HP Integrity and HP 9000

Integrated Lights-Out (iLO) Management Processor Operations Guide

Manufacturing Part Number: 5971-4289

Third Edition

September 2006

Printed in the US

Legal Notices

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

Contents

About This Document

1. Introduction

2. Ports and Indicators

3. Console Connection and Setup

8. Directory Services Installation and Configuration

Tables

Tables

Figures

About This Document

This document provides information and instructions on how to use the Integrated Lights Out (iLO) 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, you should 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 Information in This Edition

This guide has been updated with the following:

- Console setup information
- Firmware upgrade procedures
- Expanded Web GUI details
- Glossary

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
5971-4289	Microsoft® Windows® Server 2003 Linux® Red Hat & SuSE	rx1600, rx1620, rx2620, rx2600 cx2600, cx2620 rp3410, rp3440 rx4640, rp4440 rx5670 BL60p	September 2006

Table 1 Publishing History Details (Continued)

Document Manufacturing Part Number	Operating Systems Supported	Supported Product Versions	Publication Date
5971-4274	Microsoft Windows Server 2003 Linux Red Hat & SuSE	rx1600, rx1620, rx2620, rx2600 cx2600 rp3410, rp3440 rx4640, rp4440 rx5670	April 2005
E1104	Microsoft Windows Server 2003 Linux Red Hat & SuSE	rx1600, rx1620, rx2620, rx2600 cx2600 rp3410, rp3440 rx4640, rp4440 rx5670	November 2004

Document Organization

This guide is divided into the following chapters.

Chapter 1 **Introduction** Use this chapter to learn about iLO MP and its functionality and features.

Chapter 2 **Ports and Indicators** Use this chapter to learn about the available iLO MP port connectors, pinouts, and LEDs.

Chapter 3 **Console Setup** Use this chapter to assist you with the iLO MP setup process.

Chapter 4 **Accessing the Host Console** Use this chapter to learn about the methods to access the console.

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

Chapter 7 **Command Menu Interface Reference** Use this chapter to learn about the options from which commands can be executed in iLO MP.

Chapter 8 **Directory Services Installation and Configuration** Use this chapter to learn about the features, functions, installation, and configuration of iLO MP directory services.

Glossary Use the glossary to learn about iLO 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 |, you must select one of the items.

`{ }` The contents are required in formats and command descriptions. If the contents are a list separated by |, you must select one of the items.

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

| Separates items in a list of choices.

HP-UX Release Name and Release Identifier

Each HP-UX 11i release has an associated release name and release identifier. The *uname* (1) command with the -r option returns the release identifier. This table shows the releases available for HP-UX 11i.

Table 2 HP-UX 11i Releases

Release Identifier	Release Name	Supported Processor Architecture
B.11.11	HP-UX 11i v1	PA-RISC
B.11.20	HP-UX 11i v1.5	Intel® Itanium®
B.11.22	HP-UX 11i v1.6	Intel Itanium
B.11.23	HP-UX 11i v2.0	Intel Itanium

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://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://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://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

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

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

Please send comments to: netinfo_feedback@cup.hp.com.

Please include title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document. Also, please include what we did right so we can incorporate it into other documents.

1 Introduction

Integrated Lights-Out (iLO) Management Processor (iLO MP) for entry-level 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.

This chapter addresses the following topics:

- "Features" on page 16
- "Advanced Pack License" on page 20
- "Supported Systems and Required Components and Cables" on page 21
- "Supported Operating Systems and Browsers" on page 22
- "Security" on page 23
- "Help System" on page 24

Features

iLO MP functionality includes:

- Control of power, reset, and Transfer of Control (TOC) capabilities.
- Console access.
- Displays and records system events.
- Displays detailed information about the various internal subsystems.
- Provides a virtual front panel to monitor system status and see the state of front panel LEDs.

The iLO 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 MP LAN, and packets on the iLO MP LAN do not go to the operating system. It is a subsystem that does not present a LAN interface to the operating system. The iLO MP LAN is exclusive to the iLO MP and is driven by an embedded real-time operating system (RTOS) running on the iLO MP.

The iLO MP offers the following standard and advanced features. The Advanced Pack license is required to use the advanced features.

Standard Features

The iLO MP standard features provide the following basic system board management functions, diagnostics, and essential Lights-Out functionality on iLO-supported HP servers:

Always-on Capability

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

VFP

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

Multiple Access Methods

- IPMI/LAN: Through the iLO MP MAC address
- LAN: Using telnet, Web GUI, or SSH to access the iLO MP LAN
- Local RS-232 Serial Port: Using a terminal or laptop computer for direct connection
- Remote/Modem RS-232 Serial Port: Using a dedicated modem RS-232 serial port and external modem

Security

The iLO 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, SSH, and RC4

If you enter an incorrect user name and password or a log in attempt fails, the iLO MP imposes a security delay.

The iLO MP provides several login security features. 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.

User Access Control

Access to the iLO 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 MP commands. The iLO MP supports (LDAP) directory user authentication and locally stored iLO MP user accounts. iLO 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 MP Configuration Access: Right to configure all iLO MP settings (as well as some system settings, such as the power restore policy).

