Connect the monitor VGA cable to the appropriate VGA port on your server.
   b. Connect the keyboard USB cable to the appropriate USB port on your server.
   c. Connect the mouse USB cable to the appropriate USB port on your server.
3. Power on the server. The EFI Shell prompt displays.

5 Configuring DHCP, DNS, LDAP, and LDAP Lite

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

This chapter addresses the following topics:

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 command 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 HPUX system name visible through a `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 is 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 portion of the DNS standard functionality.

Use the `LC` command to perform the following actions to configure DHCP:

- Set all default LAN settings:

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

- Display current LAN settings:

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

- Modify MP DHCP status:

  ```
  MP:CM> LC -dhcp disabled (or LC -d d )
  ```

- Modify MP IP address:

  ```
  MP:CM> LC -i 192.0.2.1 (or LC -ip 192.0.2.1)
  ```

- Modify MP host name:

```
MP:CM> LC -h hostname (or LC -host hostname)
```

- Modify MP subnet mask:
  ```
  MP:CM> LC -s 192.0.2.1 (LC -subnet 192.0.2.1)
  ```

- Modify MP gateway address:
  ```
  MP:CM> LC -g 192.0.2.1 (or LC -gateway 192.0.2.1)
  ```

- Set link state to auto negotiate:
  ```
  MP:CM> LC -link auto (or LC -l a)
  ```

- Set link state to 10 BaseT:
  ```
  MP:CM> LC -link t
  ```

- Set Remote Serial Console port address:
  ```
  MP:CM> LC -web 2023 (or LC -w 2023)
  ```

- Set SSH console port address:
  ```
  MP:CM> LC -ssh 22 (or LC -ss 22)
  ```

Configuring DNS

Use the DNS command to display and modify the DNS configuration as follows:

1. From the **MP Main Menu**, enter command mode.
2. At the MP:CM> prompt, enter **DNS** (for the DNS configuration).
3. The screen displays **current DNS** data. When prompted to enter a parameter name, A to modify All, or Q to Quit, enter **A** to select all parameters.
4. The screen displays the current DHCP for DNS servers status. When prompted, enter **Enabled**, or **Disabled**.
5. The screen displays the current DHCP for DNS domain name status. When prompted, enter **Enabled**, or **Disabled**.
6. The screen displays the current register with DDNS server value. When prompted, enter, **Yes**, or **No**.
7. The screen displays the current DNS domain name. When prompted, enter a new value.
8. The screen displays the primary DNS server IP address. When prompted, enter a new value.
9. The screen displays the optional secondary DNS server IP address. When prompted, enter a new value.
10. The screen displays the optional tertiary DNS server IP address. 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 the iLO 2 MP to use a directory server to authenticate a user login using the iLO 2 MP text interface.

NOTE: The LDAP connection has an inactivity timeout of 30 minutes in Active directory. For Novell directory, there is no inactivity timeout.

To configure using the Web interface, see "Administration > Group Accounts" (page 100).

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

1. From the **MP Main Menu**, enter command mode.
2. At the MP:CM> prompt, enter **LDAP**(for the LDAP configuration).
3. Enter **D** to select **Directory Settings**. The screen displays the current LDAP directory settings.
4. Enter **A** to select all parameters. The screen displays the current LDAP directory authentication status, **D** - Disabled (default), **X** Enable with Extended Schema, or **S** Enable with Default Schema. The screen displays the local iLO 2 MP user accounts database status. If enabled, the local iLO 2 MP user database is used if there is an authentication failure using the LDAP Directory.
5. Enter **D** - Disabled, or **E** - Enabled. You must enter **E** if LDAP directory authentication is disabled. The screen displays the current LDAP server IP address.
6. Enter the IP address of the LDAP server. The screen displays the current LDAP server port address.
7. Enter a new port number. The screen displays the current object distinguished name. This specifies the full distinguished name of the iLO 2 MP 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 screen displays the Current User Search Context 1.
9. Enter a new search setting. The screen displays the Current User Search Context 2.

NOTE: The context settings 1, 2, and 3 point to areas in the directory service where users are located so the user does 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.

Following is the updated LDAP configuration:

```
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

Administrators can choose to enable directory services to authenticate users and authorize user privileges for groups of iLO 2 MPs. The iLO 2 MP 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 directory services is available from the HP Web site at http://www.hp.com/servers/lights-out.

Using directory services after a user enters their login and password, the browser sends the cookie to the iLO 2 MP. The iLO 2 MP processor accesses the directory service to determine which roles are available for that user login. The iLO 2 MP first uses the credentials to access the iLO 2 MP 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 MP device object and the role object, the iLO 2 MP determines the role object's distinguished name and the associated user privileges. The iLO 2 MP then calculates the current user privileges based on those roles and grants them to that user.

Configuring LDAP Lite Default Schema

The iLO 2 MP 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 MP privileges based on matching groups stored on each iLO 2 MP.

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

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

- Easy implementation without schema extensions - the iLO 2 MP schema-free integration is configured from any iLO 2 MP user interface (browser, command line, or script).
- Minimal administration and maintenance:
  - after initial setup, only groups and permissions require maintenance support on the iLO 2 MP; typically group and permission changes occur infrequently
  - the schema-free approach does not require updating directory databases with new iLO 2 MP devices objects
- Reliable security: iLO 2 MP schema-free does not affect standard directory attributes avoiding conflicting use of attributes that can result over time.
- Complements two-factor authentication: iLO 2 MP schema-free integration can be used in conjunction with iLO 2 MP 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 and once this process has taken place there is no advantage for the schema-free approach until a schema change is required. HP has no plans to update the HP iLO 2 MP schema at this time.

To configure LDAP Lite you need to:

1. Follow the procedure for configuring "Configuring LDAP Extended Schema" (page 53) 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 LDAP Lite using the iLO 2 MP text user interface. To configure using the Web interface, see "Administration > Group Accounts" (page 100).

📝 **NOTE:** Due to command syntax changes in LDAP Lite, some customer-developed scripts may not run. You will need to change any scripts you developed to enable them to run with the new LDAP Lite syntax.

To set up directory security groups, follow these steps.

📝 **NOTE:** You must select the default schema from the LDAP command for the LDAP Lite settings to work.

1. At the MP:CM> prompt, enter the LDAP command. 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**- Security Group Administration. The screen displays the current group configuration.

   ```
   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 screen displays the current LDAP group settings.
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 the iLO 2 MP using directories without requiring schema extensions. The iLO 2 MP acquires the user's name to determine group membership from the directory. The iLO 2 MP then cross-references the group names with its locally-stored names to determine user privilege level. The iLO 2 MP must be configured with the appropriate group names and their associated privileges. To accomplish this configuration, use one of the following options:

- Web interface, use the **Administration > Directory Settings > Group Administration** page.
- iLO 2 MP text user interface, use the LDAP command.

6 Text User Interface

This chapter provides information on the multiple options from which commands can be executed in the iLO 2 MP.

This chapter addresses the following topics:

NOTE: Server blades do not have fans or power supplies. Therefore, their response to certain commands are different than a rack mount server.

MP Command Interfaces

Below is a summary of all the MP command interfaces you can use.

MP Main Menu   The **MP Main Menu** displays 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 **Main Menu** commands (CO, VFP, CM, SMCLP, CL, SL, HE, and X) after 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 typing the CM command at the **MP Main Menu** and typing **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.

See Chapter 8: "SMASH Server Management Command Line Protocol" (page 113) for information on using SMASH SM CLP scripting commands.

Figure 6-1 visually displays the MP command interface options.

Figure 6-1 MP Command Interfaces
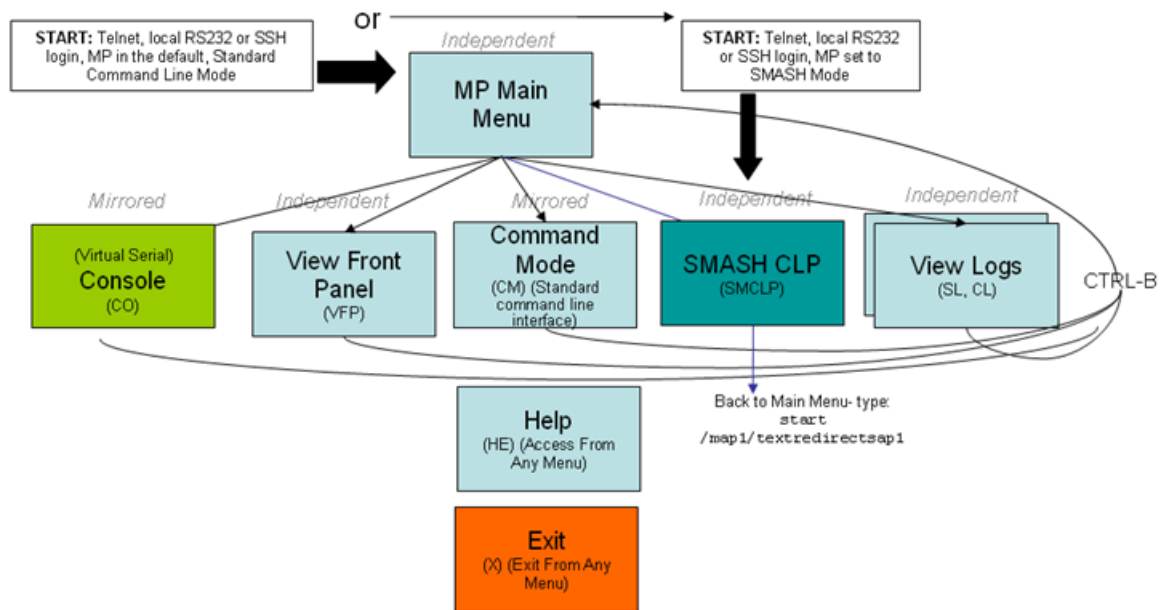
MP Main Menu

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

The iLO 2 MP has the ability to support multiple sessions to perform independent tasks:

- Having multiple windows logged into the iLO 2 MP to monitor VFP or study event logs in some windows 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 yet another window.

The **MP Main Menu** commands are listed in Table 6-1 and described below.

Table 6-1 MP Main Menu Commands and Descriptions

Command	Description
CO	Select console mode
VFP	Display virtual front panel
CM	Enter command interface mode
SMCLP	Access the server management command line protocol (SMASH SM CLP)
CL	View console log
SL	Show event logs
HE	Display help for menu or command
X	Exit

TIP: An effective method for using the iLO 2 MP 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 Command Summary

CO: Console: leave main menu and enter console mode

This command 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 type **Ctrl-Ecf**.

Type 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 Web to the system over the system LAN.

VFP: Virtual front panel

Virtual front panel (VFP) simulates the display panel on the front of the server. It gives real-time 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. When the SEL is accessed, the iLO 2 MP automatically clears the attention state from the front panel.

Each user viewing VFP is in private mode - they enter and leave without affecting other users.

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

CM: Command Mode: enter command mode

This command 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** , follow these steps:

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

If a command is in progress, a message displays informing you of system status.

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

SMCLP: Server Management Command Line Protocol

This command switches the console terminal from the **MP Main Menu** to Server Management Command Line Protocol (SMASH) SM CLP interface. For information on SMASH SM CLP see "SMASH Server Management Command Line Protocol" (page 113).

CL: Console log—view the history of the console output

This command displays up to 60 Kilobytes (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.

What is displayed is an image of the console history at the time the CL command is entered. Console output continues to be logged while this buffer is read, and nothing is lost.

SL: Show Logs — view events in the log history

This command displays the contents of the event logs that have been stored in non-volatile 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 BMC from different sources throughout the server. The iLO 2 MP polls the BMC for new events and stores them in non-volatile memory.

- System event log (SEL): High attention events and errors.
- Forward progress: All events.
- Boot log: All events between "start of boot" and "boot complete".
- Previous boot log: The events from the previous boot.

Reading the system event log turns off the attention LED (flashing yellow light on the system LEF). Accessing this log is the only way to turn off the system LED when it is flashing.

Events are encoded data that provide system information to the user. Some well-known names for similar data would be chassis codes or post codes. Events are produced by intelligent hardware modules, the OS, and system firmware. Use SL to view the event log.

Table 6-2 shows the events and actions used to navigate within the logs:

Table 6-2 Events

Event	Action
+	View the next block (forward in time)
-	View the previous block (backward in time)
Enter (<CR>)	Continue to the next or previous block
D	Dump the entire log for capture or analysis
F	First entry
L	Last entry
J	Jump to entry number
H	View mode configuration (hex)
K	View mode configuration (keyword)
T	View mode configuration (text)
A	Alert level filter options
U	Alert level unfiltered
Q	Quit and return to the **Event Log Viewer Menu**
V	View mode configuration (text, keyword, hex)

Table 6-2 Events *(continued)*

Event	Action
?	Display the **Help** menu
Ctrl-B	Exit command, and return to the **MP Main Menu**

Table 6-3 defines alert (or severity) levels.

Table 6-3 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).

HE: Display help for menu or command in the Main Help Menu

This command displays the iLO 2 MP hardware and firmware version identity, and the date and time of firmware generation.

- If executed from the **MP Main Menu**, it displays general information about the iLO 2 MP, and those commands available in the **MP Main Menu**.
- If executed in command mode, this command 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 iLO 2 MP

This command exits users from the **MP Main Menu**. If the terminal is the local serial port, users return to the login prompt. For all other types of terminals, users are disconnected from the iLO 2 MP.

Command Menu

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

The **Command Menu** commands are listed in Table 6-4 and described below.

Table 6-4 Command Menu Commands and Descriptions

Command	Description
BP	Reset BMC passwords
BLADE	Display BLADE parameters **NOTE:** This command is available only on a server blade.
CA	Configure async or serial ports
DATE	Display the current date
DC	Default configuration

Table 6-4 Command Menu Commands and Descriptions *(continued)*

Command	Description
DF	Display field replaceable unit (FRU) information
DI	Disconnect LAN console
DNS	Set DNS configuration
FW	Upgrade iLO 2 MP firmware and system hardware firmware
HE	Display help for menu or command
ID	Display or modify system information
IT	Modify the iLO 2 MP inactivity timeouts
LC	LAN configuration
LDAP	LDAP configuration
LM	License management
LOC	Display and configure locator LED
LS	LAN status
PC	Remote power control
PR	Configure power restore policy
PS	Power management module status
RB	Reset BMC
RS	Reset the system through RST signal
SA	Set access options
SNMP	Configure SNMP parameters
SO	Configure security options
SS	Display system processor status
SYSREV	Display all firmware revisions
TC	Reset through transfer of control (TOC)
TE	Tell (send a message to other users)
UC	User configuration
WHO	Display connected the iLO 2 MP users
XD	Diagnostics or reset of the iLO 2 MP

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

- To access the **Command** menu, type **CM** at the **MP Main Menu**.
- To see all the available commands, type **HE LI** at the MP:CM> prompt.
- To access the **Command** menu help, type **HE** at the MP:CM> prompt. The **Command** menu help provides information on all the **Command** menu items.
- To return to the **MP Main Menu** from any of these commands, type **Ctrl-B**.
- To modify the inactivity timeout, use the IT command. There is an inactivity timer that aborts a command if you do not complete it within a certain time period.
- To abort most commands, type **Q** at the point when the iLO 2 MP is asking for input.

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. See the individual commands listed below for the specific keywords that are applicable to that command.

Typically, tools like Expect (see "Expect Script Example" (page 63)) (http://expect.nist.gov/) are used to string together several commands to accomplish a task. These types of scripting tools enable you to write a script for one iLO 2 MP, and use it to apply the same commands to hundreds of iLO 2 MPs. Scripting tools have capabilities that enable you to:

- Write scripts to 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, and so on

Scripting tools and the command line interfaces enable you to carry out commands to multiple iLO 2 MPs such as setting the IP address on 10 MPs that were pulled from a list of 10 IP addresses that were 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 the iLO 2 MP, 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 text interface (when used with command-line arguments) and the SMASH command line interface, were both created with these types of scripting tools in mind to facilitate very powerful automation capabilities.

Expect Script Example

The following Expect script example provides an idea of a very simple script with no timeouts, no error checking, and 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 as a reference to assist you with learning about the **Command** menu commands. Command line interface scripting syntax for each command is provided to assist you with accomplishing a scripting task. The following rules apply to scripting syntax:

- **-nc** (no confirmation) is optional. This is a special keyword that designates that no user confirmation is required to execute the command. If you type **–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 needs to 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 multi-level selector, the command displays all or just the specific multi-level parameters. The absence of a specific multi-level parameter on a command that has multi-levels, causes ALL the multi-level parameters to display.

- Most commands accept **-all default**. This causes all parameters for that command to be set to their default values.
- In some multi-level 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 type **-?** by itself with the command, a usage display is produced. In the event of an incorrect command line usage, in addition to the error message, the usage display is output.
- Arguments that are in brackets **[ ]** are optional.
- Without arguments, the system prompts you for 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.

This command is used to reset the baseboard management controller (BMC) (EFI Shell) user and admin passwords.

Command line usage and scripting:

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

See also: DC, RB, UC

BLADE: Display BLADE parameters

Command access level: Login access.

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

Command access level: login access.

This command is used to facilitate the cabling and initial installation of server blades. It also provides a quick view of the enclosure status. Only a user with configuration access right can turn the enclosure locator UID LED on or off.

Onboard Administrator Configuration

- OA IP Address: IP address of the Onboard Administrator.
- OA MAC Address: MAC address of the Onboard Administrator.

Server Blade Configuration

- Rack Name : The rack name is used to logically group together enclosures in a rack. The rack name is shared with the other enclosures in the rack.
- Rack UID : Rack unique identifier: a known unique identifier for this.
- Bay Number : The blade enclosure can support as many as eight 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.

Enclosure Information

Enclosure Name: The enclosure name is used to logically group together the server bladess 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.

This command is used to set 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 HPUX is the local serial port console speed.

Baud rate: Input and output data rates are the same.

Flow control: Hardware uses RTS/CTS; software uses Xon/Xoff.

Set up the local serial port parameters as follows:

- BAUD RATES: Input and output data rates are the same — 4800, 9600, 19200, 38400, 115200 bit/sec.
- FLOW CONTROL: Hardware uses RTS/CTS; software uses Xon/Xoff.

For 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. Having inconsistent bit rate settings may 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 the iLO 2 MP; but the settings are not permanent for power cycles or blade ejection. For power cycle to the blade, the RS–232 serial port is set back to the iLO mode.

If you cannot access the MP through telnet and the port mode of operation set is the AUX UART mode, you need to 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 mode, 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 shipping settings. The hard reset returns the port default connection to MP.

> **NOTE:** The reset button distinguishes between short and long presses. Both short and long button presses will return the port default connection to the MP.

The iLO 2 MP mirrors the system console to the iLO 2 MP local 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.

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.

This command is used to display the date, as best known to the iLO 2 MP. The iLO 2 MP clock is updated from the BMC/SFW and cannot be modified. The real-time clock is only used when the iLO 2 MP 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 the default configuration

Command access level: MP configuration access.

This command is used to set all iLO 2 MP 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 the iLO 2 MP:

- In the UC command, change individual users or reset all users to default values.
- Reset passwords by pressing the **iLO 2 MP reset** button on the back panel of your HP server for greater than four seconds. After the iLO 2 MP 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 using any of the previous reset methods.

Command line usage and scripting:

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

DF: Display FRU information

Command access level: Login access.

This command is used to display 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 Console

Command access level: MP configuration access.

This command is used to disconnect the LAN, Web SSL, or SSH users from the iLO 2 MP. It does not disable the ports. To disable the ports, see the SA command for LAN/WEB/SSH/IPMI over LAN access. The TE and WHO commands are useful 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`: Domain Name Server settings

Command access level: MP configuration access.

This command is used to configure the DNS Domain Name and up to three DNS servers either manually or automatically with DHCP. You can only use this command 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 iLO 2 MP firmware

Command access level: MP configuration access.

This command is used to upgrade the iLO 2 MP firmware. This command is only available from the iLO 2 MP LAN port and the local serial port.

The version of iLO 2 MP firmware is displayed at the top of the main **Help** menu.

Before performing the upgrade, consider the following:
- Verify that the MP LAN is operational since the upgrade is performed using ftp over the MP LAN.
- You must enter the ftp server IP address, login, password, and directory in which the upgrade files reside e.g. /root/sub/sd2
- You can run the `FW` command from the LAN, Web, or local ports.
- If the upgrade is successful, the iLO 2 MP reboots with the new firmware. If the upgrade fails, the iLO 2 MP returns to the prompt with instructions on what went wrong, and what to do next.
- Upgrading the MP software and rebooting the MP can be safely performed without affecting the operation of the server. However, if this upgrade contains system programmable hardware, you must properly shut down any running operating system before starting this process since the system power is cycled after successful completion.

This command performs two functions:
- Upgrades iLO 2 MP firmware. This firmware upgrade does not affect server operation if it is for iLO 2 MP firmware only. You do not need to shut down the OS to perform this upgrade.

IMPORTANT: The EFI utility supports iLO 2 MP upgrades, but does not support FPGA or PSOC upgrades.

- Upgrades FPGA or PSOC system programmable hardware. This firmware upgrade affects server operation since system power is cycled whenever system programmable hardware is upgraded. 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.

IMPORTANT: To upgrade EFI or BMC system programmable hardware, you must use the EFI utility.

To perform a firmware upgrade, follow these steps:

1. Download the firmware from the HP Web site at: **http://www.hp.com/go/bizsupport**. Select the download for IPF firmware and follow the directions.
2. Copy the firmware image file onto your own FTP server.
3. Establish a telnet or SSH session with the iLO 2 MP.
4. Logon to the iLO 2 MP using the **Admin** password.
5. At the **MP Main Menu**, type **CM** to enter the **Command Menu**.
6. Type **FW** to enter firmware upgrade mode.
7. At the Source IP prompt, enter the IP address of the FTP server where the firmware image file resides and press **Enter**.
8. At the File Path prompt, enter the directory and path where the firmware is located. (example, /firmware/rx2660/example/)
9. At the Enter Login prompt, enter your username on the FTP server.
10. At the Enter Password prompt, enter your password on the FTP server.
11. When you are prompted to confirm, enter **Y** to confirm.

    The firmware will be upgraded. telnet, and SSH connections are dropped upon successful completion, and the iLO 2 MP automatically resets.

12. After the upgrade, reconnect and log in as user **Admin** and password **Admin** (case sensitive). The upgrade is complete. The version of the iLO 2 MP firmware displays at the top of the main **Help** menu.

CAUTION: If the upgrade process is interrupted at any time, the system board may need to be repaired or replaced.

The following is an example of a firmware upgrade confirmation upgrade:

```
New Firmware Upgrade Parameters
    * I - Source IP : 192.9.2.1
    * P - File Path : /firmware/rx4640/example/ (the appropriate path)
    * L - Login     : (your username on FTP server)
    * W - Password  : ****** (your password on FTP server)

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

    -> MP firmware upgrade in progress. . . .

    -> Retrieving upgrade file using FTP.

    -> Retrieving an upgrade file successfully.
       Programming ROM. Percent Complete: 100

    -> MP firmware upgrade complete - telnet connections will
       be dropped. MP will now reset . . . .
```

Command line usage and scripting:

```
FW [ -ip <ipaddr> —path <dirpath>
      -login <anonymous|ftp|login>  [/<password>] [ -nc ] ]
      -?
```

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

This command is used to display the iLO 2 MP hardware and firmware version identity, and the date and time of firmware generation.

- If executed from the **MP Main Menu**, help displays general information about the iLO 2 MP, and those commands available in the **MP Main Menu**.
- If executed in command mode, the command displays the **MP Help: Command Menu List**. The command 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.

This command is used to display and modify the following:

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

> **NOTE:** The system host name information is not retained across iLO 2 MP 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> ] } ] [ -nc ]
      -?
```

IT: Inactivity timeout settings

Command access level: MP configuration access.

This command is used to prevent sessions to the system from being inadvertently left open. When you initiate an iLO 2 MP command, other users are prohibited to execute 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 the iLO MP locked in a command preventing other users from executing iLO 2 MP commands. 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 MP 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 (IP address, and so on)

Command access level: MP configuration access.

This command is used to modify the LAN configuration.

IMPORTANT: If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, the iLO 2 MP 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, the iLO 2 MP alerts you to manually reset the iLO 2 MP.

Configurable parameters include:

- 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 it 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, it is useful to 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 Serial Console 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 directory settings is an iLO 2 MP Advanced Pack license feature that enables centralized user account administration using directory services.

This command is used to display and modify the following LDAP directory settings:

- Directory Authentication: Choosing enable or disable, activates or deactivates directory support on the iLO 2 MP.
  - Enable with Extended Schema: selects directory authentication and authorization using directory objects created with the HP schema. Select this option if the directory server has been 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 this option is selected. In the **Group Administration** page, configure one or more directory groups by entering the distinguished name of the group and privileges that should be granted to users who are members of that group.
  - Disable deactivates directory support on the iLO 2 MP.
- Local User Accounts: Includes or excludes access to local iLO 2 MP user accounts. If local user accounts are enabled, you may log in to the iLO 2 MP 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 against the directory first, then 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: Distinguished Name (DN) of the iLO 2 MP, specifies where this iLO 2 MP 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 that are applied to the login name entered to access the iLO 2 MP.

  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 the iLO 2 MP. All objects listed in the directory can be identified using their unique distinguished name. However, distinguished names can be long, users may not know their distinguished user names, or they may have accounts in different directory contexts. Search contexts allow users to specify common directory contexts, so that users do not have to enter their full distinguished name at login. iLO 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 successful.

  Example 1: Instead of logging in as "cn=user,ou=engineering,o=hp", search context of "ou=engineering,o=hp" allows a user to login as "user"

  Example 2: (This format can be used only 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 may login as: "user@domain.hp.com", in which case a search context of "@domain.hp.com" allows the user to login as "user".

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

This command is used 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.

The group administration section of LDAP command enables users 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.

When a user attempts to login into the iLO 2 MP, the iLO 2 MP reads that user's directory name in the directory to determine the groups the user is a member of. The iLO 2 MP 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.

`LDAP`: LDAP Lite

LDAP Lite enables you to use directory authentication for logging in to the iLO 2 MP without having to do any schema extension on the directory server or snap-in installation on the client. For information on configuring LDAP Lite, see "Configuring LDAP Lite Default Schema" (page 54).

📝 **NOTE:** Due to command syntax changes in LDAP Lite, some customer-developed scripts may not run. You will need to change any scripts you developed to enable them to run with the new LDAP Lite syntax.

`LM`: License management

Command access level: MP configuration access.

This command is used to view your current license status. Use it to enter a license key to enable the following features:

- Directory-based authentication and authorization using LDAP.
- LDAP Lite: schema-free directory integration.
- Integrated Remote Console (vKVM and vMedia)

Command line usage and scripting:

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

`LOC`: Locator UID LED configuration

Command access level: MP configuration access.

This command is used to display the current status of the locator UID LED and enables you to turn the locator UID LED on or off.

In server blades, this command also allows you to turn the enclosure locator UID LED on or off. The UID LED is used to physically identify the blade in a datacenter environment. It emits a blue light when turned on. It does not have its own button to turn it on or off; you can only control the UID LED by the BMC.

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.

This command is used to display all parameters and the current status of the iLO 2 MP LAN connections. The LAN parameters are not modified by the execution of this command.

Command line usage and scripting:

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

See also: DNS, LC, SA

PC: Power control access

Command access level: Power control access.

This command is used to provide the following options for remote control of the system power:

ON	Turns the system power on (the 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 bring the software down before power is turned off. To turn the system off properly, ensure that the OS is in the proper shutdown state before issuing this command. Use the proper OS commands or use the graceful shutdown option of the PC command.
CYCLE	Turns the system power off and on. The delay between off and on is 30 seconds.
Graceful Shutdown	The BMC sends a signal to the OS to shutdown prior to turning off the system power.

For proper system shutdown, shut down the OS before issuing this command, or use the PC command's graceful shutdown option.

Command line usage and scripting:

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

Example of the PC command with output:

```
[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

PR: Power restore policy configuration

Command access level: MP configuration access.

This command is used to configure 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 switch or execute a 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 was removed or lost.

Command line usage and scripting:

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

See also: PC

PS: Power status — display the status of the power management module

Command access level: Login access.

This command is used to display the system power state and the temperature and status of the power supplies and fans.

Command line usage and scripting:

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

See also: PC, SS

RB: Reset BMC

Command access level: MP configuration access.

This command is used to reset the BMC by toggling the GPIO BMC reset line.

Command line usage and scripting:

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

See also: PC, SS

RS: Reset system through RST signal

Command access level: Power control access.

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

This command is used to cause the system (except iLO 2 MP) to be reset through the RST signal.

Execution of this command irrecoverably halts all system processing and I/O activity and restarts the computer system. The effect of this command is similar to cycling the system power. The OS is not notified, no dump is taken on the way 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.

This command is used to set access permissions for users logging in to the MP over the LAN. You can set the iLO 2 MP to allow telnet access, Web access, SSH, IPMI over LAN, or all four.

If LAN or Web users are connected at the time a disable from this command is executed, they are disconnected. Any future incoming connection request to the corresponding port is rejected.

NOTE: This command does not affect the ability of the iLO 2 MP to perform firmware upgrades over the LAN.

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.

This command is used to perform 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.

NOTE: Currently, the SNMP alert feature is only supported on the BL860c server blade.

• Configure up to four destination IP addresses where SNMP alerts will be sent. Alerts will be sent by the iLO 2 MP 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, follow these steps:

1. At the MP:CM> prompt, enter **SNMP**.
2. Enter **N** to change the SNMP status. 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. Enter **T** to change the SNMP alert status. 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. Enter **1 2 3 4** to configure a destination IP address for SNMP alerts. The default is **blank** (unused).
7. Enter **C** to configure the community string to secure the access to the MIB objects. The default is **public**.

Command line usage and scripting

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

Command line usage and scripting for BL860c:

```
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 (login timeouts, password faulty, SSL certificate generation, SSH keys)

Command access level: MP configuration access.

This command is used to modify the security option of the iLO 2 MP.

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 (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 user is brought back to the MP Login: prompt.

- Number of Password Faults allowed: 1 to 10. This parameter defines the number of times a console can attempt to login before being rejected and having its connection closed.
- SSL certificate: enables the generation of SSL certificates.
- SSH keys generation: enables SSH keys authorization.
- Firmware upgrade: enables firmware upgrades over PCI.
- iLO 2 MP reset: enables an iLO 2 MP reset through IPMI (from BMC, system, or IPMI over LAN).
- iLO 2 MP password reset: enables iLO 2 MP 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 — Displays the status of the system processors

Command access level: Login access.

This command is used to display the status of the system processors and which processor is the monarch.

The iLO 2 MP learns the system configuration through the events it receives from the system. There will likely be a delay between any processor configuration change and what is displayed by this command. A more reliable way to get the processor configuration information is at the EFI or BCHprompt.

Command line usage and scripting:

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

See also: PS

SYSREV: Firmware revisions

Command access level: Login access.

This command is used to display current revisions of firmware in the system.

Example of the SYSREV command with output:

```
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
```

Command line usage and scripting:

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

TC: System reset through INIT or TOC (Transfer of Control) signal

Command access level: MP configuration access.

Under normal operation, shut down the OS before issuing this command.

This command is used to cause the system to be reset through the INIT (or TOC) signal. Execution of 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 on the way 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.

This command is used to treat all displayable characters following the `TE` command as a comment. Characters typed are broadcasted to the connected console clients when you press the **Return** key. 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.

This command is used by administrators to add, modify, re-enable, or delete 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 the iLO 2 MP and to execute "Status" or "Read-only" commands (view event logs, check system status, power status, and so on) but not to execute any commands that would alter the state of the iLO 2 MP or the system.

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

An iLO 2 MP user can also have any or all of the following 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`

*   iLO 2 MP Configuration Access: Right to configure all iLO 2 MP settings (as well as 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 virtual media applet.

NOTE: The virtual media feature is only available if you have the iLO 2 MP Advanced Pack license and the user virtual media 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 of the `UC` command with output:

```
[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 MP connected users

Command access level: Login access.

This command is used to display 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 — MP **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 displays as well.

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

Command line usage and scripting:

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

See also: `DI, TE`

XD: Diagnostics or reset of the iLO 2 MP

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

This command is used to perform simple checks to confirm the iLO 2 MP's health and its connectivity status. The following tests are available:

- iLO 2 MP Parameter Checksum in NVRAM.
- Verify I2C connection (get BMC device ID).
- LAN connectivity test using the `ping` command.
- History of firmware updates and other activities

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

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

Command line usage and scripting:

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

7 Web Graphical User Interface

One of the methods available to access the iLO 2 MP is the Web graphical user interface (GUI). This chapter describes the functions and options of the Web interface with examples and descriptions of the Web GUI.

Some of the functionality in the Web GUI will only display if you have the iLO 2 MP Advanced Pack license. For more information on the iLO 2 MP Advanced Pack license, see "Advanced Pack License" (page 23) and the HP Web site 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 MP Web GUI.

This chapter addresses the following topics:
- "System Status" (page 83)
- "Remote Console" (page 88)
- "Virtual Devices" (page 93)
- "Administration" (page 96)
- "BL c-Class" (page 110)
- "Help" (page 111)"

System Status

The **System Status** tab enables you to access the following pages:
- Status Summary: General and Active Users
- Server Status: General and Identification
- System Event Log

System Status > Status Summary > General

The **Status Summary General** page (Figure 7-1) displays a brief status summary of the system.

Figure 7-1 Status Summary General Page
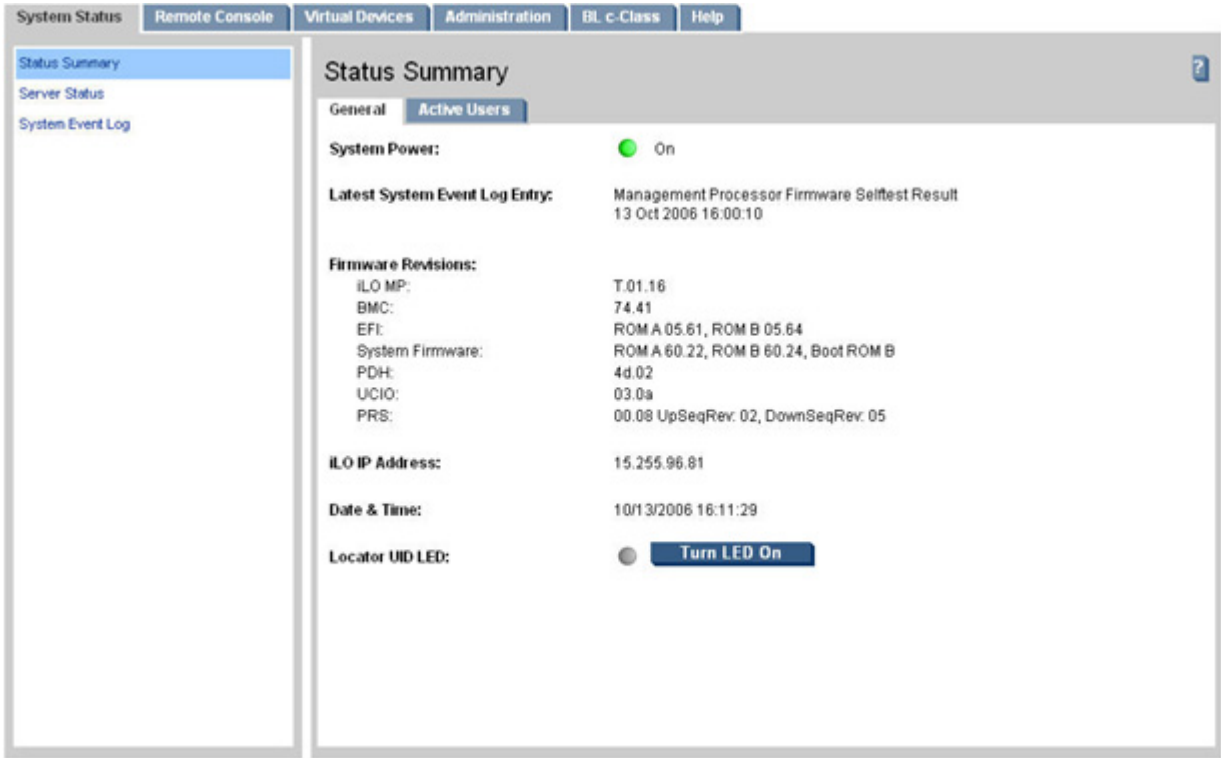
> **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-1 lists the fields and descriptions.

Table 7-1 Status Summary General Page Description

Field	Description
System Power	The current power state (ON/OFF/STANDBY) of the system along with the corresponding power LED state.
Latest System Event Log Entry	The most recent entry in the System Event Log (SEL).
Firmware Revisions	Displays current revisions of firmware (iLO, BMC, system firmware) in the system. Also displays firmware revisions of other firmware such as DHCP, UCIO, and so on.
iLO 2 MP IP Address	The IP address of the iLO 2 MP subsystem.
Date & Time	Displays the date and time as known to the iLO 2 MP.
Locator LED	Displays the status of the (Blue) Locator or Unit Identifier (UID) LED and enables you to turn the Locator LED on or off. Note: The system's (Yellow) Attention indicator, which is separate from the locator LED, is lit automatically if a Warning event is present in the System Event Log. To clear the Attention indicator, read the System Event Log.

System Status > Status Summary > Active Users

The **Active Users** page (Figure 7-2) displays information about the users currently logged in to the iLO 2 MP.

Figure 7-2 Status Summary Active Users Page
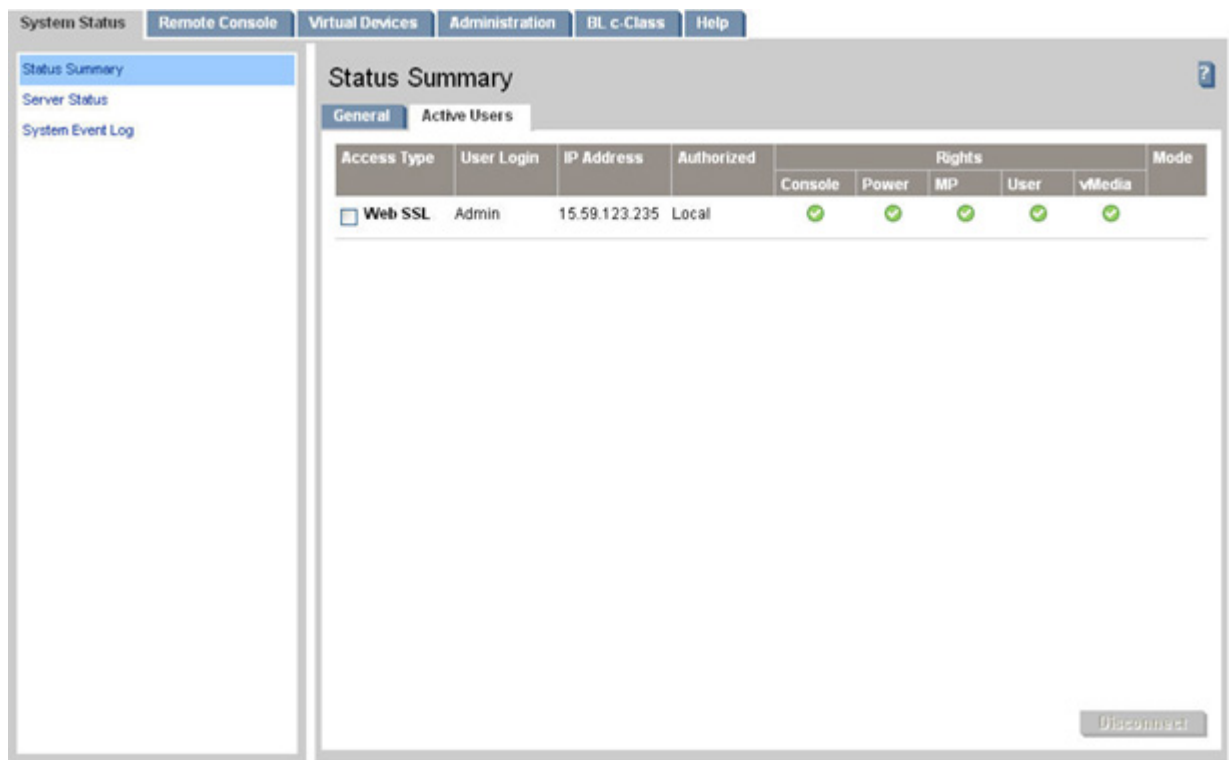
NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-2 lists the fields and descriptions.

Table 7-2 Active Users Page Description

Field	Description
Access Type	There are multiple access methods: Serial, telnet, SSH, SSL Web or IPMI over LAN. IPMI, vMedia, and vKVM/IRC 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 user.
Authorized	This indicates the type of authentication: LDAP directory user authentication (LDAP) or locally stored iLO 2 MP user accounts (Local).
Rights	Rights control the iLO functions a user can perform. There are five user access rights: console access, iLO 2 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 MP mode that the user is in. Text user interface 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.

System Status > Server Status > General

The **Server Status General** page (Figure 7-3) displays the following information: system power state, status of the power supplies, temperature, and status of the fans. It also displays the status of the system processors and which processor is the monarch.

Figure 7-3 Server Status General Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-3 lists the fields and descriptions.

**Table 7-3 Server Status General Page Description**

Field	Description
System Power	The current power state of the system along with 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 Onboard Administrator. See "BL c-Class" (page 110).

System Status > Server Status > Identification

The **Identification** page () enables you to configure system information for identifying the server.

Figure 7-4 Server Status Identification Page

Enter the system host name. Obtain the factory-set default system host name from the MAC address label on the server. The system host name is 14 characters long, consisting of the letters **mp** followed by the 12 characters of the Media Access Protocol (MAC) (example: mp0014c29c064f). This address is assigned to the system board. The system board has a unique MAC address that identifies the board on the network.

IMPORTANT: Make sure you obtain the MAC address to the system board and not the MAC address to the server core LAN card.

Enter the relevant details like location, rack id, position, contact person name, telephone number, e-mail, and pager number.

Many of the fields are published by the iLO 2 MP's SNMP for visibility to management applications on the network.

System Status > System Event Log

The **System Event Log** page (Figure 7-5) enables you to view the contents of the event logs that have been stored in nonvolatile memory. A user with login rights can view the system event log. Only a user with iLO configuration access right can clear the logs.

Figure 7-5 System Event Log Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

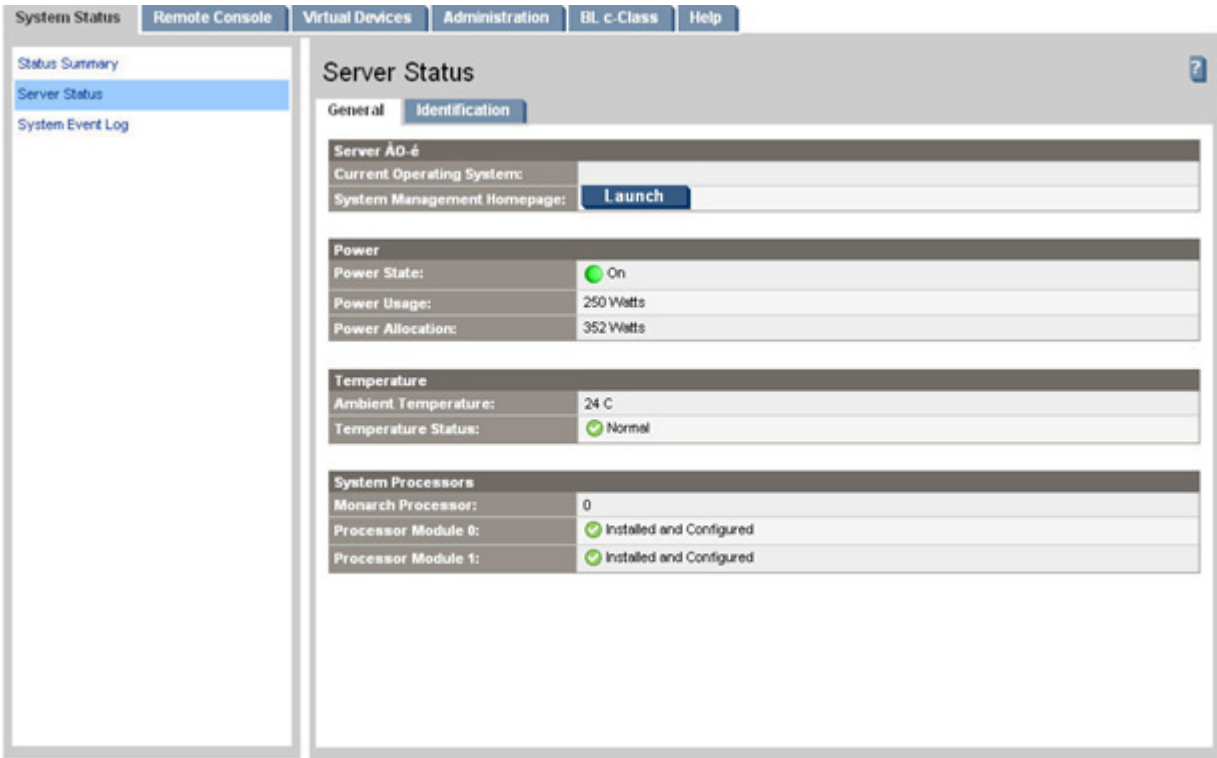Table 7-4 lists the fields, buttons, and descriptions.

Table 7-4 System Event Log Page Description

Fields and Buttons	Description
System Event Log	High attention events and errors. Reading the system event log turns off the attention LED (or blinking yellow light on the system LED).
Forward Progress Log	Contains events of all event types. Does not need to be cleared. In a Web GUI session you cannot view forward progress logs, only system event 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.

Table 7-4 System Event Log Page Description *(continued)*

Fields and Buttons	Description
Previous Boot Log	The boot log from the previous boot.
Delete Log	Deletes the log.

NOTE: You can only view the most pertinent fields for each event on the Web. For a more complete decode of the events, use the text user interface available by logging in to the iLO 2 MP through telnet or SSH.

Events

Events may be a result of a failure or an error (such as, fan failure, Machine-Check, and so on). They may indicate a major change in system state (such as, firmware boot start, system power on/off). Or they may be forward progress markers, (such as, CPU selftest complete).

Events are produced by intelligent hardware modules, the OS, and system firmware. Events funnel into BMC from different sources throughout the server. The iLO 2 MP polls the BMC for new events and stores them in non-volatile 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 Console

The **Remote Console** tab enables you to access the following pages:
- Integrated Remote Console
- Remote Serial Console

You can also connect to the system console by launching **View Console** from the **Remote Console** page.

Remote Console > Integrated Remote Console

The **Integrated Remote Console** (IRC) page (Figure 7-6) offers a remote console interface for Windows clients running Internet Explorer. The IRC data stream is encrypted, enabling you to securely view and manage the server. The **IRC** page refreshes every 10 seconds.

The IRC enables you to view the server graphics console and control the keyboard and mouse, as if you were standing in front of the remote server. Because the iLO 2 MP IRC is hardware-based, it is available regardless of the state of the operating system.

NOTE: Internet Explorer version 6 with service pack 1 and above is the only supported browser for this feature and Windows is the only supported operating system on HP Integrity servers. Additionally clients must allow downloading and usage of signed ActiveX controls.

Only one user has access to the IRC at a time. Only a user with console access right can use this feature. If a user does not have console access right, see the **User Administration** page under the **Administration** tab to add the access right.

NOTE: This feature is only available if you have the iLO 2 MP Advanced Pack license. If the iLO 2 MP is not licensed to use the IRC, see the **Licensing** page under the **Administration** tab to activate the Advance Pack License.

For more information on the IRC, see Chapter 10: "Integrated Remote Console and vKVM" (page 175).

Figure 7-6 Integrated Remote Console Page
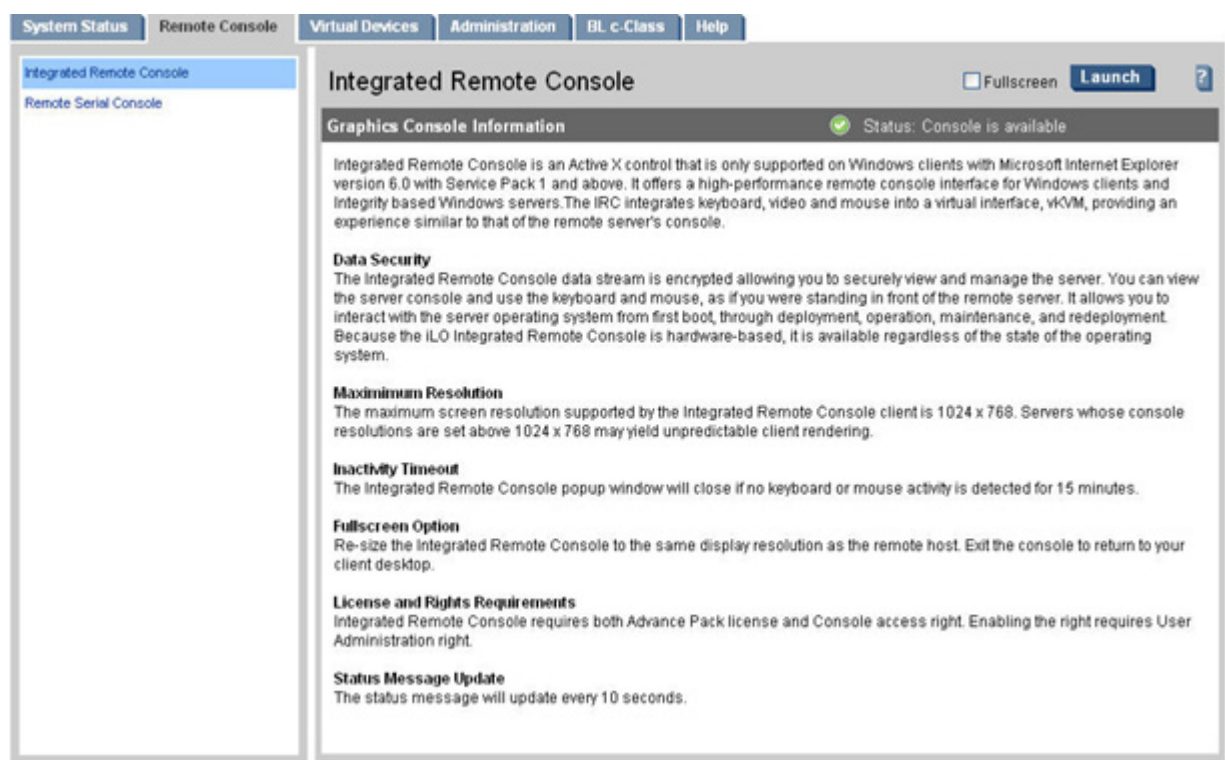
NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-5 lists the fields, buttons, and description,

Table 7-5 IRC Page Description

Fields and Buttons	Action
Fullscreen	Select to re-size the IRC. Note: For fullscreen with multi-head client, launch the browser from the primary display.
Launch	Re-sizes the IRC to the same display resolution as the remote host. To open the server's graphic console in a new browser window, click the **Launch** button. The IRC window opens (Figure 7-7).

Figure 7-7 Integrated Remote Console Window
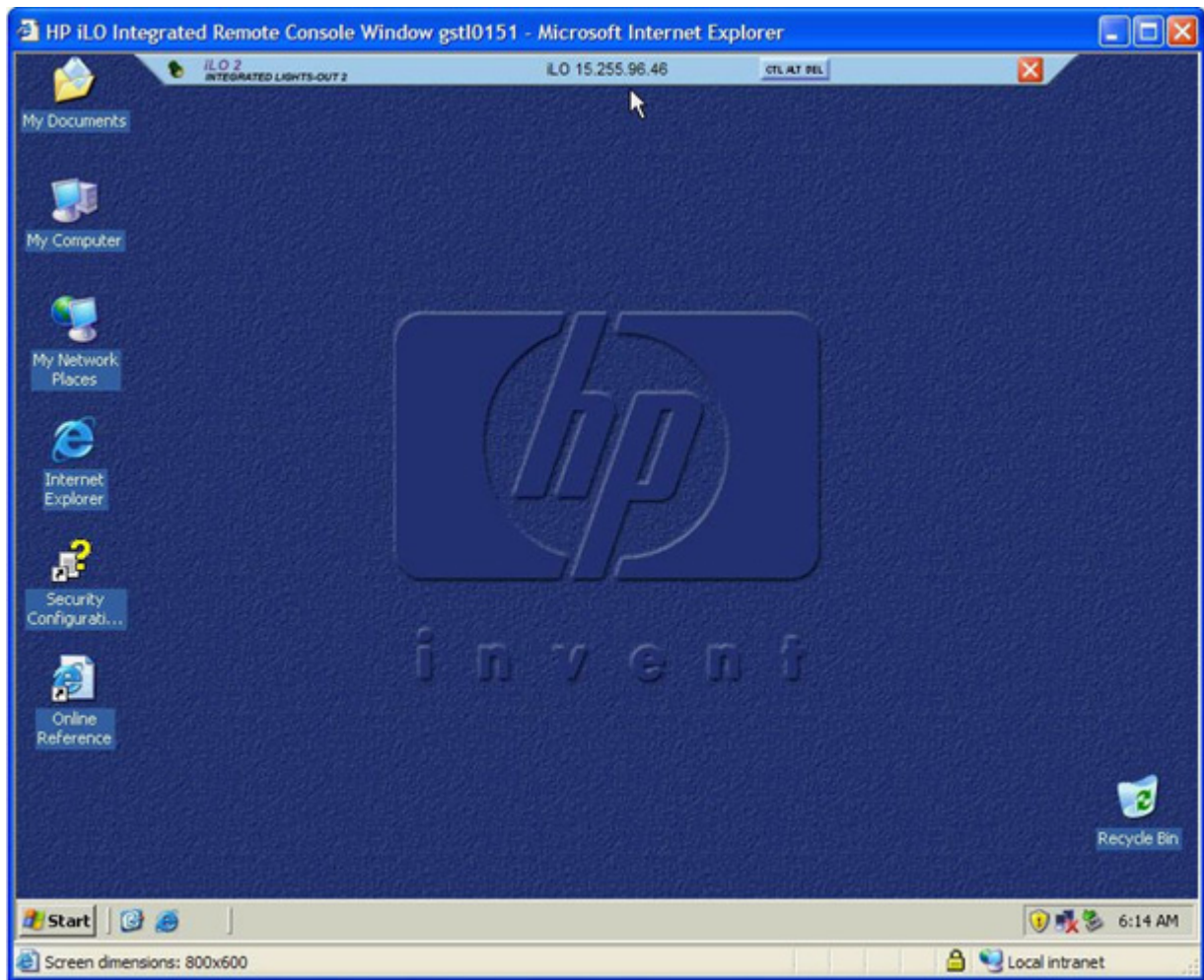
Table 7-6 lists the menu bar, buttons, and actions you can perform in the IRC.

Table 7-6 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 **ctrl alt del** sequence on a remote console.
Exit (red button)	Enables you to close and exit the console and return to the client desktop.

The IRC enables you to:
- View the server system's display.
- Perform maintenance activities.
- Interact with the server.
- Open and run applications on the server using the keyboard and mouse control.

Remote Console > Remote Serial Console

The **Remote Serial Console** page (Figure 7-8) enables you to securely view and manage a remote server. Only a user with console access right can use this feature.

Figure 7-8 Remote Serial Console Page
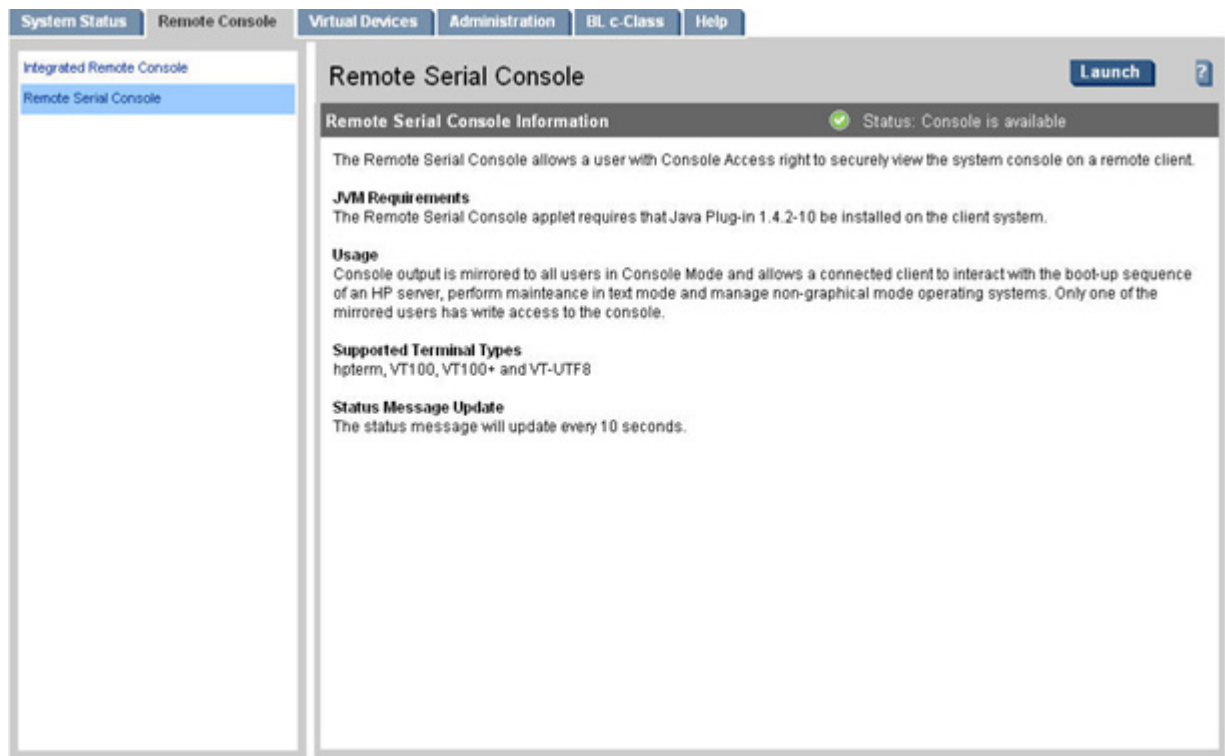
NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

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 the iLO 2 MP.

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 MP 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, type **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 MP 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:
  - VT100
  - VT100+
  - VT-UTF8

IMPORTANT: Do not mix hpterm and vt100 terminal types at the same time.

To connect to the system console (Figure 7-9), click **Launch**.

NOTE: If the **Launch** button 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 7-9 Remote Serial Console Window
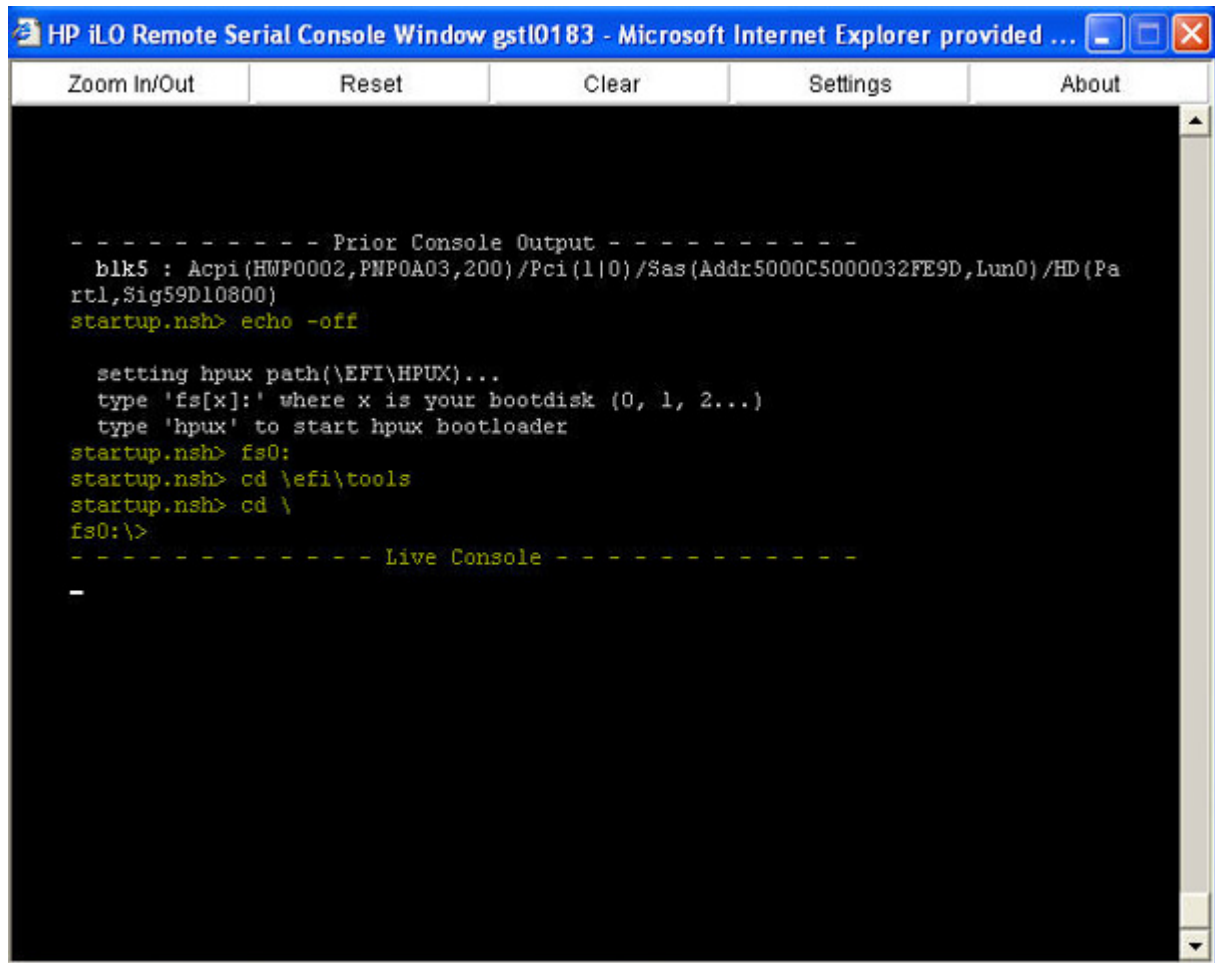
Using this feature you can:

- 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 MP interface using the provided link in the banner, leave the iLO 2 MP 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 non-volatile 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

The iLO 2 MP 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 the iLO 2 MP. The iLO 2 MP 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, an administrator can access a console application such as Windows EMS remotely over the network. The iLO 2 MP contains the functional equivalent of the standard serial port (16550 UART) register set, and the iLO firmware provides a Java applet that connects to the server serial port. If the serial redirection feature is enabled on the host server, iLO 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's serial port, you can use the iLO virtual serial port feature to remotely login 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*, at:
http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00263709/c00263709.pdf

Virtual Devices

The **Virtual Devices** tab enables you to access the following pages:
- Power & Reset
- Virtual Media

Virtual Devices > Power & Reset

The **Power & Reset** page (Figure 7-10) 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 the iLO 2 MP.

Figure 7-10 Power & Reset Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-7 lists the fields, buttons, and descriptions.

Table 7-7 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. Only a user with iLO configuration access right can 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 will stay 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.

Table 7-7 Power & Reset Page Description *(continued)*

Fields and Buttons	Description
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. Only a user with power control access right can 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. Only a user with iLO configuration access right can 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. Only a user with iLO configuration access right can issue this option.
iLO 2 MP	This feature has the following options: • Reset to the iLO 2 MP default configuration: This option enables you to set all iLO 2 MP parameters back to their default values. Only a user with iLO configuration access right can issue this option. • Reset the iLO 2 MP: This option enables you to reset the iLO 2 MP. You can safely perform an iLO 2 MP reset without affecting the operation of the server. Only a user with iLO configuration access right can issue this option.
Submit	Click this button to submit selections.

Virtual Devices > Virtual Media

The **Virtual Media** page (Figure 7-11) provides access to a virtual CD/DVD drive or an image file, which can direct a remote host server to boot and use standard media from anywhere on the network. The **Virtual Media** page refreshes every 10 seconds. Only one user can connect a virtual device at a time.

📝 **NOTE:** The virtual media feature is only available if you have the iLO 2 MP Advanced Pack license and the user virtual media access right.

For more information on virtual media, see .

Figure 7-11 Virtual Media Page

| System Status | Remote Console | Virtual Devices | Administration | BL. c-Class | Help |

Power & Reset
Virtual Media

Virtual Media   [Launch] [?]

CD-ROM Support   ✔ Status: vMedia is available

Connects a USB CD-ROM/DVD drive or CD-ROM disk image files 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. Only El Torito bootable CD_ROM format DVD and CD media is supported at system boot time. Removeable USB floppies and memory devices are not supported.

JVM Requirements
The Virtual Media applet requires that Java Plug-in 1.4.2-10 be installed on the client system.

License and Rights Requirements
Usage of the applet requires both Advance Pack license and the user's Virtual Media right be enabled. The right can be enabled from the Administration tab's User Administration page by someone with User right. Licensing is enabled on the Administration tab's Licensing page.

Status Message Update
The status message will update every 10 seconds.

> **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-8 lists the features, buttons, and descriptions.

Table 7-8 Virtual Media Page Description

Features and Buttons	Description
Virtual Media	Connects the CD/DVD or images on your client PC, or anywhere in the network, to the remote server so they appear local to the server during system boot or while the operating system is available.
JVM Requirements	Java Virtual Machine (JVM). This feature requires prior installation of Java Plug-in 1.4.2_10 or above.
License and Rights Requirements	Usage of the virtual media applet requires that both the iLO 2 MP Advance Pack License and the user virtual media right be enabled.
Launch	Opens a Java applet window which enables connection of USB CD/DVD devices and disk image files available on the client as virtual devices on the server. (See Chapter 11: "Virtual Media" (page 179) for more information.) The applet window refreshes every 10 seconds.

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

Administration > Firmware Upgrade

The **Firmware Upgrade** page (Figure 7-12) enables you to remotely upgrade the firmware from an FTP source. Only a user with iLO configuration access right can use this feature.

The upgrade is performed using FTP over the iLO 2 MP LAN, which must be operational.

There are two separate functions you can perform with this command. Depending on which upgrade you perform you may or may not need to shut down the OS:

- Upgrades iLO 2 MP firmware. This firmware upgrade will not affect server operation if it is for iLO 2 MP firmware only. You do not need to shut down the OS to perform this upgrade.
- Upgrades system programmable hardware. This firmware upgrade will affect server operation since system power is cycled whenever system programmable hardware is upgraded.

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.

Figure 7-12 Firmware Upgrade Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

To perform a firmware upgrade, follow these steps:

1. Download the firmware from the HP Web site at: **http://www.hp.com/go/bizsupport** for IPF firmware and follow the directions.
2. Copy the firmware image file onto your own FTP server.

Table 7-9 lists the fields, buttons, and descriptions. The parameters are mandatory for a firmware upgrade.

Table 7-9 Firmware Upgrade Page Description

Fields and Button	Description
Current Firmware Revision	The version of the iLO 2 MP firmware displays.
Source IP	Enter the IP address of the FTP server where the firmware image file resides.
File Path	Enter the directory and path on the server where the firmware upgrade image resides (for example: /firmware/rx4640/example/). Do not enter the file name of the actual firmware image file into the file path parameters.
Login	Enter your username on the FTP server.
Password	Enter your password on the FTP server.
Submit	Click the **Submit** button. If the upgrade is successful, the iLO 2 MP reboots using the new firmware. If the upgrade fails, the iLO 2 MP returns to the existing state. A reason for what went wrong is provided along with instructions on what you need to do.
Cancel	Cancels the action.

Administration > Licensing

The **Licensing** page (Figure 7-13) is used to enter a license key to enable the iLO 2 MP Advanced Pack features.

Figure 7-13 Licensing Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

The iLO 2 MP offers some advanced features, which can be used only with the iLO 2 MP Advanced Pack license:

- Directory-based authentication and authorization using LDAP
- LDAP Lite schema-free integration
- Integrated Remote Console (vKVM)
- Virtual Media

Table 7-10 lists the fields, buttons, and descriptions.

Table 7-10 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 license key used to enable the iLO 2 MP Advanced Pack features. Fields are case sensitive.
Submit	Submits the key for activation.
Cancel	Cancels the action.

iLO provides a mechanism to install a license key which unlocks the advanced features. There are two types of licenses:

1. iLO 2 MP Advanced Evaluation License, a 30-day evaluation license allows usage of advanced features for 720 hours of iLO 2 MP uptime.
2. iLO 2 MP Advanced Permanent License allows perpetual use of the advanced features.

Administration > User Administration > Local Accounts

The User **Administration** page (Figure 7-14) 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 the iLO 2 MP, add new users assign rights, and modify or delete existing users. Only a user with administration access right can use this feature.

Figure 7-14 Local Accounts Page
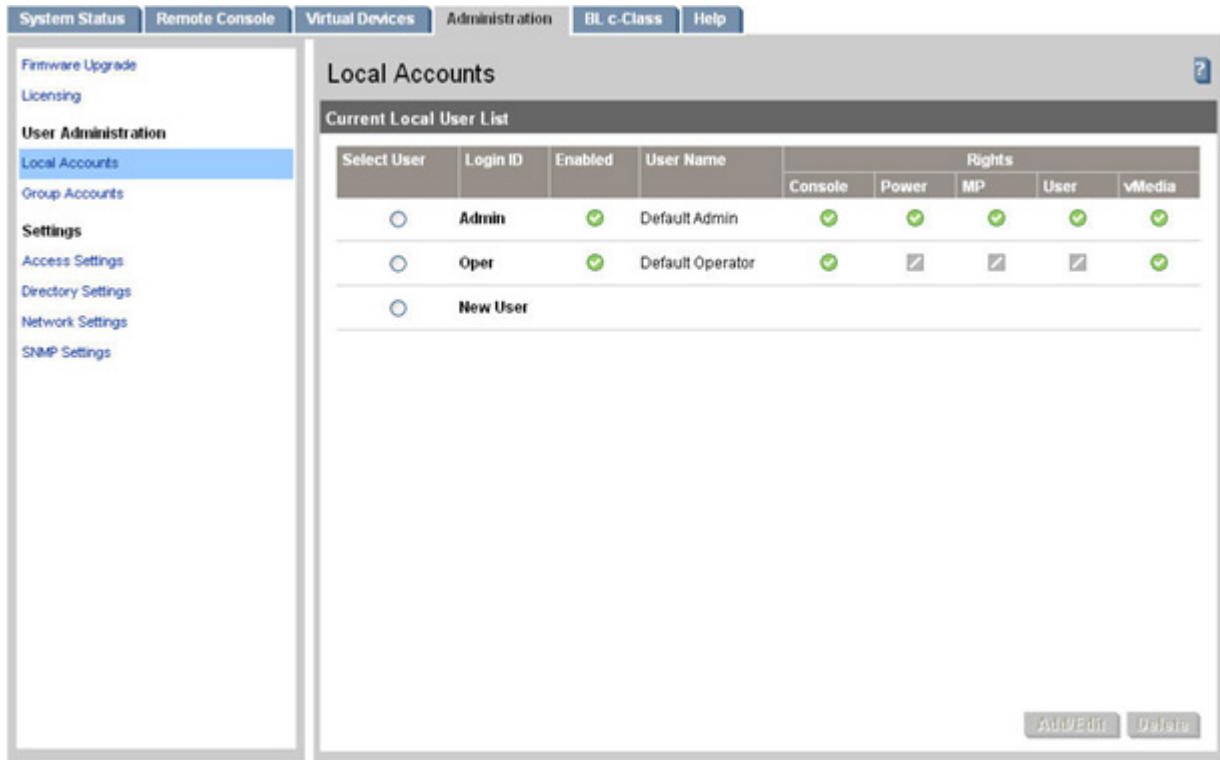
> **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

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 7-11 lists the fields and descriptions.

Table 7-11 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 rights, 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.

Administration > Group Accounts

The **Group Accounts** page (Figure 7-15) 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 the iLO 2 MP, the iLO 2 MP reads that user's directory name in the directory to determine the groups the user is a member of. The iLO 2 MP 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.

📝 **NOTE:** This feature is only available if you have the iLO 2 MP Advanced Pack license.

Figure 7-15 Group Accounts Page

📝 **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-12 lists the fields, buttons, and descriptions.

Table 7-12 Group Accounts Page Description

Fields and Buttons	Description
Administrator	Click the **Administrator** radio button and click the **Edit** button to open the **Group Settings** page and enter information.
User	Click the **User** radio button and click the **Edit** button to open the **Group Settings** page and enter information.
Custom (1,2,3,4)	Click the **Custom 1,2,3,4** radio button and click the **Edit** button to open the **Group Settings** page and enter information
Edit	The **Edit** button opens the **Group Settings** page.
Cancel	Cancels the action.

Administration > Settings > Access Settings

The **Access Settings** tab enables you to access the following pages:

- LAN
- Serial
- Login Options

Administration > Access Settings > LAN

The **LAN** page (Figure 7-16) enables you to modify LAN settings. Only a user with iLO configuration access right can use this feature.

Figure 7-16 Access Settings LAN Page

> **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-13 lists the fields, buttons, and descriptions.

Table 7-13 LAN Page Description

Fields and Buttons	Description
Telnet	You can enable or disable telnet access to the iLO 2 MP using the enable or disable option.
SSH	You can enable or disable SSH access to the iLO 2 MP using the enable or disable option.
	An industry-standard client-server connectivity protocol that provides a secure remote connection. The iLO 2 MP supports:
	- SSH2 implementation
	- Authentication algorithms RSA and DSA
	- Encryption algorithms 3DES-CBC and AES128-CBC
	- Integrity algorithms HMAC-SHA1 and MD5

Table 7-13 LAN Page Description *(continued)*

Fields and Buttons	Description
Web SSL	You can enable or disable the Web SSL access to the iLO 2 MP 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.

Administration > Settings > Serial Page

The **Serial** page (Figure 7-17) enables you to set the serial port parameters. Only a user with iLO configuration access right can use this feature.

Figure 7-17 Access Settings Serial Page

📝 **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-14 lists the fields, buttons, and descriptions.

Table 7-14 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.

Administration > Settings > Login Options Page

The **Login Option** page (Figure 7-18) enables you to modify the security options of the iLO 2 MP. Only a user with iLO configuration access right can use this feature.

Figure 7-18 Login Options Page

> **NOTE:** The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-15 lists the fields, buttons, and descriptions.

Table 7-15 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 the iLO 2 MP. The default number of password faults allowed is three.
Submit	Submits the information.
Cancel	Cancels the action.

Administration > Directory Settings > Current LDAP Parameters

The **Current LDAP Parameters** page (Figure 7-19) enables you to edit LDAP parameters. Only a user with iLO configuration access right can use this feature.

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

Figure 7-19 Current LDAP Parameters Page

📝 **NOTE:**   The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-16 lists the fields and descriptions.

Table 7-16 Current LDAP Parameters Page Description

Field	Description
Directory Authentication	Choosing enable or disable, activates or deactivates directory support on iLO 2 MP: • 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 MP 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 MP 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.

Table 7-16 Current LDAP Parameters Page Description *(continued)*

Field	Description
Distinguished Name	Distinguished Name of the iLO 2 MP, 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 the iLO 2 MP.
Submit	Submits the information.
Cancel	Cancels the action.

Administration > 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, the iLO 2 MP 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 the iLO 2 MP 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, the iLO 2 MP alerts you to manually reset the iLO 2 MP. 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.

Administration > Network Settings > Standard

The **Standard** page (Figure 7-20) enables you to configure the network settings and LAN configuration. Only a user with iLO configuration access right can configure the network settings.

Figure 7-20 Network Settings Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-17 lists the fields, buttons, and descriptions.

Table 7-17 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 MP 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 MP 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.

Administration > Network Settings > Domain Name Server

The **Domain Name Server** (DNS) page (Figure 7-21) 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. Only a user with iLO configuration access right can use this feature.

NOTE: You can only configure the DNS server if DHCP is enabled.

Figure 7-21 Domain Name Server Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-18 lists the fields, buttons, and descriptions.

Table 7-18 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.

Administration > SNMP Settings

The **SNMP Settings** page (Figure 7-22) enables you edit SNMP feature settings. Only a user with iLO configuration access right can use this feature.

Figure 7-22 SNMP Settings Page

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Table 7-19 lists the fields and descriptions.

Table 7-19 SNMP Settings Page Description

Field	Description
SNMP	Choosing **Enable** or **Disable**, activates or deactivates the SNMP feature support on this iLO 2 MP.
SNMP Alerts	**NOTE:** Currently, the SNMP alert feature is only supported on the BL860c server blade. Enter **E** to enable or **D** to disable all SNMP alerts. 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 the iLO 2 MP.

BL c-Class

The **Onboard Administrator** page (Figure 7-23) is used to facilitate the cabling and initial installation of servers blade. It also provides a quick view of the enclosure status. Only a user with configuration access right can turn the enclosure locator UID LED on or off.

NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

Before moving on to HP BladeSystem OA setup, HP recommends that you read the *HP BladeSystem Onboard Administrator User Guide* on the Web 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.

You can find other OA docs, on the Web at:

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=3709&prodSeriesId=3188465

The *HP BladeSystem Onboard Administrator User Guide* provides the following information in detail:

- Access Requirements
- Running 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

Figure 7-23 BL c-Class > Onboard Administrator

Table 7-20 lists the fields and descriptions.

Table 7-20 Onboard Administrator Page Description

Field	Description
OA IP Address	The IP address of the onboard administrator.
OA MAC Address	The MAC address of the onboard administrator.
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.

Help

The iLO 2 MP has a robust help system.

To access iLO 2 MP help, click the **Help** tab.

Figure 7-24 Help Page
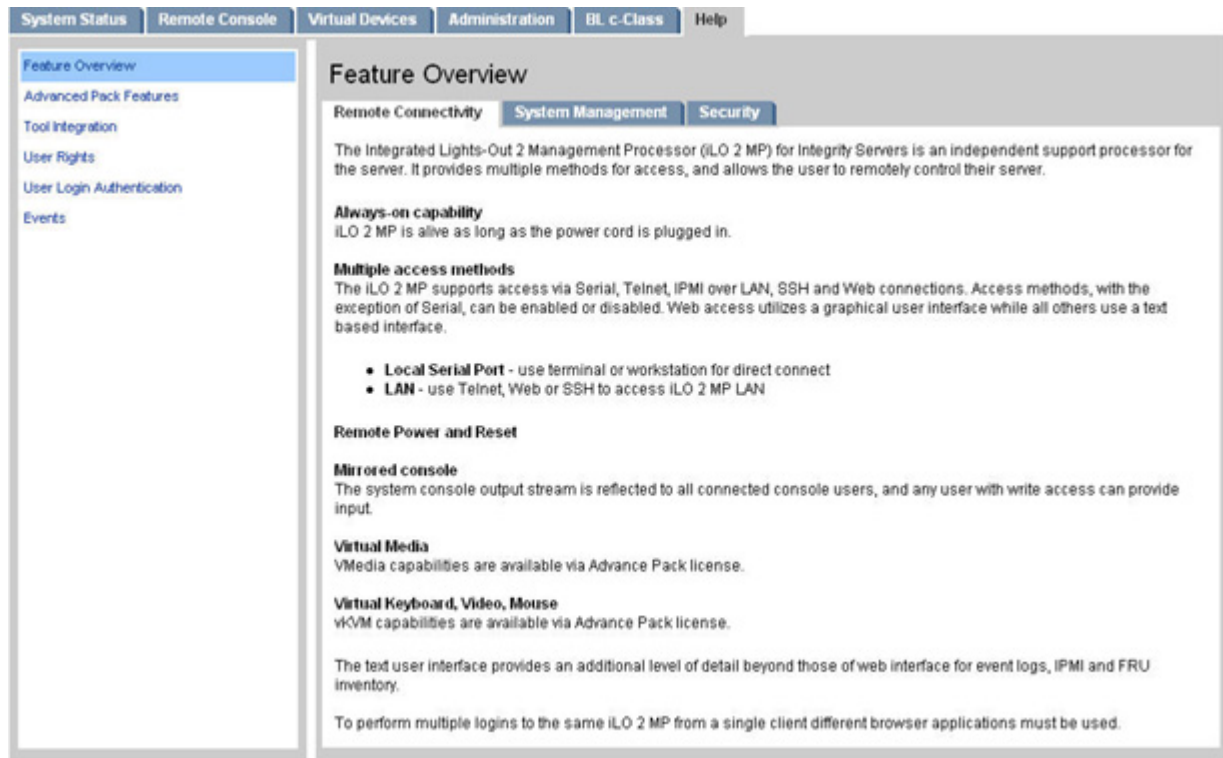
NOTE: The **BL c-Class** tab is a feature that is only available on the HP Integrity BL860c server blade.

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.

8 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.

SMASH SM CLP is not just an industry standard scripting language; it is an industry-standard command-line interface that will eventually be on all management processors, from all vendors.

In several years, HP Integrity systems will migrate to having this interface as their primary text user interface, in order to be common with usage throughout the industry.

> **IMPORTANT:** The current DMTF CLI implementation is a pre-standard release and is subject to change. At this time, SMASH SM CLP is not the primary text user interface or the primary scripting interface for the iLO 2 MP. The text user interface is the primary text interface of the iLO 2 MP. The entire text user interface of the iLO 2 MP, available on telnet and SSH, supports 100% of the MP functionality. SMASH CLP does not support all the iLO 2 MP features, and is only a prototype implementation at this point.

This chapter addresses the following topics:

SM CLP Features and Functionality Overview

CLP offers the following features:

- Provides a user-friendly method to view and manage server information with commands that are already in a format that facilitates scripting.
- Offered in addition to iLO 2 MP's existing CLI.
- Uses scripts to automate some iLO 2 MP tasks, especially when you are setting up many identical servers.
- Available from any text user interface (serial, telnet, and SSH).
- CLP sessions are independent from each other and non mirrored.
- 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 a SM CLP service are established over a transport protocol. Once the session has been 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 the iLO 2 MP. The command is received and processed by the iLO 2 MP, 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 only executed if a user has the privilege level required for that specific 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, follow these steps:

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 a SM CLP session and disconnect from the iLO 2 MP, use the `exit` command. To switch from SM CLP to the iLO 2 Main Menu interface, use the `start /map1/textredirectsap1` command.

Changing the iLO 2 Default Interface to SM CLP

iLO 2 MP 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, follow these steps.

1. At the **MP Main Menu**, enter `CM`.
2. From the `CM` prompt, enter **`SA`**.to modify iLO 2 MP 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.

```
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, you are presented with the iLO CLP prompt. Each time a command is executed, you are returned to the CLP prompt as shown in the following example.

`<current default target>hpiLO->`

Where `<current default target>` is your current target.

Each time a CLI command is executed, the output returned follows this general format:

```
</> hpiLO-> {CLPcommand}
status=0
status_tag=COMMAND COMPLETED
... command output returned...
</>hpiLO->
```

If an invalid command is entered, 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 is slightly different:

```
</> 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:

<verb> <options> <target> <properties>

Where:

- <verb> is the command verb.
- <options> are selections that affect the action, behavior, or output of the verb.
- <target> is the implicit or explicitly-identified managed element the command is directed to.
- <properties> are attributes of the target relative to the command execution.

Command Verbs

Verbs select a management action for target.

The command verbs listed in Table 8-1 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 8-1 shows the supported command verbs.

Table 8-1 Supported Command Verbs

Command	Action
cd	Change 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 executing "cd <some target>, you can shorten commands.
	For example, to find the current iLO 2 MP firmware version, you could issue the command show /map1/swinventory1/swid1. However, if you issue the cd /map1/swinventory1/swid1 command, a simple show command displays the information.
create	Create a new instance of an object.
delete	Delete an instance of a target object.

Table 8-1 Supported Command Verbs *(continued)*

Command	Action
exit	Terminates the SM CLP session.
help	Displays context sensitive help. `help` displays general help and all supported commands. `help <some verb>` displays help for that specific verb. `help <some target>` displays help for that specific target. `help <some property>` displays help for that specific property.
load	Used to move a binary image to iLO 2 MP 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 issue the `show` command with an explicit or implicit target (see "System1 Target" (page 120), "Map1 (iLO 2) Target" (page 121), "Command Targets" (page 117), for more information on implicit and explicit targets).
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 that is 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 address any of the following ways:

By using the target's absolute path

`</> hpiLO-> show /map1/telnetsvc1`

By using the target's relative path form **map1** target

`</map1> hpiLO-> show telnetsvc1`

By using implicit (current) target's with 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 multiple properties are given 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 verb and must be prefaced with '-'

Most command options have both a full name and a short form; for example:

```
show -level all orshow -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 that is 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 (ME).

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 provide the syntax used for the desired functionality:

Show information about default target and one level of contained MEs

```
</>hpiLO-> show -l 2
```

Show all contained ME

```
</>hpiLO-> show -l all
```

Show information about `system1` and all contained ME

```
</>hpiLO-> show -l all system1
```

Display Option

The display option filters the information returned in command results.

The following examples provide the syntax used for the desired functionality:

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 **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*`

Command options either require an argument or require no argument.

Table 8-2 shows the available command options.

Table 8-2 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 would prevent execution.
-help	-h	Provides command-specific help.
-level <n>	-l	Instructs MAP to execute the command for the current (specified) target plus targets contained through the specified level of depth (n).
-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 CLP must interpret the characters provided by the transport as UTF8 representation of the characters, including those in Table 8-3. They must interpret the characters according to the descriptions in Table 8-3.

Table 8-3 lists the SM CLP Reserved Characters.

Table 8-3 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 which 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 will be appended to the current line.
,	comma	Delimits items in an option argument term that is to be interpreted as a list of option arguments. Also delimits values for an option argument.
=	assignment operator	A single equals sign '=' is used to separate a property name from a desired value for the property when used with verbs which modify or create an instance. It will not have a space before or after it in an expression of a property and its value.

Table 8-3 SM CLP Reserved Characters and Character Sequences *(continued)*

Character or Sequence	Name	Description and Uses
==	equivalence operator	Two consecutive equals signs "==" without whitespace between them are used to separate a property name from a desired value when filtering instances for which results should be returned.
-	hyphen	When preceded by a space, the hyphen is the SM CLP option indicator.
/ ◎	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 an option argument term which is a comma separated list, delineates the values of an argument from the next option argument.
"	double quote	Delineates a string of text that may contain the SM CLP term separator (space) so that the SM CLP Command Processor will treat 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 is located under this target.

Table 8-4 shows **system1** target properties.

Table 8-4 system1 Properties

Property Name	Description	Access and Values
EnabledState	Provides information about the system power state.	Read only Can have the following values: Enabled: indicates that the system power is off. Disabled: indicates that the system power is on.

Verbs

- show
- help
- reset: resets the system
- start: turns system power on
- stop: performs graceful shutdown of the system

    If used with option **-force**, turns system power off

System Reset Power Status and Power Control

This section covers the system reset power status and power control commands.

System Reset

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
```

Power Status

To display the power state of the system, query the value of the enabled state property of the **system1** target. For example:

```
</>hpiLO-> show -d properties=enabledstate system1
status=0
status_tag=COMMAND COMPLETED
/system1
      Properties
      EnabledState=Enabled
```

Power 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.
```

Power 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 MP namespace. Functions and information related to iLO 2 MP is located under the **map1** target.

Table 8-5 shows **map1** target properties.

Map1 (iLO 2) Target   121

Table 8-5 map1 Properties

Property Name	Description	Access and Values
Dedicated	Value indicating whether the computer system is a special-purpose system (for example, dedicated to a particular use), versus being a general-purpose system.	Read only. The value is set to *management*.
Name	Name that identifies the iLO 2 MP.	Read only. The value is set to *iLO 2 Advanced, HP Integrity*.

Verbs

- show
- help
- reset: resets the iLO 2 MP
- load: updates iLO 2 MP firmware

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->
```

Reset iLO 2 MP Example

To reset the iLO 2 MP, issue the `reset` command to the **map1** target.

```
</>hpiLO-> reset map1
status=0
status_tab=COMMAND COMPLETED
iLO was issued a reset
```

Text Console Services (System Console, MP Menu Interface)

This section describes targets, their properties, and supported verbs necessary to implement the console services in SM CLP.

You can invoke the following text console services from SM CLP: System Console, **MP Main Menu**.

- Any text console service is represented by a dedicated to it **textredirectsap** target.
- Target /**map1/textredirectsvc1** represents iLO 2 MP's ability to provide text console redirection service.

Invoking 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 8-6 shows **textredirectsap1** target properties.

Table 8-6 /map1/textredirectsap1 Properties

Property Name	Description	Access and Values
EnabledState	Used to show if 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*. Type **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	The Name property uniquely identifies this access point.	Read only. The value is set to *MP Main Menu.*

Verbs

- cd
- help
- show
- start: switch to **MP Main Menu**

Invoking System Console Interface from SM CLP

This section provides information on how to invoke the system console interface from the SM CLP.

Target: system1/consoles1/textredirectsap1

This target represents the system text console (currently launched through the iLO 2 MP's CO command).

Table 8-7 shows **textredirectsap1** target properties.

Table 8-7 /system1/consoles1/textredirectsap1 Properties

Property Name	Description	Access and Values
EnabledState	Used to show if the test 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 *Esc*. Typing **Esc** (at the system console returns you back to the SM CLP interface (press **Esc** and press the **Shift** and **(** keys.
Description	Description of this text redirection service access point.	Read only. The value is set to *System Test Console Interface*.
Name	This property uniquely identifies this access point.	Read only. The value is set to *System Test Console*.

Verbs

- cd
- help
- show
- start: switch to system text console

Examples

The following examples provide commands used to switch between the system console and the SM CLP.

Start System Console Session

```
</>hpiLO->start /system1/consoles1/textredirectsap1
```

Find out the Session Termination Character Sequence for System Console

```
</> hpiLO-> show -d properties=SessionTerminateSequence
   /system1/consoles1/testredirectsap1
status 0
status_tag=COMMAND COMPLETED

/system1/consoles1/testredirectsap1
   Properties
      SessionTerminateSequence=Esc (
```

Exit System Console Session Back to SM CLP

Type **Esc** (at the system text console to return to the SM CLP interface (press and release the **Esc** key and press the **Shift** and **(** keys together.)

Enter MP Main Menu Interface from SM CLP

```
</>hpiLO->start /map1/textredirectsap1
```

Exit MP Menu Session back to SM CLP

SMCLP is the character sequence that switches you from the **MP Main Menu** interface back to a SM CLP session.

Firmware Revision Display and Upgrade

This section describes how to view firmware revisions in the system and perform updates using SM CLP.

- 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 MP's ability to install firmware.
- **/map1/swinventory1** represents a collection of all swid's 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 8-8 shows **swinstallsvc1** target properties.

Table 8-8   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
- help
- show

Target: map1/swinventory1

SoftwareInventory is a dedicated collection for all firmware in the system known to the iLO 2 MP.

Table 8-9 shows **swinventory1** target properties.

Table 8-9   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
- help
- show

Target: map1/swinventory1/swid#

SoftwareIdentity represents software in the system known to the iLO 2 MP (map1).

Table 8-10 shows **swid#** target properties.

Table 8-10 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
- help
- show
- load: moves an image to the iLO 2 MP

The following is a possible list of swid's in the system:

- /map1/swinventory1/swid1: represents iLO 2 MP 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

Firmware Revision Display

This example displays only the iLO 2 MP 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 MP. The latest firmware can be found on the HP Web site at:

http://www.hp.com/servers/lights-out

The following examples show how to update the iLO 2 MP firmware version:

Command format: `load -source <URL>[<target>]`

<URL>example: protocol://username:password@hostIP/filename

- The **protocol** field is mandatory and must be ftp.
- The **username:password** field is optional (if it is omitted, anonymous ftp is used).
- The **hostIP** field is mandatory; this is the IP address of the ftp server where the upgrade files are located.
- The **filename** field is mandatory; this is the upgrade files directory path.

📝 **NOTE:**   The SM CLP only performs a cursory syntax verification of the <URL> value. Visually ensure the <URL> is valid.

Currently, the firmware profile enables the load verb to target either an actual device itself or the `swid` of that device. For instance, if swid1 represents iLO 2 MP firmware, use the following command:

```
load -source ftp://192.0.2.1/MPFW_E0301 /map1
```

or

```
load -source ftp://192.0.2.1/MPFW_E0301 /map1/swinventory1/swid1
```

Upgrade iLO 2 MP firmware from an ftp server (username/password provided)

```
hpiLO-> load -source ftp://john:abc123@5.111.111.1/MPFW_E0201 map1
```

Remote Access Configuration (Telnet, SSH)

The iLO 2 MP 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 the iLO 2 MP.

Target: map1/telnetsvc1

The **telnetsvc1** target represents the telnetsvc service provided by **map1**.

Table 8-11 shows **telnetsvc1** target properties.

Table 8-11 telnetsvc1 Properties

Property Name	Description	Access and Values
EnabledState	Used to show if telnet is enabled or disabled.	Read only. Can have the following values: Enabled, Disabled
Protocol	The protocol this service provides.	Read only. The value is set to *telnet*

Verbs

- start: enables iLO 2 MP telnet service
- stop: disables iLO 2 MP telnet service
- show
- help

Telnet Examples

The following examples provide 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 the iLO 2 MP.

Target: map1/sshsvc1

The **sshsvc1** target represents the SSH service provided by **map1**.

Table 8-12 shows **sshsvc1** target properties.

Table 8-12 sshsvc1 Properties

Property Name	Description	Access and Values
EnabledState	Used to show if SSH service is enabled or disabled.	Read only. Can have the following values: Enabled, Disabled
Protocol	The protocol this service provides.	Read only. The value is set to *SSH*.

Verbs

- start: enables iLO 2 MP SSH service
- stop: disables iLO 2 MP SSH service
- show
- help

SSH Examples

The following examples provide 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

This section describes targets, target properties, and supported verbs necessary to implement the iLO 2 MP network configuration through SM CLP.

Target: map1/enetport1

The **enetport1** target represents capabilities and management of the iLO 2 MP Ethernet port.

Table 8-13 shows **enetport1** target information.

Table 8-13 enetport1 Properties

Property Name	Description	Access and Values
AutoSense	Specified if the iLO 2 MP Autosense feature is enabled. If it is disabled, iLO 2 MP network speed is set to 10 mbs/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
- help
- show
- set

Target: map1/enetport1/lanendpt1

The **lanendpt1** target represents the iLO 2 LAN endpoint settings.

Table 8-14 shows **lanedpt1** target properties.

Table 8-14 lanedpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the iLO 2 MP LAN state.	Read only. Can have the following 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
- help
- show

Target: map1/enetport1/lanendpt1/ipendpt1

The **ipendpt1** target represents the iLO IP endpoint settings.

Table 8-15 shows **ipendpt1** target properties.

Table 8-15 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	Used to indicate the configuration method which resulted in the configuration being assigned to this ipendpt.	Read only. Can have the following 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
- help
- show
- set

Target: map1/dhcpendpt1

The **dhcpendpt1** target represents the iLO 2 MP DHCP client.

Table 8-16 shows **dhcpendpt1** target properties.

Table 8-16 dhcpendpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the state of iLO 2 MP DHCP.	Read only. Can have the following values: Enabled: the iLO 2 MP DHCP client is enabled. Disabled: the iLO 2 MP DHCP client is disabled.
OtherTypeDescription	Textual description of this protocol endpoint.	Read only. The value is set to *DHCP*.

Verbs

- cd
- help
- show
- start: Enables iLO 2 MP DHCP
- stop: Disables iLO 2 MP DHCP

Target: map1/dnsendpt1

The **dnsendpt1** target represents the iLO 2 MP DNS client.

Table 8-17 shows **dnsendpt1** target properties.

Table 8-17 dnsendpt1 Properties

Property Name	Description	Access and Values
EnabledState	Represents the state of iLO 2 MP DNS.	Read only Can have the following values: Enabled: the iLO 2 MP DNS client is enabled. Disabled: the iLO 2 MP DNS client is disabled.
Hostname	Represents the host name currently assigned to the iLO 2 MP.	Read only. iLO 2 MP's current host name.
OtherTypeDescription	Textual description of this protocol endpoint.	Read only. The value is set to *DNS*.

Verbs

- cd
- help
- show

Target: map1/enetport1/lanendpt1/ipendpt1/gateway1

The **gateway1** target represents the gateway server.

Table 8-18 shows **gateway1** target properties.

Table 8-18 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. The value is set to *default gateway*.

Target: map1/dnsserver1, map1/dnsserver2, map1/dnsserver3

The **dnsserver1**, **dnsserver2**, and **dnsserver3** targets represent the iLO 2 MP's primary, secondary, and tertiary DNS servers respectively.

Table 8-19 shows **dnsserver1**, **dnsserver2**, and **dnsserver3** target properties

Table 8-19 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. The value is set to *DNS server*.

Verbs

- show
- help
- set

Target: map1/settings1/dnssettings1

The **dnssettings1** target contains iLO 2 MP DNS settings.

Table 8-20 shows **dnssettings1** target properties.

Table 8-20 dnssettings1 Properties

Property Name	Description	Access and Values
DNSServerAddress	Contains IP address 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 MP Domain name	Read/write
RegisterThisConnections Address	Indicates whether iLO 2 MP registers with the DDNS server.	Read/write. Can have the following values: Yes: register with DDNS server No: do not register with DDNS server
RequestedHostName	iLO 2 MP host name.	Read/write.

Verbs

- cd
- help
- show
- set

Network Examples

The following examples provide specific network commands.

Determine iLO 2 MP's 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=192.0.2.1
```

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
```

User Accounts Configuration

This section describes targets, their properties, and supported verbs used for configuring and viewing iLO 2 MP user accounts using SM CLP.

Target: map1/group1

The **group1** target represents a collection of user accounts on this iLO 2 MP.

Table 8-21 shows **group1** target information.

Table 8-21 group1 Properties

Property Name	Description	Access and Values
Description	Textual description of this collection target.	Read only. The value is set to *collection of user accounts*.

Verbs

- cd
- help
- show

Target: map1/group1/account#

The **account#** target represents a user account on this iLO 2 MP (where # is the instance number of the specific account). You can configure up to 19 user accounts on the iLO 2 MP.

Table 8-22 shows **account#** target properties.

Table 8-22 account# Properties

Property Name	Description	Access and Values
UserID	Login name of this user account.	Read/write. UserID can be specified in ASCII characters up to 24 characters long.
UserPassword	User password.	Read/write. UserPassword can be specified in ASCII characters and has to be least six characters long.
Name	User name of this account.	Read/write. UserID can be specified in ASCII characters up to 24 characters long.
oemhp_privileges	Privileges of this user account.	Read/write. Valid values are: <console,power,mp,user,virtual), <all> or <none>.

Verbs

- cd
- help
- show
- set
- create: create a new user account
- delete: delete a user account

User Account Examples

The following examples provide specific user account commands.

Display all user accounts on this iLO 2 MP

```
</> 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 MP 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 MP Web GUI or the iLO 2 MP **Command** menu.

Target: map1/settings1/oemhp_ldapsettings1

The **oemhp_ldapsettings1** target represents iLO 2 MP LDAP directory configuration settings.

Table 8-23 shows **oemhp_ldapsettings1** target information.

Table 8-23 oemhp_ldapsettings1 Properties

Property Name	Description	Access and Values
oemhp_dirauth	Represents the iLO 2 MP 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 MP user accounts. Disabled: disable local iLO 2 MP 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 MP 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
- help
- show
- set

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 iLO2 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 Directory Services Installation and Configuration

You can install and configure the iLO 2 MP directory services to leverage the benefits of a single point of administration for the iLO 2 MP user accounts.

This chapter provides information on the features and functions, installation, and configuration of the iLO 2 MP directory services.

This chapter addresses the following topics:

- "Directory Services" (page 137)
- "Directory Services for Active Directory" (page 141)
- "Directory Services for eDirectory" (page 152)
- "User Login Using Directory Services" (page 161)
- "Certificate Services" (page 162)
- "Directory-Enabled Management" (page 163)
- "Directory Services Schema (LDAP)" (page 169)

Directory Services

The following are benefits of directory integration:

- Scalability: The directory can be leveraged 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. A change at a single role then applies to all users and the iLO 2 MP devices associated with that role.
- Single point of administration: You can use native administrative tools, like Microsoft Management Console (MMC) and ConsoleOne, to administrate the iLO 2 MP users.
- Immediacy: A single change in the directory rolls out immediately to associated iLO 2 MPs. This eliminates the need to script this process.
- Reuse of username 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 the iLO 2 MP.
- Flexibility: You can create a single role for a single user on a single iLO 2 MP, you can create a single role for multiple users on multiple iLO 2 MPs, or you can use a combination of roles — whatever is suitable for your enterprise.
- Compatibility: iLO 2 MP directory integration applies to the iLO 2 MP products. The integration supports the popular directories Active Directory and eDirectory.
- Standards: iLO 2 MP directory support builds on the LDAP 2.0 standard for secure directory access.

Features Supported by Directory Integration

The iLO 2 MP directory services functionality enables you to:

- 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 the iLO 2 MP and iLO 2 MP users.

Installing directory services for the iLO 2 MP requires extending the directory schema. A schema administrator must complete extending the schema.

The local user database is retained. You can decide not to use directories, use a combination of directories and local accounts, or use directories exclusively for authentication.

Installation Prerequisites

Follow these steps before installing directory services:

- Obtain an iLO 2 MP Advanced Pack license.
- Configure LDAP.

Installing Directory Services

To successfully enable directory-enabled management on any iLO 2 MP, complete the following steps:

1. Plan

   Review the following sections:

   - "Directory Services" (page 137).
   - "Directory Services Schema (LDAP)" (page 169).
   - "Directory-Enabled Management" (page 163).

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 Web site (http://www.hp.com/servers/lights-out).

   b. Run the schema installer ("Schema Installer" (page 139)) once to extend the schema.

   c. Run the management snap-in installer ("Management Snap-In Installer" (page 141)) and install the appropriate snap-in for your directory service on one or more management workstations.

3. Update

   a. Flash the ROM (Upgrade the iLO 2 MP Firmware) on the iLO 2 MP with the directory-enabled firmware.

   b. Set directory server settings and the distinguished name of the iLO 2 MP objects on the Directory Settings in the iLO 2 MP user interface.

4. Manage

   a. Create a management device object and a role object ("Directory Services Objects" (page 147)) using the snap-in.

   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 on managing the directory service, see "Directory-Enabled Management" (page 163). Examples are available in "Directory Services for Active Directory" (page 141) and "Directory Services for eDirectory" (page 152).

Schema Documentation

To assist with the planning and approval process, HP provides documentation on 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 169).

Directory Services Support

The iLO 2 MP 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 MP 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. This solution makes no distinction between eDirectory running on NetWare, Linux, or Windows. To spawn an eDirectory schema extension requires Java® 1.4.2 or later for SSL authentication.

The iLO 2 MP supports Microsoft Active Directory running on one of the following operating systems:

- Windows 2000 family
- Windows Server 2003 family

The iLO 2 MP 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 the iLO 2 MP uses LDAP over SSL to communicate with the directory servers. The iLO 2 MP software is designed to install in an 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*

Installing directory services for the iLO 2 MP requires extending the eDirectory schema. An administrator must complete extending the schema.

Schema Required Software

The iLO 2 MP requires specific software, which extends the schema and provides snap-ins to manage the iLO 2 network. An HP Smart Component is available for download that contains the schema installer and the management snap-in installer. You can download the HP Smart Component from the HP Web site at: **http://www.hp.com/servers/lights-out**.

Schema Installer

Bundled with the schema installer are one or more .xml files. 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 installer includes three important screens:

- Schema Preview
- Setup
- Results

Schema Preview

The **Schema Preview** screen (Figure 9-1) enables you to view the proposed extensions to the schema. This screen reads the selected schema files, parses the XML, and displays it as a tree view. It lists all of the details of the attributes and classes that are installed.
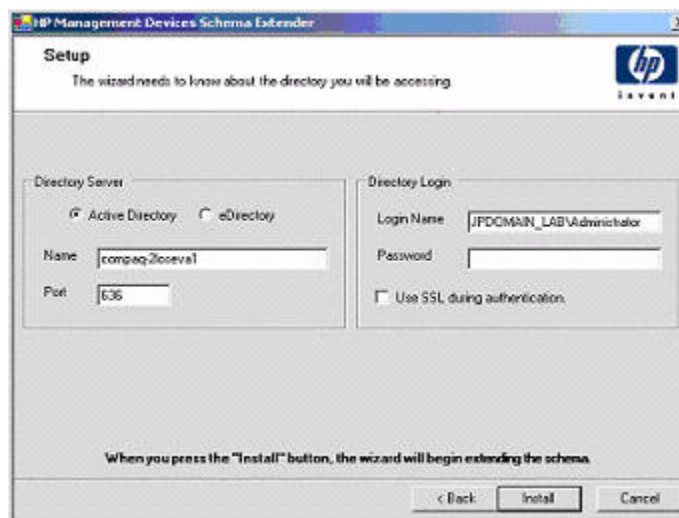
Figure 9-1 Schema Preview Screen
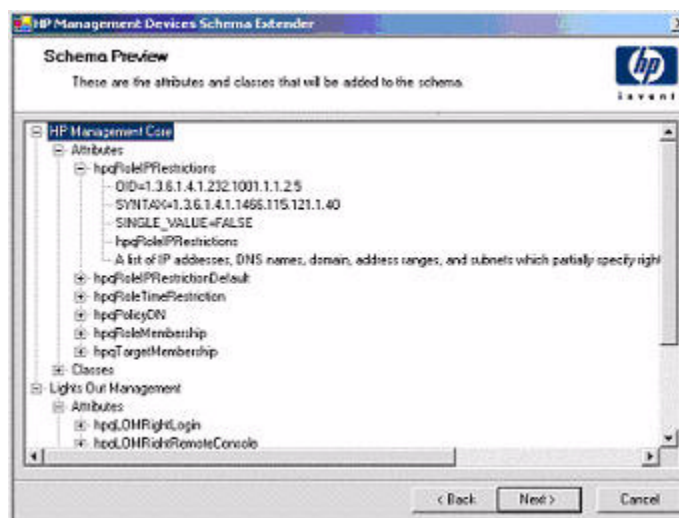
Setup

Use the **Setup** screen (Figure 9-2) to enter the appropriate information before extending the schema.

Figure 9-2 Schema Setup Screen

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: Extending the schema on active directory requires that you are an authenticated schema administrator, that the schema is not write protected, and that the directory is 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 get write access to the schema on Windows 2000 requires a change to the registry safety interlock. If you select the **Active Directory** option, the schema extender attempts to make the registry change. It will only succeed if you have rights to do this. 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. These 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

The **Results** screen (Figure 9-3) displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Figure 9-3 Schema Results Screen
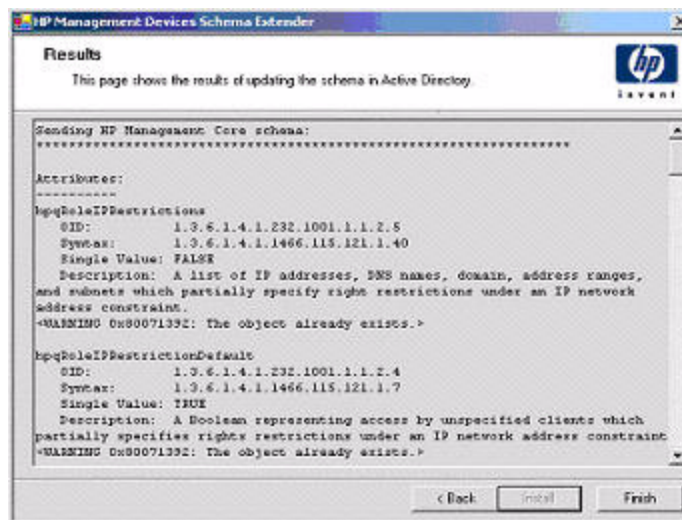
Management Snap-In Installer

The management snap-in installer installs the snap-ins required to manage the iLO 2 MP objects in a Microsoft Active Directory Users and Computers directory or in a Novell ConsoleOne directory.

To create an iLO 2 MP directory using iLO 2 MP snap-ins, perform the following tasks:

• Create and manage the iLO 2 MP and role objects.
• Make the associations between iLO 2 MP 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 the iLO 2 MP on the HP Web site at:
http://h18004.www1.hp.com/support/files/lights-out/us/index.html.

The following sections provide installation prerequisites, preparation, and a working example of directory services for active directory.

Active Directory Installation Prerequisites

Following are prerequisites for installing Active Directory:

- The Active Directory must have a digital certificate installed to enable the iLO 2 MP to connect securely over the network.
- The Active Directory must have the schema extended to describe the iLO 2 MP object classes and properties.
- The iLO 2 MP firmware must be Version F.01.57 or later.
- The iLO 2 MP advanced features must be licensed.

Directory services for the iLO 2 MP 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:** Installing directory services for the iLO 2 MP requires extending the active directory schema. You must be an active directory schema administrator to complete extending the schema.

- Extending the schema in the Microsoft Windows 2000 Server Resource Kit, available at: **http://msdn.microsoft.com**.
- Installing active directory in the Microsoft Windows 2000 Server Resource Kit, available at: **http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit**/.
- 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*.

The iLO 2 MP requires a secure connection to communicate with the directory service. This requires the installation of the Microsoft CA. For more information, see the following Microsoft technical references:

- Appendix D—Configuring Digital Certificates on Domain Controllers for Secure LDAP and SMTP Replication at:
  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp
- Microsoft Knowledge Base Article 321051: How to Enable LDAP over SSL with a Third-Party Certification Authority.

Directory Services Preparation for Active Directory

To set up directory services for use with the iLO 2 MP, follow these steps:

1. Install Active Directory. For more information, see Installing Active Directory in the Microsoft Windows 2000 Server Resource Kit.
2. Install the Microsoft Admin Pack (the ADMINPAK.MSI file, which is located in the i386 subdirectory of the Windows 2000 Server or Advance 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 if you have sufficient rights. You can also do this by setting

HKEY_LOCAL_MACHINE SYSTEM CurrentControlSet Services NTDS Parameters Schema Update Allowed in the registry to a non-zero value (see the "Order of Processing When Extending the Schema" section of Installation of Schema Extensions in the Windows 2000 Server Resource Kit) or by doing the following (This step is not necessary if you are using Windows Server 2003.):

> ⚠ **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.

    a.   Start MMC.
    b.   Install the Active Directory Schema snap-in in MMC.
    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 to create a certificate or install Certificate Services because the iLO 2 MP communicates with Active Directory using SSL. Install Active Directory before installing Certificate Services.

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, which contains the installers for the schema extender and the snap-ins. You can download the Smart Component from the HP Web site at: **http://www.hp.com/servers/lights-out**.

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 will run 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 Web site at: **http://www.microsoft.com**.

Snap-In Installation and Initialization for Active Directory

Follow these steps to install the snap-ins and configure the directory service:

1. Run the snap-in installation application to install the snap-ins.
2. Configure the directory service to have the appropriate objects and relationships for the iLO 2 MP management:
    a. Use the management snap-ins from HP to create the iLO 2 MP, policy, admin, and user role objects.
    b. Use the management snap-ins from HP to build associations between the iLO 2 MP object, the policy object, and the role object.
    c. Point the iLO 2 MP object to the admin and user role objects (admin and user roles automatically point back to the iLO 2 MP object).

    For more information on iLO 2 MP objects, see "Directory Services Objects" (page 147).

At a minimum, create:
- One role object that contains one or more users and one or more iLO 2 MP objects.
- One iLO 2 MP object corresponding to each iLO 2 MP that is 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 LDAP Lite.

Assume that a company has an enterprise directory including the domain mpiso.com, arranged as shown in Figure 9-4.

Figure 9-4 Directory Example
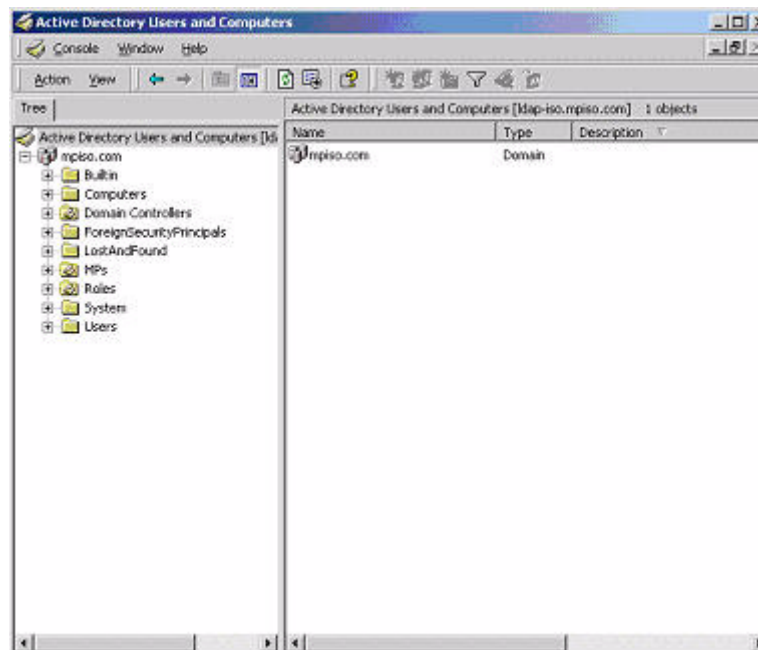
1. Create an organizational unit to contain the iLO 2 devices managed by the domain. In this example, two organizational units are created, called Roles and MPs.
2. Use the HP provided Active Directory Users and Computers snap-ins to create iLO 2 objects in the MPs organizational unit for several iLO 2 devices.

a. Right-click the **MPs** organizational unit found in the mpiso.com domain, and select **NewHPObject**.

b. Select **Device** for the type in the **Create New HP Management Object** dialog box (Figure 9-5).

Figure 9-5 Create New HP Management Object Dialog Box
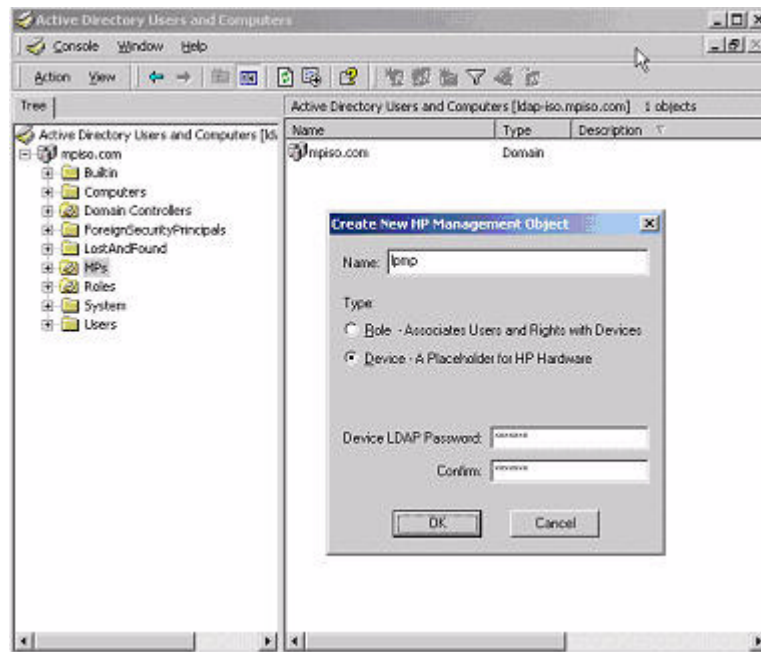
c. Enter an appropriate name in the **Name** field of the dialog box. In this example, the DNS host name of the iLO 2 device, lpmp, is used as the name of the iLO 2 object, and the surname is iLO 2.

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**.

a. Select **Role** for the type field in the **Create New HP Management Object** dialog box.

b. Enter an appropriate name in the **Name** field of the dialog box. In this example, the role contains users trusted for remote server administration and is called **remoteAdmins**. Click **OK**.

c. Repeat the process, creating a role for remote server monitors called **remoteMonitors**.

5. Use the HP provided Active Directory Users and Computers snap-ins to assign the roles rights, and associate the roles with users and devices.

a. Right-click the **remoteAdmins** role in the Roles organizational unit in the mpiso.com domain, and select **Properties**.

b. Select the **HP Devices** tab and click **Add**.

c. Using the **Select Users** dialog box (Figure 9-6), select the iLO 2 object created in step 2: **lpmp** in folder mpiso.com/MPs. Click **OK** to close the dialog.

Figure 9-6 Select Users Dialog Box
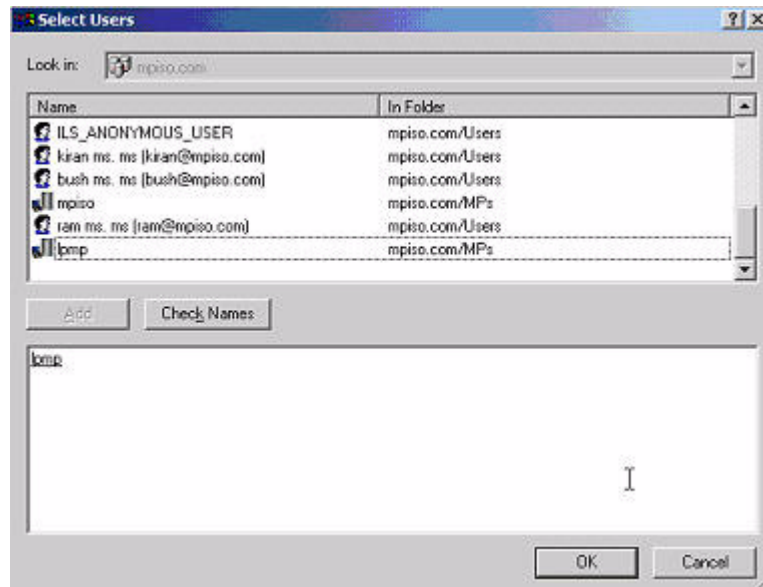
d. Click **Apply** to save the list.

Add users to the role. Click the **Members** tab, and add users using the **Add** button and the **Select Users**dialog box. The devices and users are now associated.

6. Use the **Lights Out Management** tab to set the rights for the role. All users and groups within a role have the 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. Click the checkboxes next to each right and click **Apply**.

Figure 9-7 Lights-Out Management Tab
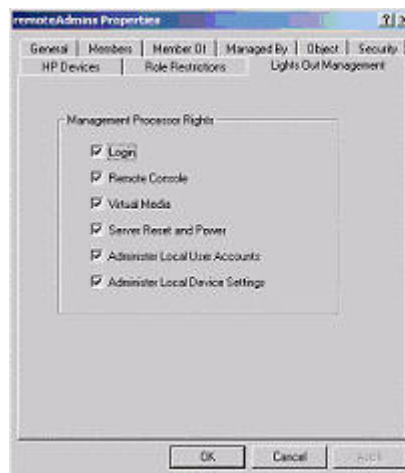
7. Click **OK** to close the property sheet.
8. Using the same procedure as in step 4, edit the properties of the remoteMonitors role, add the lpmp device to the Managed Devices list on the **HP Devices** tab, and add users to the remoteMonitors role using the **Members** tab.

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 in both the remoteAdmins and remoteMonitors roles, he or she has all the rights, because the remoteAdmins role has those rights.

To configure iLO 2 and associate it with an iLO 2 object used in this example, use settings similar to the following on 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, to gain access, user Mel Moore (with the unique ID MooreM, located in the Users organizational unit within the mpiso.com domain, who is also a member of one of the remoteAdmins or remoteMonitors roles) would be allowed to log in to the iLO 2. 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 the managed device and user or groups already contained within the directory service. User management of iLO 2 requires three basic objects in the directory service:

- iLO 2 object
- Role object
- User objects

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 show the new entries.

After the snap-in is installed, you can create iLO 2 objects and iLO 2 roles in the directory. Using the Users and Computers tool, you can:

- Create iLO 2 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 within Active Directory Users and Computers after you have installed the HP snap-ins.

Managing HP Devices Within a Role

Use the **HP Devices** tab (Figure 9-8) to add the HP devices to be managed within a role. T
- o 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**.
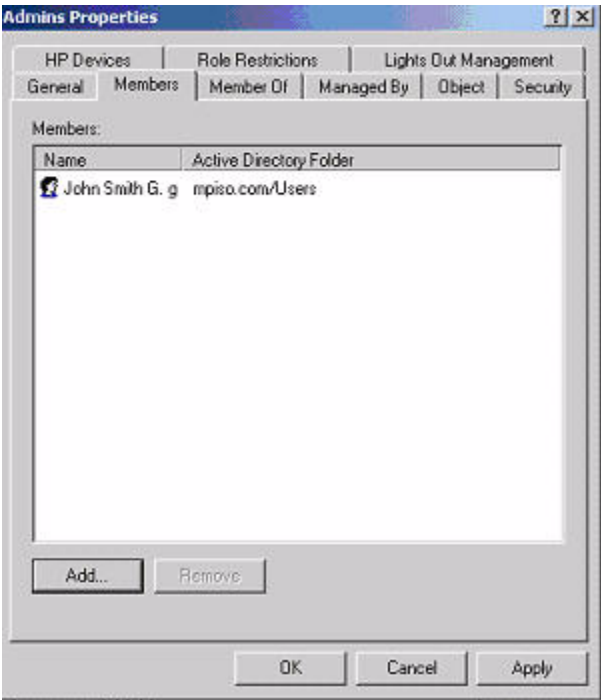
Figure 9-8 HP Devices Tab
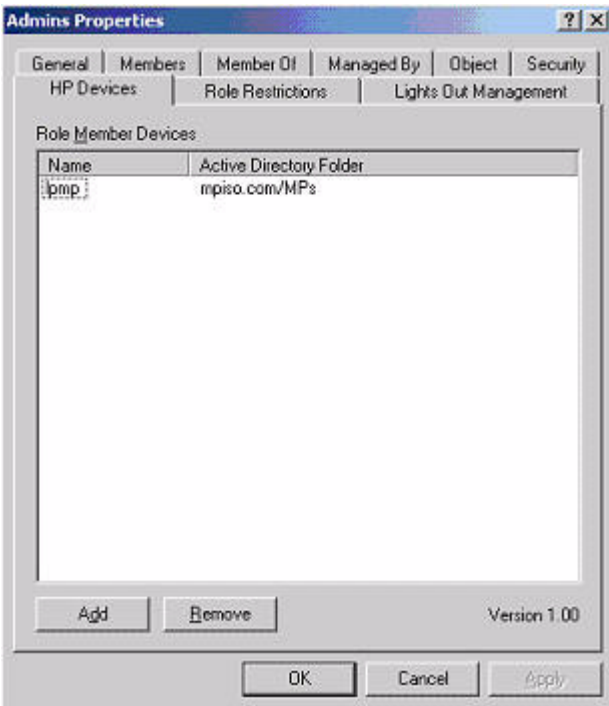
Managing Users Within a Role

After user objects are created, use the **Members** tab (Figure 9-9) to manage the users within the role. T

- o browse to the specific user you want to add, click **Add**.
- To remove a user from the list of valid members, highlight an existing user and click **Remove**.
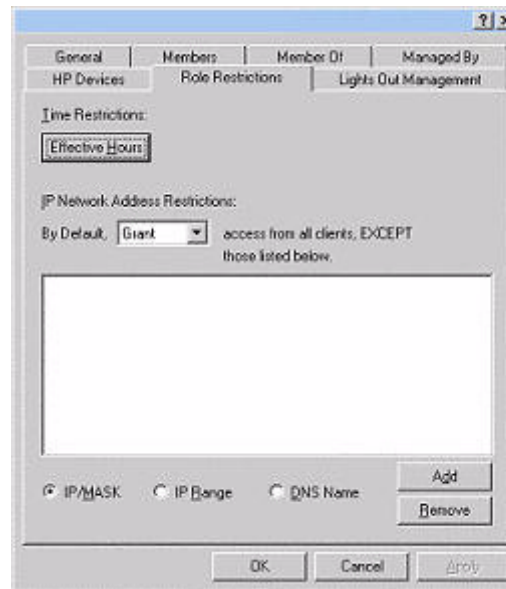
Figure 9-9 Members Tab

Setting Login Restrictions

The **Role Restrictions** subtab (Figure 9-10) enables you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
  - DNS Name

Figure 9-10 Role Restrictions Subtab

Setting Time Restrictions

- To manage the hours available for login by members of the role, click the **Effective Hours** button.
- To select the times available for login for each day of the week in half-hour increments, use the **Logon Hours** pop-up window (Figure 9-11). 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.

Figure 9-11 Logon Hours Pop-up Window
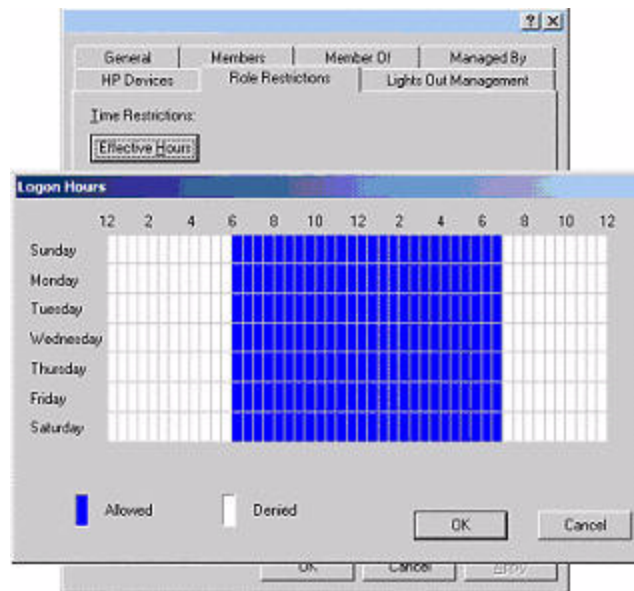
- Use the default setting to allow access at all times.

Defining Client IP Address or DNS Name Access

You can grant or deny access to an IP address, IP address range, or DNS names.

In the **By Default** drop-down menu, select whether to grant 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** tab and click **Add**. The **New IP/Mask Restriction** pop-up window opens (Figure 9-12).

Figure 9-12 New IP/Mask Pop-up Window
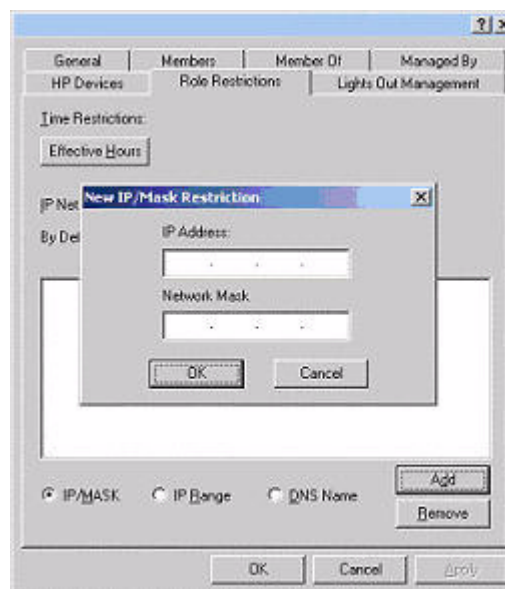
2. In the **New IP/Mask Restriction** pop-up window, enter the information and click **OK**.
3. The **DNS Name** option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com. Select

DNS Name in the **Role Restrictions** tab and click **Add**. The **New DNS Name Restriction**
pop-up window opens.

4. Enter the information and click **OK.**
5. Click **OK** to save the changes.

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 the role. You can make users and group objects
members of the role, giving the users or group of users the rights granted by the role. Use the
Lights Out Management tab (Figure 9-13) to manage rights.

Figure 9-13 Lights Out Management Tab
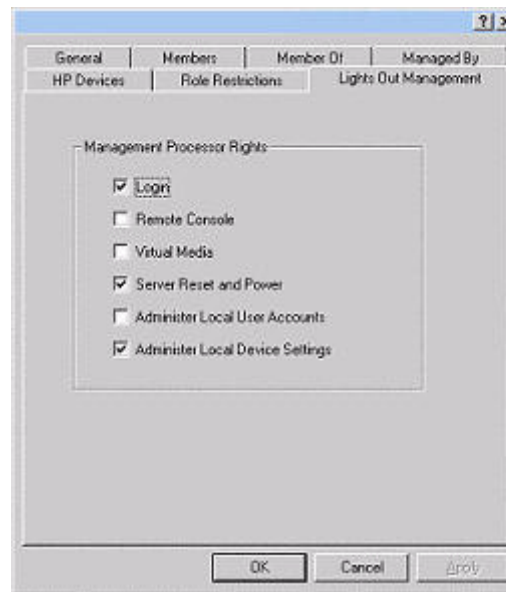
The available rights are:

Table 9-1 Lights Out Management Tab Description

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 the iLO 2 MP or the system.
Remote Console	This option enables you to access the system console (the host OS).
Virtual Media	This option enables you to connect devices such as CD/DVD and network drives as virtual devices through the network.
Server Reset and Power	This option enables you to execute iLO 2 MP 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 you to administer local iLO 2 MP user accounts.
Administer Local Device Settings	This option enables you to administer local device settings.

Directory Services for eDirectory

The following sections provide installation prerequisites, preparation, and a working example of directory services for eDirectory.

NOTE: LDAP Lite is not supported with eDirectory.

Snap-In Installation and Initialization for eDirectory

See "Snap-In Installation and Initialization for Active Directory" (page 143) for instructions on using the snap-in installation application.

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 MP Devices in eDirectory

The following example shows how to set up roles and HP devices in a company called samplecorp, which consists of two regions: region1 and region2.

Assume samplecorp has an enterprise directory arranged according to the Figure 9-14.

Figure 9-14 Roles and Devices Example
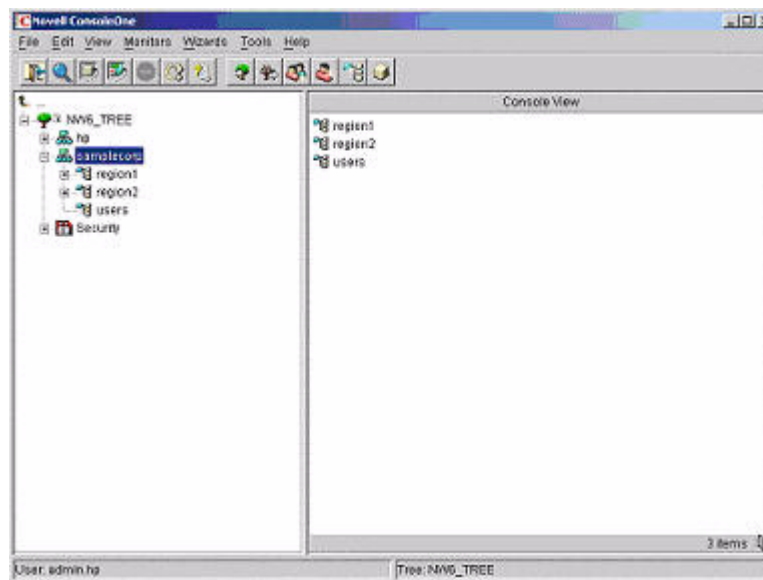
Begin by creating organizational units in each region to contain the iLO 2 MP devices and roles specific to that region. In this example, two organizational units are created, called roles and HP devices, in each organizational unit (region1 and region2).

Creating Objects

To create iLO 2 MP objects, follow these steps:

1. Use the HP provided ConsoleOne snap-ins to create iLO 2 MP objects in the HP devices organizational unit for several iLO 2 MP devices.
2. Right-click the **HP devices** organizational unit, found in the region1 organizational unit, and 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 MP device, rib-email-server is used as the

name of the iLO 2 MP object, and the surname is RILOEII (iLO 2 MP). Click **OK**. The **Select Object Subtype** dialog box (Figure 9-15) opens.

Figure 9-15 Select Object Subtype Dialog Box
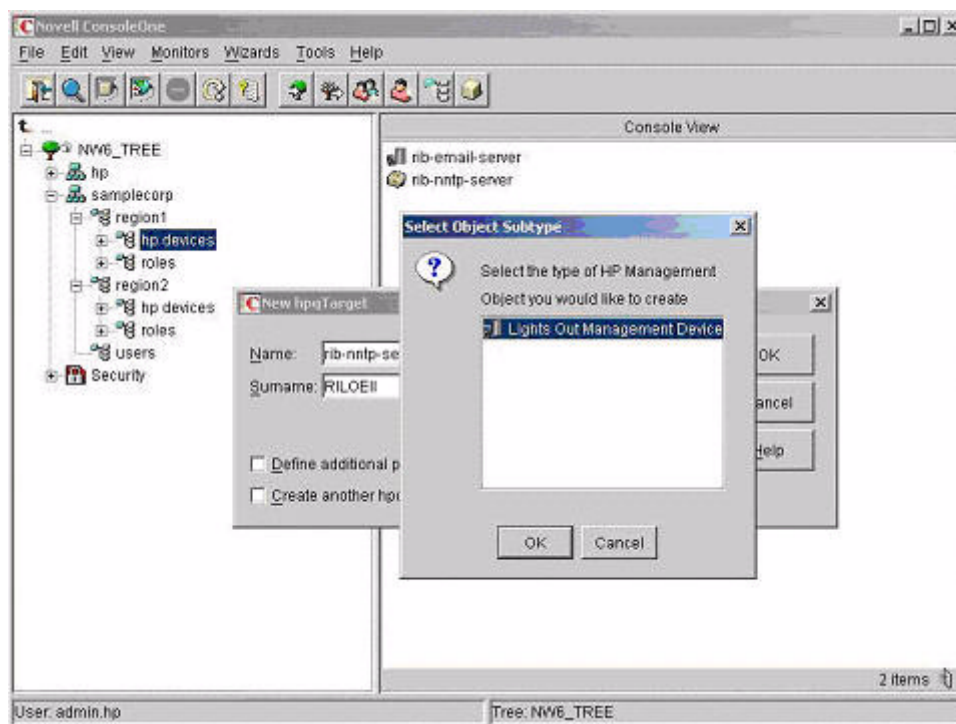
c.   Select **Lights Out Management Device** from the list, and click **OK**.

d.   Repeat the process for several more iLO 2 MP devices with 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, follow these steps:

1.   Use the HP provided ConsoleOne snap-ins to create HP role objects in the roles organizational units.

a.   Right-click the **roles** organizational unit, found in the region2 organizational unit, and 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. Click **OK**. The **Select Object Subtype** dialog box opens.

d.   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 roles in region1, and a remoteAdmins and a remoteMonitors role in roles in region2.

3.   Use the HP provided ConsoleOne snap-ins 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 MP objects created in step 2. Click **OK** and click **Apply**.

d. Next, add users to the role. Click the **Members** tab, and add users using the **Add** button and the **Select Object** dialog box. The devices and users are now associated.

e. Use the **Lights Out Management Device Rights** subtab of the **HP Management** tab (Figure 9-16) to set the rights for the role.

Figure 9-16 Setting Role Rights
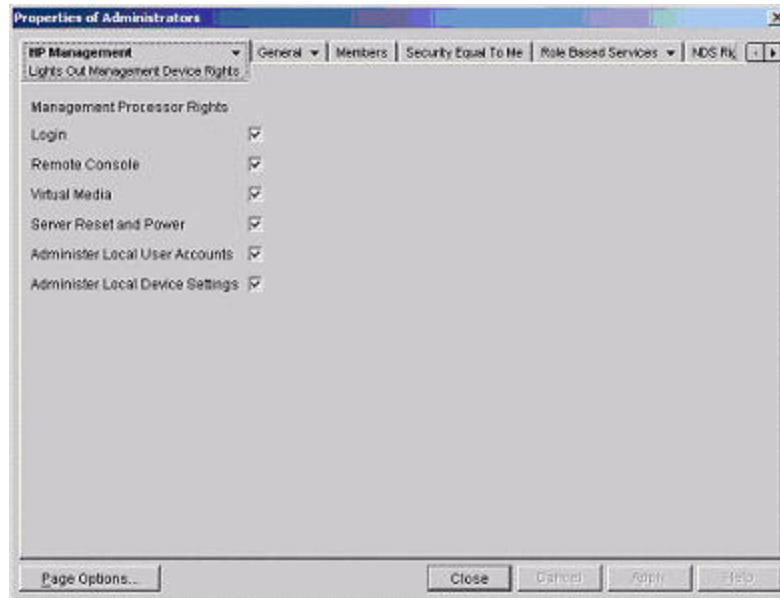
All users within a role will have the rights assigned to the role on all of the iLO 2 MP devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the iLO 2 MP functionality. Select the boxes next to each right, and click **Apply**.

f. Click **Close** to close the property sheet.

4. Using the same procedure as in step 3, edit the properties of the remoteMonitors role:

a. Add the three iLO 2 MP 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 able to authenticate and view the server status.

User rights to any iLO 2 MP 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 MP device is a managed device. Following the preceding examples, if a user is in both the remoteAdmins and remoteMonitors roles, he or she will have all the rights, because the remoteAdmins role has those rights.

To configure an iLO 2 MP device and associate it with an iLO 2 MP object used in this example, use settings similar to the following on the iLO 2 MP directory settings text user interface.

📝 **NOTE:** Use commas, not periods, in LDAP Distinguished Names 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 the iLO 2 MP. He would type csmith (case insensitive) in the **Login Name** field of the iLO 2 MP login and use his eDirectory password in the **Password** field to gain access.

Directory Services Objects for eDirectory

Directory services objects enable virtualization of the managed devices and the relationships between the managed device and 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 9-17) to add the HP devices to be managed within a role.

Figure 9-17 Role Managed Devices Subtab
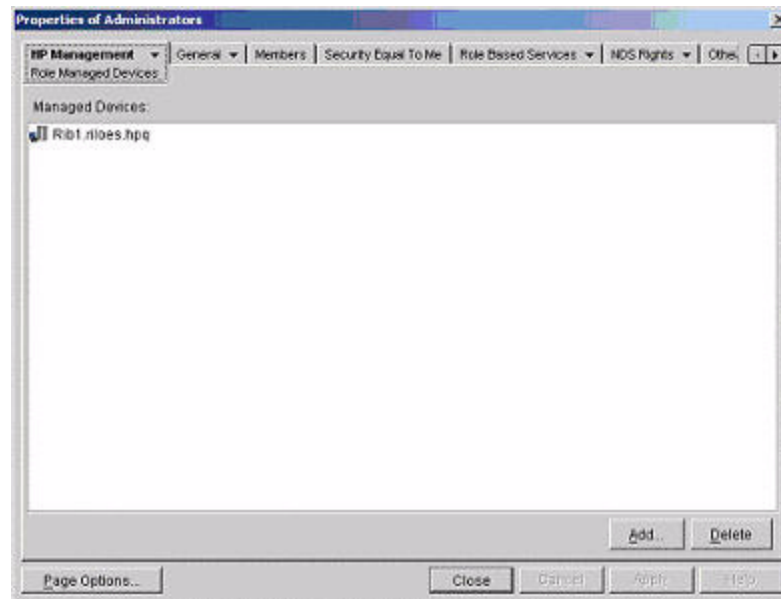
To browse to the specific HP device and add it as a managed device, click **Add**.

Adding Members

After you create user objects, use the **Members** tab (Figure 9-18) to manage the users within the role.

Figure 9-18 Members Tab (eDirectory)
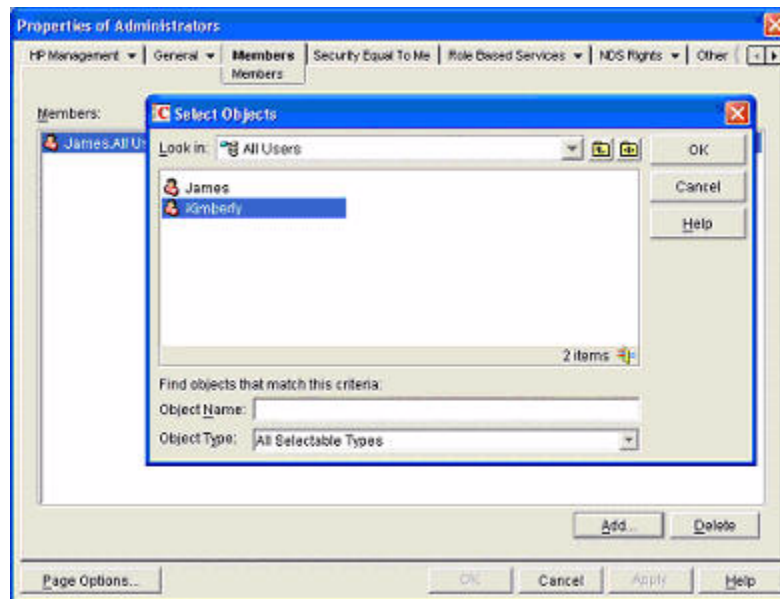
To browse to the specific user you want to add, click **Add**.

To remove a user from the list of valid members, highlight an existing user and click **Delete**.

Setting Role Restrictions

The **Role Restrictions** subtab (Figure 9-19) enables you to set login restrictions for the role.

Figure 9-19 Role Restrictions Subtab (eDirectory)
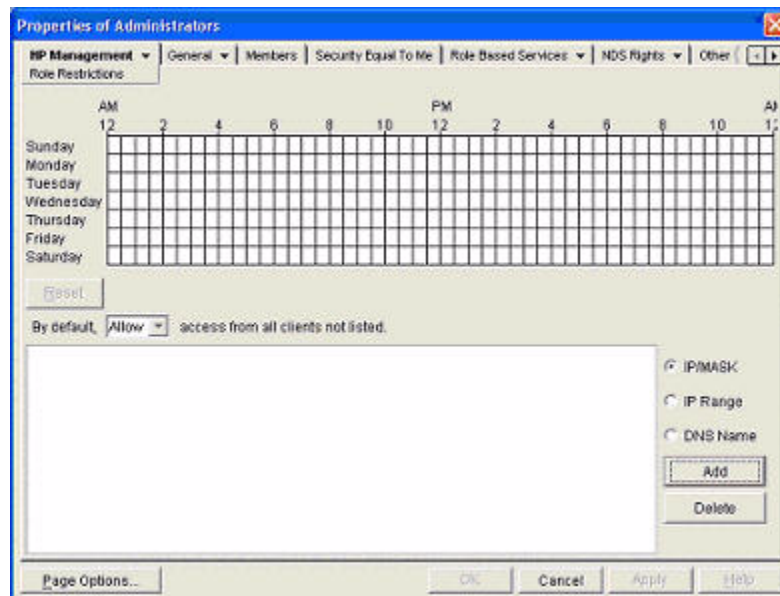
These restrictions include:

- 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 the role by using the time grid displayed in the **Role Restrictions** subtab (Figure 9-19). 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 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.

In the **By Default** drop-down menu, 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** pop-up for the IP/Mask option is shown.
2. In the **Add New Restriction** pop-up window (Figure 9-20), enter the information, and click **OK**.

Figure 9-20 Add New Restriction Pop-up Window
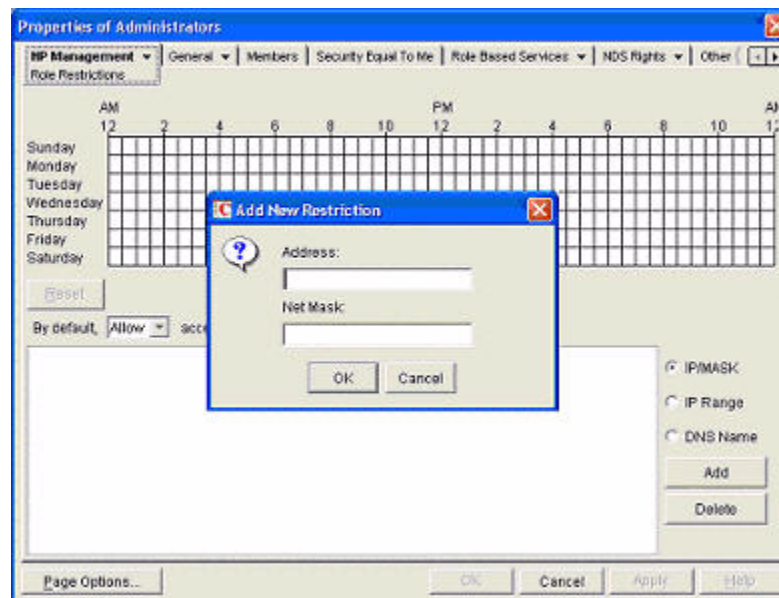
3. Select **DNS Name** in the **Role Restrictions** subtab and click **Add**. The **DNS Name** option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com. The **New DNS Name Restriction** pop-up window opens.
4. Enter the information and click **OK**.
5. Click **Apply** to save the changes.

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. You can make users and group objects members of the role, giving the users or group of users the rights granted by the role. Use the **Lights Out Management Device Rights** subtab of the **HP Management** tab (Figure 9-21) to manage rights.

Figure 9-21 Lights-Out Management Device Rights Tab
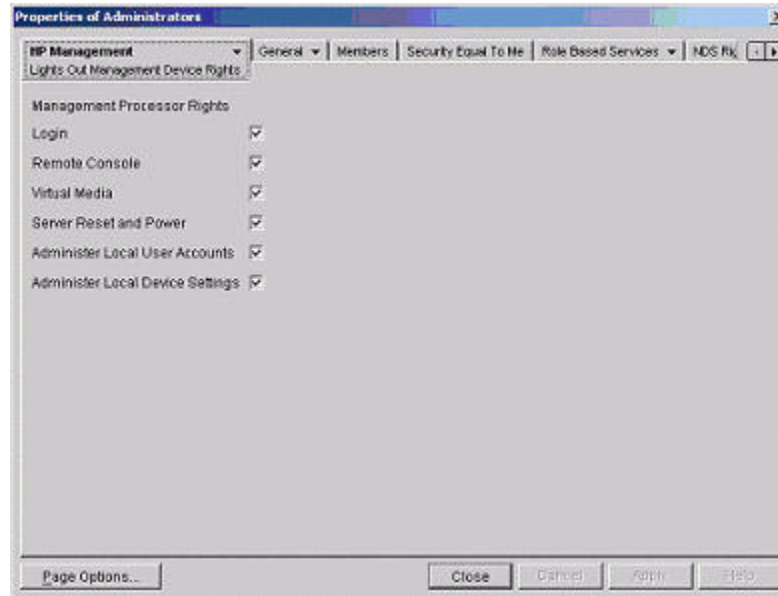
Options and descriptions are as follows:

Table 9-2 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 MP or the system.
Remote Console	This option enables you to access the system console (the host OS).
Virtual Media	This option enables you to connect devices such as CD/DVD and network drives as virtual devices through the network.
Server Reset and Power	This option enables you to execute iLO 2 MP power operations to remotely power on, power off, or reset the host platform, as well as configure system's power restore policy.
Administer Local User Accounts	This option enables you to administer local iLO 2 MP user accounts.
Administer Local Device Settings	This option enables you to configure all iLO 2 MP settings, as well as reboot the iLO 2 MP and update the iLO 2 MP firmware.

Snap-Ins Installation and Schema Extension for eDirectory on a Linux Platform

This section describes a method that does not require a Windows client to install snap-ins and schema extension for eDirectory on a Linux platform.

Schema extension is the addition of new classes to the existing classes. You can use these classes to create objects to support a specific utility. New classes, such as hpqTarget, hpqPolicy and hpq

role, are added. HP has created objects using these classes to support iLO 2 MP devices (created using the 'hpqTarget' class), and iLO 2 MP admins and monitors (created using the 'hpqRole' class). These objects support the Login Authentication utility to the iLO 2 MP device and enable iLO 2 MP users to execute commands based on their assigned roles.

Installing the Java Runtime Environment

As a prerequisite for extending the schema, you need to have Java Runtime Environment (JRE) 1.4.2 installed. To ensure you have the correct version of JRE installed on your system, follow these steps:

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.sun.com Web site.

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 the older version.

   # **rpm –Uv j2re-1_4_2_04-linux-i586.rpm**

4. Add the entry **/usr/java/j2re1.4.2_04/bin** into the .bash_profile file.

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. You need to create this directory because it is not present. Creation of the directory and copying of the two .jar files to the HP directory are done automatically when the hpdsse.shfile is executed.

> **NOTE:**   The hpdsse.sh file is obtained when theSchema.tar tarball is extracted. This process is explained in the Schema Extension section. You can download schema extensions from the Web 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.

Schema Extension

To obtain the hpdsse.sh file, do the following:

1. Download the tar file to the Linux system on which 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 the instructions. As per the instructions, provide the server name, Admin DN, and Admin password as command line arguments to extend the schema.

4. To see the results, check the schema.log file, which is created after the schema extension is complete.

The log file must show the classes and attributes created. In addition it should show the result as Succeeded. If the objects already exist, the message Already Exists should appear in the log file.

The **Already Exists** message displays only when you try to run the same .sh file after schema extension is complete. The SSL port (636) is used during the schema extension. You verify this by running the **netstat -nt grep :636** command while the hpdsse.sh file is being executed.

Verification of Snap-Ins and Schema Extension

To verify the snap-ins and schema extension, do the following:

1. Launch **ConsoleOne** and log on to the tree.
2. Check for the new classes by opening the **Schema Manager** from the **Tools** drop-down menu.

All the classes related to the HP directory services must be present in the classes list. The classes are 'hpqRole,' hpqTarget,' 'hpqPolicy,' and 'hpqLOMv100'.

Configure Directory Settings in the iLO 2 MP (LDAP Command)

Use the **LDAP Command Menu** in the iLO 2 MP CLI to configure iLO 2 MP 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

> 📝 **NOTE:** The short form of the login name by itself does not tell the directory which domain you are trying to access. 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)

  Example: jsmith@hp.com

> 📝 **NOTE:** Directory users specified using the @ searchable form can be located in one of three searchable contexts, which are configured within Directory Settings.

- User name form

  Example: John Smith

> 📝 **NOTE:** Directory users specified using the user name form can be located in one of three searchable contexts, which are configured within Directory Settings.

- Local users—Login-ID

> 📝 **NOTE:** On the iLO 2 MP 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, do the following:

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 the **Certificate Services** checkbox. Click **Next**.
5. Click **OK** at the warning that the server cannot be renamed. 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 for the **Valid for** field. 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 the iLO 2 MP communicates with Active Directory using SSL, it is necessary to 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 displays.

Configuring Automatic Certificate Request

To specify 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. Click **Next** when the Automatic Certificate Request Setup wizard starts.
9. Select the **Domain Controller** template, and click **Next**.
10. Select the certificate authority listed. (It is the same CA defined during the Certificate Services installation.) Click **Next**.
11. Click **Finish** to close the wizard.

Directory-Enabled Management

This section is for administrators who are familiar with directory services and with the iLO 2 MP product. See "Directory Services" (page 137) to familiarize yourself. Make sure you understand the examples and are comfortable with setting up.

Directory-enabled remote management enables you to:

- Create iLO 2 MP objects:

  Create one iLO 2 MP device object to represent each device that will use the directory service to authenticate and authorize users. See "Directory Services" (page 137) for additional information on creating iLO 2 MP device objects for active directory ("Directory Services for Active Directory" (page 141)) and eDirectory ("Directory Services for eDirectory" (page 152)). In general, you can use the HP provided snap-ins to create objects. It is useful to give the iLO 2 MP device objects meaningful names, such as the device's network address, DNS name, host server name, or serial number.

- Configure iLO 2 MP devices:

  Every iLO 2 MP device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. See "Configure Directory Settings in the iLO 2 MP (LDAP Command)" (page 160) for details on the specific directory settings. In general, you configure each device with the appropriate directory server address, iLO 2 MP 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 their users and administrators into groups. In many cases, it is convenient to use the existing groups and associate the groups with one or more iLO 2 MP role objects. When the devices are associated with the role objects, you can control access to the iLO 2 MP 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. 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 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 the role.

When you use trustee or directory rights assignments to extend role membership, users must be able to read the iLO 2 MP object representing the iLO 2 MP device. Some environments require the same trustees of a role to also be read trustees of the iLO 2 MP object to successfully authenticate users.

Using Multiple Roles

Most deployments do not require the same user to 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 can only grant rights, never 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 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 can have two types of users: administrators of the iLO 2 MP device or host server and users of the iLO 2 MP 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 MP administrators in that role, as well as to the administrative role.

The following figure 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 initial login, more advanced rights are assigned to the admin user through the admin role—server reset and remote console.
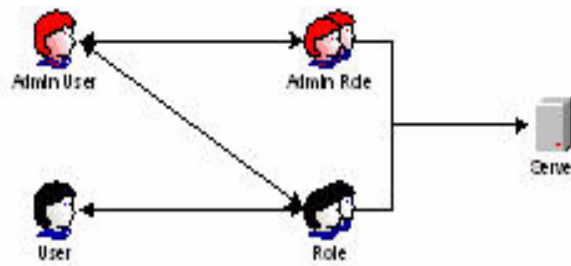
In the following figure, the admin user gains the admin role right in a different way. The admin user initially logs in through the admin role and is assigned admin rights—server reset, remote console, and login.
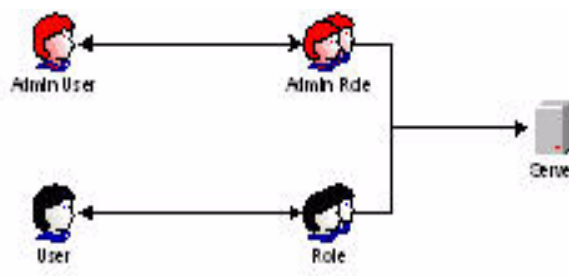
Creating Roles to Follow Organizational Structure

Often, the 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 the 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 results in 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 on a role, see "Setting Role Restrictions" (page 156) or "Setting Time Restrictions" (page 157).

Role Time Restrictions

You can place time restrictions on iLO 2 MP roles. Users are granted the rights specified for the iLO 2 MP devices listed in the role, only if they are members of the role and meet the time restrictions for that role.

iLO 2 MP devices use local host time to enforce time restrictions. If the iLO 2 MP 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 satisfied if the time is set on the iLO 2 MP device. The time is normally set when the host is booted, and it is maintained by running the agents in the host operating system, which enables the iLO 2 MP device to compensate for leap year and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing iLO 2 MP firmware, can cause the iLO 2 MP device clock to not be set. Also, the host time must be correct for the iLO 2 MP 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 that are on the same logical network.

In binary math, if the bits of a client machine address, added to the bits of the subnet mask, 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 goes down 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 iLO 2 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.

How Directory Login Restrictions Are Enforced

The following figure shows how two sets of restrictions potentially limit a directory user's access to iLO 2 MP 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 MP privileges based on rights specified in one or more roles.
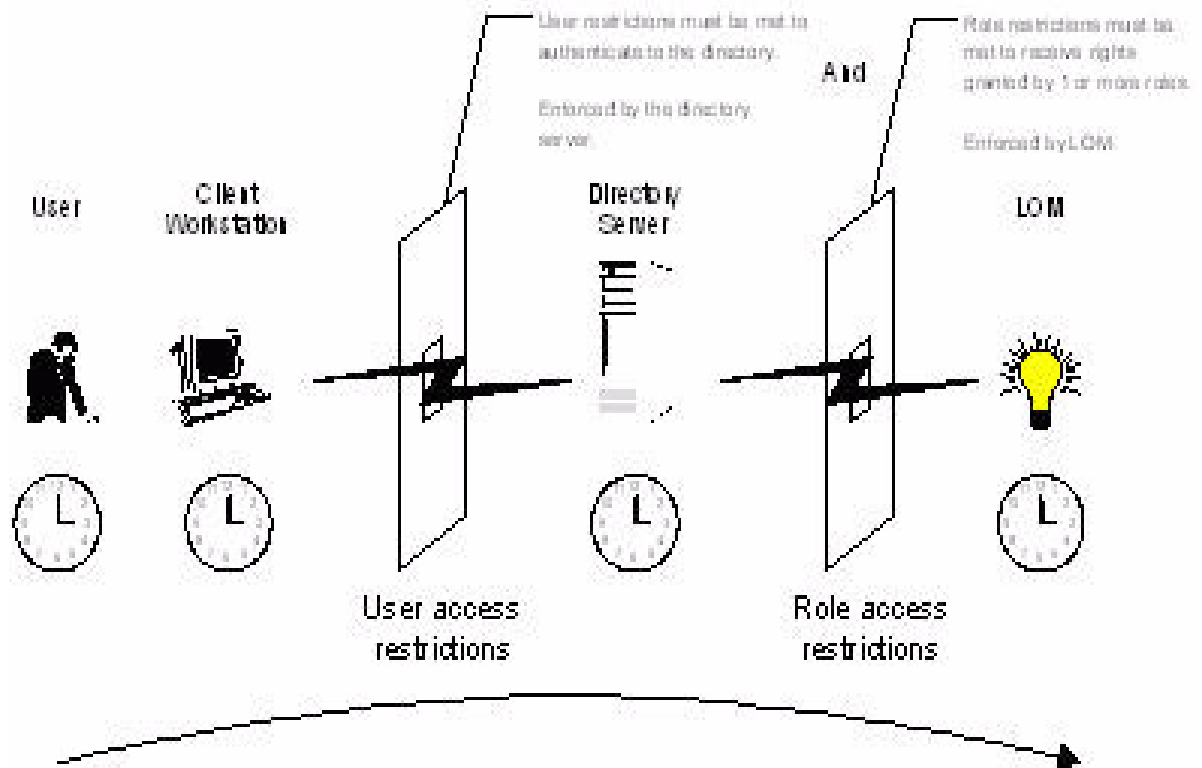
How User Time Restrictions Are Enforced

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 at the directory server, but if the directory server is located in a different time zone 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.

The directory server evaluates user time restrictions, but the determination can be complicated by time zone changes or by the authentication mechanism.
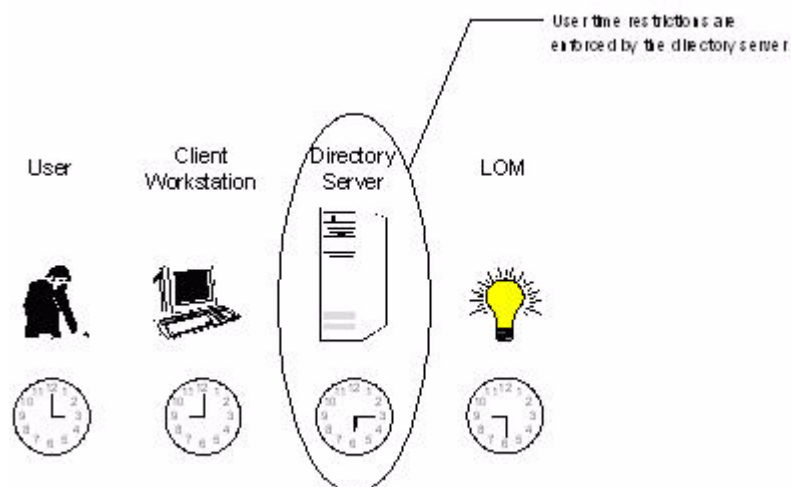
User Address Restrictions

You can place network address restrictions on a directory user account, and the directory server enforces these restrictions. See the directory service documentation for details on the enforcement of address restrictions on LDAP clients, such as a user logging in to an iLO 2 MP 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 MP device as a directory user, the iLO 2 MP 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 MP device. However, because the user is proxied at the iLO 2 MP device, the network address of the authentication attempt is that of the iLO 2 MP 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 may have a security policy in which iLO 2 MP administrators are allowed to use the iLO 2 MP 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 may allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

In this example, security policy dictates general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.
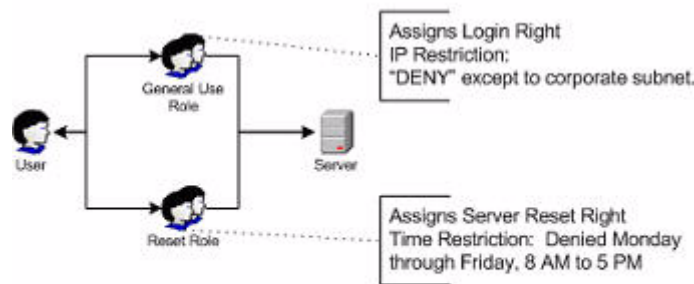
Alternatively, the directory administrator could create a role that grants the login right and restrict it to the corporate network, create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because 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 MP 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 meets 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.
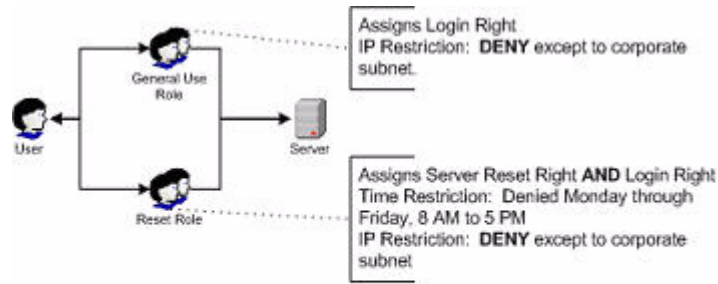
Directory Services Schema (LDAP)

A directory schema specifies the types of objects that a directory may have and the mandatory and optional attributes of each object type. The following sections describe both the HP management core, and the iLO 2 MP-specific LDAP object identifier classes and attributes.

HP Management Core LDAP Object Identifier Classes and Attributes

Object identifiers (OIDs) are unique numbers that are used in 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:

- Core classes
- Core attributes

NOTE: Roles such as hpqTargets, and so on, are for extended schema LDAP only. They are not used in LDAP Lite.

Core Classes

Table 9-3 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

Table 9-3 lists the core LDAP OID classes.

Core Attributes

Table 9-4 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

Table 9-4 Core Attributes *(continued)*

Attribute Name	Assigned OID
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

Table 9-4 lists the core LDAP OID attributes.

Core Class Definitions

Table 9-5, Table 9-6, and Table 9-7 define the HP Management core classes.

hpqTarget

Table 9-5 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 9-6 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 9-7 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 9-8 through Table 9-13 define the HP management core class attributes.

hpqPolicyDN

Table 9-8 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 9-9 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 9-10 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 9-11 hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	This attribute is a Boolean 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 9-12 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

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Options	Multi Valued
Remarks	This attribute is only used on role objects. 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 would be 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 9-13 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
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 MP-Specific LDAP OID Classes and Attributes

The schema attributes and classes in Table 9-14 and Table 9-15 may depend on attributes or classes defined in the HP management core classes and attributes.

iLO 2 MP Classes

Table 9-14 iLO 2 MP Classes

Class Name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

iLO 2 MP Attributes

Table 9-15 iLO 2 MP 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

Table 9-15 iLO 2 MP Attributes *(continued)*

Class Name	Assigned OID
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 MP Class Definitions

hpqLOMv100

Table 9-16 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 MP products.
Class Type	Auxiliary
SuperClasses	None
Attributes	hpqLOMRightConfigureSettings—1.3.6.1.4.1.232.1001.1.8.2.1hpqLOMRightLocalUserAdmin—1.3.6.1.4.1.232.1001.1.8.2.2hpqLOMRightLogin—1.3.6.1.4.1.232.1001.1.8.2.3hpqLOMRightRemoteConsole—1.3.6.1.4.1.232.1001.1.8.2.4hpqLOMRightServerReset—1.3.6.1.4.1.232.1001.1.8.2.5hpqLOMRightVirtualMedia—1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

iLO 2 MP Attribute Definitions

Table 9-17 through Table 9-22 define the iLO 2 MP core class attributes.

hpqLOMRightLogin

Table 9-17 hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Login right for HP iLO 2 MP 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 9-18 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Remote console right for iLO 2 MP 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 9-19 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Virtual media right for HP iLO 2 MP 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 9-20 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 MP 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 9-21 hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Local user database administration right for HP iLO 2 MP 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 9-22 hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Configure devices settings right for HP iLO 2 MP 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.

10 Integrated Remote Console and vKVM

Integrated Remote Console (IRC) enables you to securely view and manage HP Windows-based Integrity servers with the iLO 2 MP through Windows clients running Internet Explorer. The IRC integrates keyboard, video and mouse into a virtual interface providing an experience similar to that of the remote server's console. With IRC, you can view the server system's display to directly interact with the server and perform maintenance activities as well as open and run applications on the server using the keyboard and mouse control.

The IRC screen window refreshes every 10 seconds.

The iLO 2 MP graphical IRC provides Virtual Keyboard, Video (monitor), and Mouse (vKVM) capabilities with KVM over IP performance.

vKVM enables a user with console access right and the Advanced Pack license to:

- Access the server from any location on the same network.
- 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 their login passwords without administrator access right.
- Remotely change the configuration parameters of the IRC.

This chapter addresses the following topics:

IRC Usage

The IRC runs as an ActiveX control that is downloaded to clients running Internet Explorer 6.0 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 the iLO 2 MP on the first client connection.

The IRC uses encryption and compression to provide a secure connection.

> **NOTE:** When working on multiple systems, all controls for each system are displayed in a separate screen for each server. Additionally clients must allow downloading and usage of signed ActiveX controls.

Before running the IRC, note the following:

1. Verify if 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 see if the remote console/IRC is available for use, click **Remote Console Integrated Remote Console**. If the **Launch** button is grayed out and the `Maximum console number has been reached` status message displays, the remote console/IRC is in use by another client.
2. Verify if 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. You can view this information on the **Administration Licensing** tab. For more information, see "Advanced Pack License" (page 23).

4. Disable any pop-up blocking applications. Pop-up blocking applications prevent the IRC from running.

5. Accept the IRC certificate. Refusing to accept the IRC certificate displays a red **X** in the IRC and prevents the IRC from working on that client.

Mouse and Keyboard Limitations

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 IRC closes after 15 minutes if there is no mouse or keyboard activity.
- A slight delay may be observed between the physical and virtual mouse pointer.

NOTE: If you run system discovery utilities, such as MAPPER or IOSCAN, the output may recognize and display an extra keyboard and mouse which are not physically connected. This is a consequence of the vKVM feature.

Supported Browsers and Client Operating Systems

The IRC is supported in the following browser and operating systems

Browser

Microsoft Internet Explorer 6 with service pack 1 and above.

Operating Systems

Microsoft Windows 2000 Professional, Microsoft Windows XP Professional, and Microsoft Windows 2003 Client operating systems.

The IRC is not supported for HP-UX, Linux, or OpenVMS.

Supported Resolutions and Browser Configurations

Set your Windows-based HP Integrity server to the following specifications to properly access and view the IRC and optimize performance.

Microsoft Windows Server 2003 Console Resolution Settings

The following settings are based on your operating system:

Server Display Properties

- Plain background (no wallpaper pattern) on the host server.
- Set client screen resolution higher than the host server for best remote console performance.
- Display resolution of 800 x 600 pixels, or the maximum supported resolution of 1024 x 768 pixels.

NOTE: The resolution on the host server should not exceed 1024 x 768. Resolutions beyond this setting can produce unpredictable results.

- 256-color or 24-bit color mode.

Server Mouse Properties

- Select **None** for mouse pointer scheme.
- 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**.

NOTE: To automate the setting of the optimal mouse configuration, download the Lights-Out Optimization utility from the HP Web site. (http://www.hp.com/servers/lights-out). Click the **Best Practices** graphic and click the **Maximize Performance** links.

Accessing the IRC

To access the IRC, select **Remote Console > Integrated Remote Console** () and click **Launch**. The IRC may experience a slight delay as it first loads on your browser.

Figure 10-1 Integrated Remote Console Page
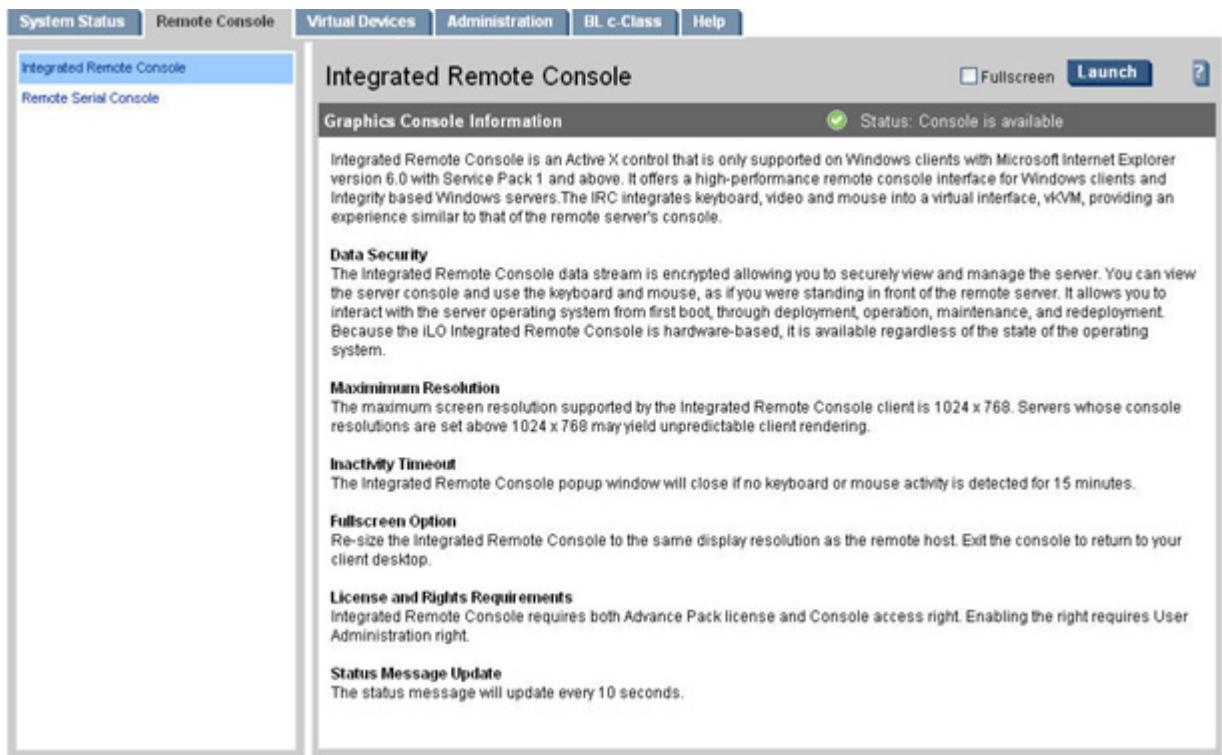
The IRC displays the host server's graphics console (Figure 10-2).

Figure 10-2 Integrated Remote Console Window

The **Menu** bar has the following options:

Thumb Tack	Enables you to keep the menu open or to retract when the mouse is moved away.
Exit	(red button) enables you to exit and close the console.
Ctrl+Alt+Del	Enables a user to simulate ctrl+alt+del sequence on remote console.

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 may recognize and display an extra keyboard and mouse which are not physically connected.

Integrated Remote Console Fullscreen

The IRC Fullscreen causes your client to resize to the same resolution as the remote server. The IRC Fullscreen attempts to pick the best client display settings for that resolution; however, some monitors can have trouble with the highest screen refresh rates supported by the video adapter. If this occurs, check your desktop properties by right-clicking on the desktop and selecting **Properties**>**Settings**>**Advanced**>**Monitor** and select a lower screen refresh rate.

To re-size the IRC to the same display resolution as the remote host, click the **Fullscreen** checkbox before you click **Launch**.

Use the red **X** button to exit the IRC and return to your client desktop.

11 Virtual Media

Virtual media (vMedia) provides administrators with virtual devices that mimic physical hardware devices, such as a virtual 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.

📝 **NOTE:**   Floppy disk or USB memory devices are not currently supported.

Booting from the iLO 2 MP 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 MP device uses a client-server model to perform the vMedia functions. The iLO 2 MP 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 MP as it requests it.

📝 **NOTE:**   vMedia is part of the iLO 2 MP Advanced Pack feature set and is enabled by licensing the optional iLO 2 MP Advanced Pack license and the virtual media right. If not licensed, the message `iLO 2 feature not licensed` displays. For more information, see "Advanced Pack License" (page 23).

This chapter addresses the following topics:
*   "Using the iLO 2 MP Virtual Media Devices" (page 179)
*   "Operating System USB Support" (page 184)
*   "Java Plug-in Version" (page 185)
*   "Supported Browsers" (page 185)

Using the iLO 2 MP Virtual Media Devices

Connect client-based virtual media to a host HP Integrity server through a graphical interface using a signed Java™ applet. Refusing to accept the applet certificate prevents browser-based virtual media from working (a red **X** appears). It also prevents the remote console applet from working because it is also signed using the same certificate.

📝 **NOTE:**   The virtual media feature is only available if you have the iLO 2 MP Advanced Pack license and the user virtual media access right.

To access the iLO 2 MP virtual media devices using the graphical interface, follow these steps:

1.   From the **Virtual Devices** tab, select **Virtual Media**. The **Virtual Media** applet loads in support of the virtual media device by clicking the **Launch** button.

Figure 11-1 Virtual Media Page
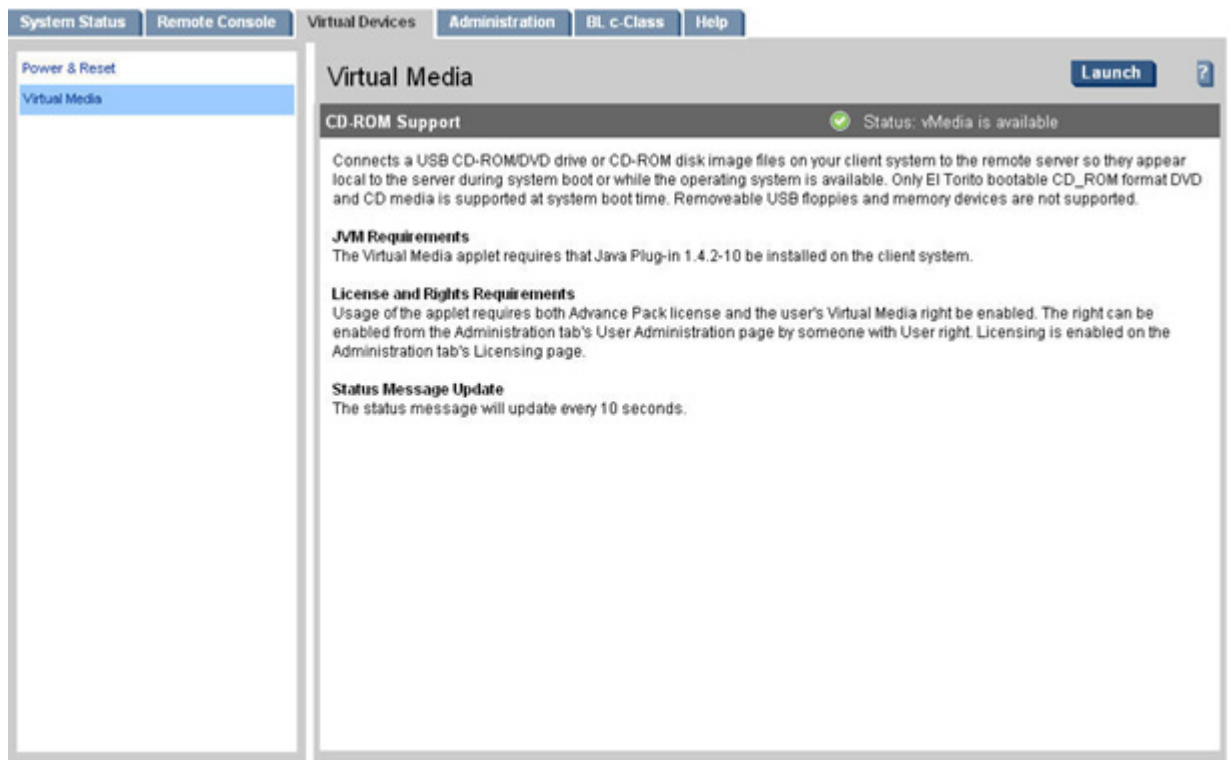
2. At this point, you can connect to a virtual CD/DVD device or create an iLO 2 MP disk image file.

NOTE: When you disconnect the iLO 2 MP virtual media, you may 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-provided feature to stop the device before disconnecting it from the virtual media.

Virtual CD/DVD

The iLO 2 MP virtual CD/DVD is available at server boot time for operating systems specified in "Operating System USB Support" (page 184). Booting from the iLO 2 MP virtual CD/DVD enables you to deploy an operating system from network drives with DVD 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 MP virtual CD/DVD is also available after the host server operating system loads. You can use the iLO 2 MP 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 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 MP virtual media CD/DVD appears to your operating system just like any other CD/DVD. When using the iLO 2 MP for the first time, the host operating system may prompt you to complete a**New Hardware Found** wizard.

To use a physical CD/DVD drive in your client system, follow these steps:

1. From the **Virtual Devices** tab, select **Virtual Media**. The **Virtual Media** content page displays.
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 **Virtual Media** applet's popup window opens (Figure 11-2).

   This feature requires prior installation of Java Plug-in 1.4.2 or 1.5.

   This feature also requires the virtual media right as well as the Advance Pack License. For more information, see "Advanced Pack License" (page 23). If a user does not have the virtual media right, it can be granted through the **User Administration** page under the **Administration** tab by a user with Admin privileges.

📝 **NOTE:** Only one user and one device can be connected at a time.

Figure 11-2 Virtual Media Dialog Box (before connection)
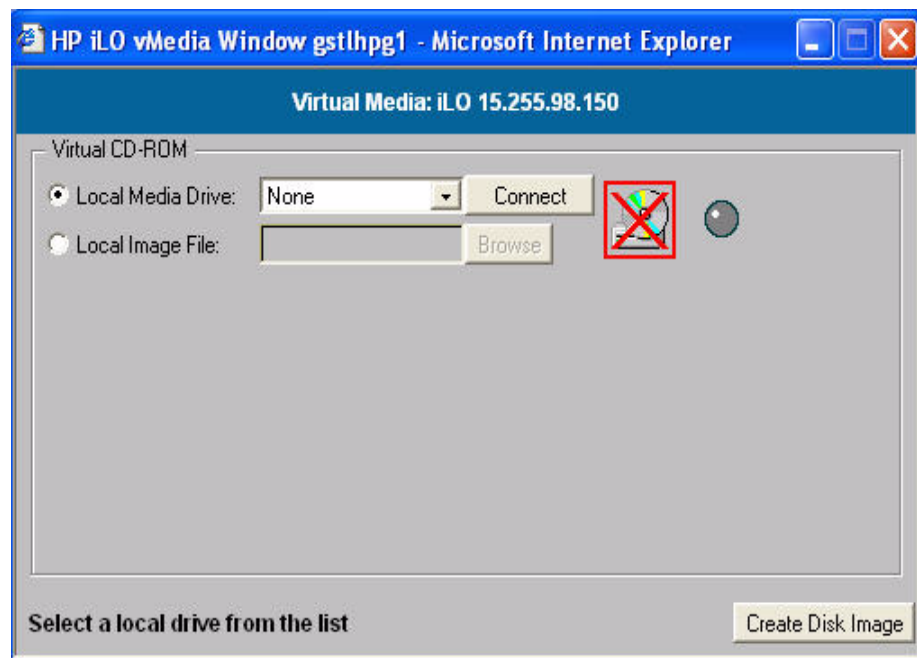
3. Select **Local Media Drive**.
4. Select the drive letter of the desired physical CD/DVD drive on your client system from the drop-down menu.
5. Click **Connect**. The connected drive icon and LED changes state to reflect the current status of the virtual CD/DVD.

Figure 11-3 Virtual Media Dialog Box (after connection)
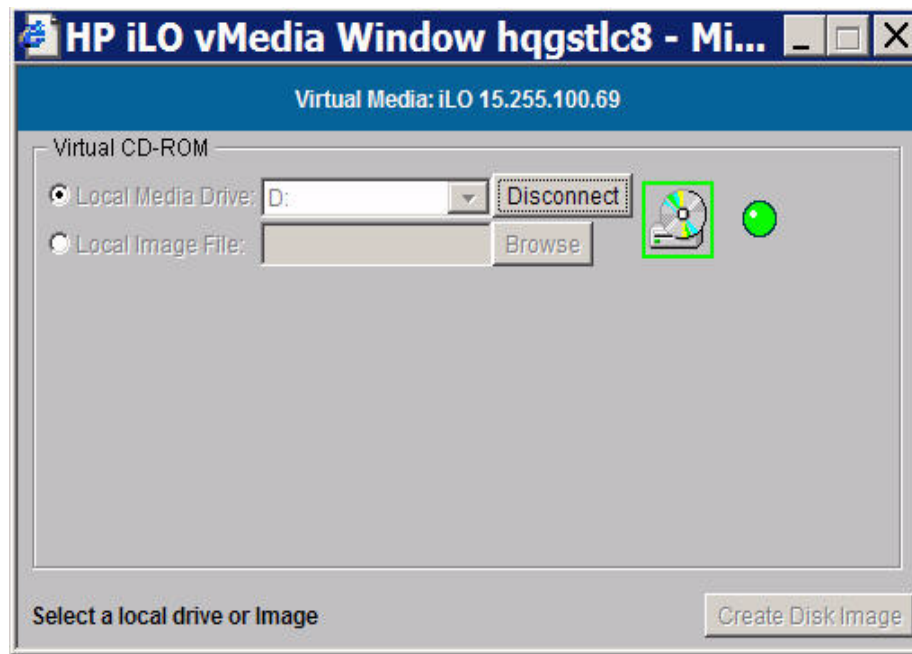
When connected, virtual devices are available to the host server until you close the **Virtual Media** applet or sign out from a Web session. When you are finished using the virtual CD/DVD, disconnect the device from the host server or close the applet.

📝 **NOTE:** The **Virtual Media** applet must remain open when using a virtual media device.

Virtual Media CD/DVD Operating System

- 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 BL c-Class blade systems, 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, March 2006

  To recognize the hardware path and special files, run `ioscan -kfnC disk`.

  To mount the virtual CD/DVD/image file on a directory, use **# mount <special files path> /<dir-name>**

- OpenVMS is not currently supported

Creating the iLO 2 MP Disk Image Files

The iLO 2 MP virtual media 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 MP virtual media is faster when image files are used. The utility to create the iLO 2 MP CD/DVD disk image files is integrated into the **Virtual Media** applet; however, images can also be created using industry standard tools such as DD.

Store image files on your client PC or on a network drive that can be accessed from your client using a fast network segment. A disk image file results in better performance than using a physical CD disk in your client PC.

Use the **Disk>>Image** option to create image files from physical diskettes or CD/DVDs. 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 MP **Create Media Image** utility does not currently support USB devices in Linux or NetWare.

The following procedure shows how to create an iLO 2 MP disk image file.

1. Select **Local Image File** within the Virtual CD-ROM section of the **Virtual Media** applet.
2. Select **local media drive** from the drop-down menu.

Figure 11-4 Local Image File Dialog Box
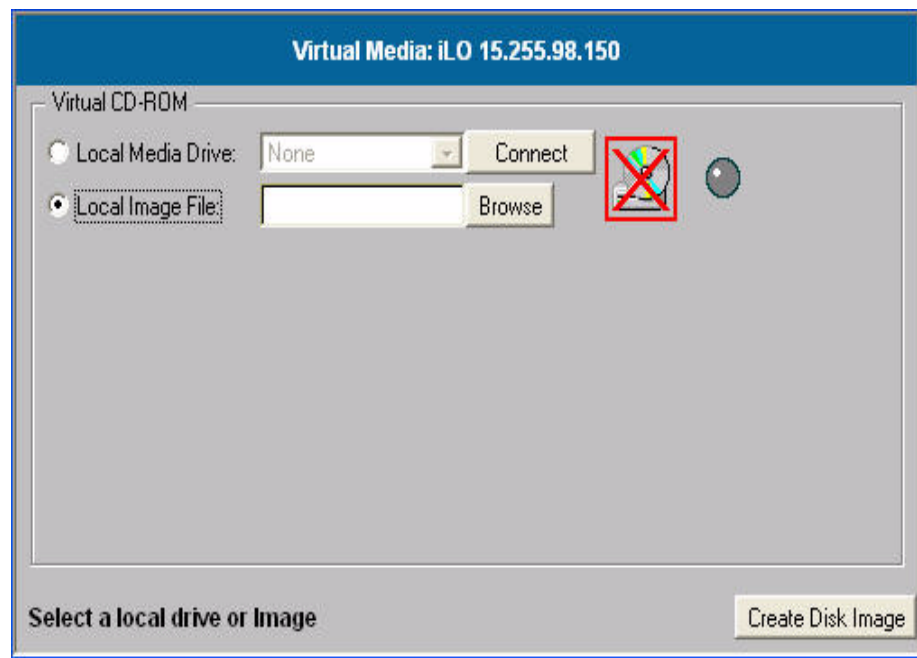
3. Enter the path or file name of the image in the text-box or click **Browse** to open the **Create Media Image** dialog box and locate the image file.

NOTE: Although the **Drive** menu items list `floppy` as an option, vMedia does not currently support the floppy option.

Figure 11-5 Create Media Image Box
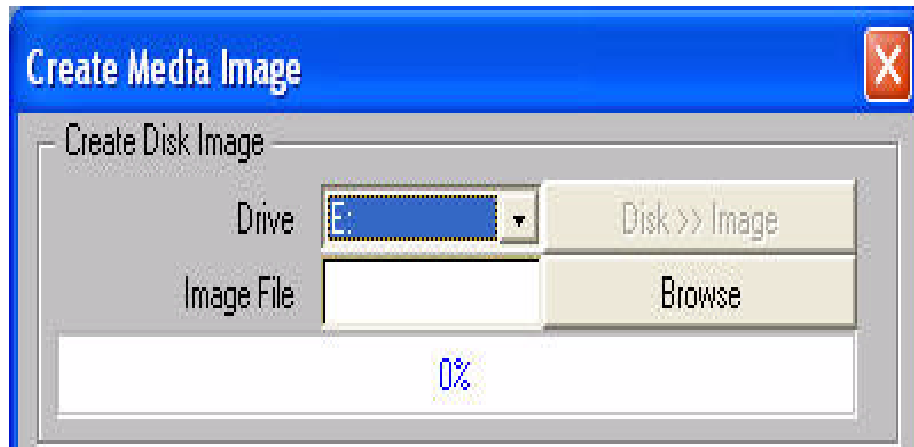
4.   Click **Create Disk Image**. The **Virtual Media** applet begins the process of creating the image file. The process is complete when the progress bar reaches 100%. This creates a file that emulates the disk on the local system. To cancel the creation of an image file, click **Cancel**.

To insert the next CD during an OS install or any application install with multiple image files, follow these steps:

1.   Click **Browse** to select the next image file or to replace the CD/DVD with the next CD/DVD.
2.   Click **OK** on the host server to continue installation.

NOTE: Do not click **Disconnect** to select the next CD/DVD image file.

The connected drive icon and LED changes state to reflect the current status of the virtual CD/DVD. When connected, virtual devices are available to the host server until you close the **Virtual Media** 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 **Virtual Media** applet must remain open when using a virtual media device.

The iLO 2 MP virtual media CD/DVD appears to your operating system just like any other CD/DVD. When using the iLO 2 MP for the first time, the host operating system may prompt you to complete a **New Hardware Found** wizard.

Virtual Media Applet Timeout

The **Virtual Media** applet does not timeout when it is connected to a host server. The **Virtual Media** applet must remain loaded while virtual media is in use. The **Virtual Media** applet closes if the user logs out.

Operating System USB Support

To use virtual media devices, your operating system must have support for USB mass storage devices.

Different operating systems provide varying levels of USB support. The iLO 2 MP uses the built-in USB drivers of the operating system. The level of USB support in the operating system affects the level of support for the iLO 2 MP virtual media. In general, any operating system issues that affect a USB CD/DVD drive also impacts the iLO 2 MP virtual media.

The HP server ROM provides support at server boot time for virtual media with El Torito bootable CD format.

Table 11-1 lists operating system USB capabilities and the corresponding the iLO 2 MP virtual media capabilities by USB CD.

Table 11-1 USB CD Capabilities

	Operating system install using Virtual USB CD	Operating system run time using Virtual USB CD*
Linux Red Hat ES/RHEL 4 U3	Yes	Yes
Linux SuSe SLEX 10 SP3	Yes	Yes
HP-UX 11.23 HWE 0606	Yes	Yes
OpenVMS 8.3	Not currently supported	Not currently supported
Windows Enterprise Edition	Yes	Yes
*Any additional software packages that must be installed can be accomplished using the system run time method.		

Java Plug-in Version

The vMedia feature requires prior installation of Java Plug-in 1.4.2_10 or 1.5.

Supported Browsers

Table 11-2 lists the supported browsers for virtual media.

Table 11-2 iLO 2 MP Supported Browsers and Operating Systems

Browsers	Operating System					
Java Plug-in 1.4.2_10	HPUX	Windows		Linux		VMS
	11.23	WS 2003 Enterprise	XP	Red Hat Enterprise	SuSE	8.3
Mozilla 1.7.12.01.00	X					
Mozilla 1.7.13		X	X	X	X	
Internet Explorer 6.0		X	X			
HP Secure Web Browser 1.7.13		X	X			X

Glossary

A

Address
In networking, a unique code that identifies a node in the network. Names such as **host1.hp.com** are translated to dotted-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. The client can authenticate the server as well. 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 at system power on. 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) to which it provides an interface. The BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity. 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.

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 entails interacting with the MAP through the following process:
  — 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 type 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 one and only one response data transmission to the client.
	The CLP allows for extensibility through four 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, developed by the DMTF, for describing 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 bought four different servers from four different vendors, and networked 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 the iLO 2 MP and the server that controls basic functionality. Also know as *host console*.

D

DDNS	Short for dynamic Domain Name System, its the way iLO 2 can automatically get its name registered by the Domain Name System, so when iLO 2 gets its new IP address from DHCP, users can connect to the new iLO 2 using the host name, rather than the new IP number.
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 move 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	The Distributed Management Task Force is the industry organization that authors and promotes management standards and integration technology for enterprise and Internet environments for the purpose of furthering 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 get 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, wherein 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 then 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 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 the iLO 2 MP and the server that controls basic functionality. Also know 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	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	Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.
Integrated Lights Out (iLO)	offers remote server management through an independent management processor (MP). iLO was introduced into most 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	Short for Internet Protocol. IP specifies the format of packets and the 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. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time. An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. 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 could be an IP address. 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	A hardware-level interface specification that was designed primarily for 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 FRU inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

K

Kernel	The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.
kVMS	keyboard, video, mouse, storage. A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

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) and across multiple platforms.

M

Manageability Access Point (MAP)	A network-accessible interface for managing a computer system. A MAP can be instantiated by a management process, a management processor, a service processor or a service process.
Managed Object	The actual item in the system environment that is accessed by the provider. For example, a Network Interface Card.

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. It is not the actual database itself; it is implementation dependant.
Management Processor (MP)	The component providing 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 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 the local subnet address from the rest of a given 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	Onboard Administrator is the enclosure management processor, subsystem, and firmware base used to support the HP BladeSystem BL860c and all the managed devices contained within the enclosure. Onboard Administrator provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Utilizing this hardwired knowledge, Onboard Administrator performs initial configuration steps for the enclosure, allows for run-time management and configuration of the enclosure components, and informs you of problems within the enclosure through email, SNMP, or the Insight Display.
Options	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) to which 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 is 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 the 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

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.

SM Command Line Protocol (SM CLP)   Server Management CLP specification defines a user-friendly command line protocol to manipulate CIM instances defined by the SM profiles specification.

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.

System Management Architecture for Server Hardware (SMASH)   SMASH is 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.

T

Target Address   The target addressing scheme provides an easy-to-use way 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.

Targets   A target is the implicit or explicitly-identified managed element the command is directed to. Command targets specify managed elements in the system. Targets follow the SM addressing specification.

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 450M bits per second (USB 2.0). A USB port connects devices, such as mouse pointers, keyboards, and printers, to the computer system.

User   The Command Line Protocol (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 human or 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 UFcT is 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 UFiP is 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 addressing association.

User Friendly instance Tag (UFiT)   A UFiT is a unique instance tag within the scope of the target instance's containment class. A UFiT is created by adding an non-zero positive integer suffix to the target instance's UFcT.

User Friendly Tag (UFT)   A UFT is a short, user friendly tag for a CIM class name or instance. There are two types of UFTs; UFcT and UFiT (defined below).

User Name   A combination of letters, and possibly numbers, that identifies a user to the system.

UTF-8   (8-bit Unicode Transformation Format) is a variable-length character encoding for Unicode.

V

Verb   The verb selects a management action for target.

VPN   Virtual private network, or a network that is constructed using public wires (the Internet) to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Index