Multiple Users

Multiple users can interact with the iLO MP. However, iLO 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 MP can support multiple simultaneous connections of all types, to do so can impact performance. HP does not recommend running more than eight simultaneous connections.

The iLO 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)
- 4 SSH
- 1 local RS-232 serial port
- 4 IPMI over LAN
- 4 telnet
- 1 remote (modem)

IPMI over LAN

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

Updateable Firmware

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

Internal Subsystem Information

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

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.

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

Event Logging

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

Advanced Features

The advanced features require the iLO MP Advanced Pack license. See “Advanced Pack License” on page 20.

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

SSH

Secure Shell (SSH) is an industry-standard client-server connectivity protocol that provides a secure remote connection. the iLO MP supports:

- SSH2 implementation.
- Authentication algorithms RSA and DSA.
- Encryption algorithms 3DES-CBC and AES128-CBC.
- Integrity algorithms HMAC-SHA1 and MD5.

HP Systems Insight Manager (HPSIM) Group Actions

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

Directory-based Secure Authorization Using LDAP

The directory-based authentication and authorization option enables iLO MP user accounts to be defined in a centralized database on an LDAP server. iLO MP users are authenticated when logging in to the iLO MP and authorization is given each time an iLO 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 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 into the iLO 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 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 MP object or privileges, and the only thing the iLO MP queries from the directory server is to authenticate the user name and password.

In normal, or extended, LDAP implementation, if you want to use directory authentication for logging into the iLO 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

A free 30-day evaluation license is available for download on the HP Web site **`http://h71028.www7.hp.com/enterprise/cache/279991-0-0-0-121.html`** The evaluation license activates and accesses iLO MP Advanced features. You can only install one evaluation license per iLO MP. After the evaluation period, an iLO MP Advanced license is required to continue using the advanced features. iLO MP Advanced features automatically deactivate when the evaluation license key expires.

You can use the following iLO MP Advanced Pack features if you have the license:

- Directory-based authentication and authorization using LDAP.
- LDAP Lite: schema-free directory integration.
- Secure shell (SSH) access.
- Group actions through HP Systems Insight Manager (HPSIM).

Obtaining and Activating iLO MP Advanced Pack Licensing (AB500A)

To utilize iLO MP Advanced Pack license features, you must have the iLO MP and the minimum required iLO MP firmware version E.03.13 (see Table 1-1, “Supported Systems and Required Components Matrix,” on page 21 for more details). When you order iLO MP hardware, either separately or when you purchase a new system, you can also order the iLO MP Advanced Pack license. You can order just the iLO MP Advanced Pack license if you already have the iLO MP.

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 and HP 9000 Servers; Certificate of License to Use; License Installation Card* to activate your license.

Supported Systems and Required Components and Cables

There are several ways you can connect to the iLO MP. The connection method depends on the options purchased with your server. The factors in determining which method is available to you depends mainly on the operating system purchased, and whether iLO hardware was purchased or included with your server.

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

Table 1-1 Supported Systems and Required Components Matrix

Supported Systems	Required Components	Required Cables
rx1600 rx1620 rx2620	• iLO hardware; optional • Minimum iLO firmware version: E.03.15	Emulation device connector included with emulation device (not provided by HP).
cx2600 cx2620 rx2600 rp3410 rp3440	• iLO hardware; factory installed • Minimum iLO firmware version: E.03.15	Emulation device connector included with emulation device (not provided by HP).
rx4640 rp4410 rp4440	• I/O baseboard; factory installed • Minimum iLO firmware version: E.03.15	Emulation device connector included with emulation device (not provided by HP).
rx5670	• MP/SCSI Core I/O Card; factory installed • Minimum iLO firmware version: E.03.15	Emulation device connector included with emulation device (not provided by HP).
BL60p	• iLO hardware; factory installed • Minimum iLO firmware version: E.03.15	Local I/O cable Emulation device connector included with emulation device (not provided by HP).

Supported Operating Systems and Browsers

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

For graceful host operating system shutdown, HP Systems Insight Manager integration requires health drivers and management agents or remote console access.

Table 1-2 lists the supported operating systems and browsers.

Table 1-2 Supported Operating Systems and Browsers

Java Runtime Plug-In	**Operating System**					
Version 1.4.2	HPUX	Windows		Linux		VMS
	11.23	XP	WS 2003	Red Hat RHEL 4 U3	SuSE ES/SLE S10	8.3
Browsers						
Mozilla 1.7.12.01.00	X					
Mozilla 1.7.12		X	X			
Internet Explorer 6.0 w/SP1		X	X			
Firefox 1.5		X	X			
Firefox 1.0.7-.4.4.ia64				X		
Mozilla 1.78					X	
OpenVMS Secure Web Browser						

Security

Because iLO has such powerful capabilities to change a computer setup, it is important to have strong security surrounding the iLO device. HP carefully considered security requirements of the enterprise and architected iLO to include authentication, authorization, data integrity, and privacy.

- Authentication is determining who is at the other end of the network connection. iLO incorporates authentication techniques with the use of 128-bit SSL (Secure Socket Layer) encryption.
- Authorization refers to determining whether the user attempting to perform a specific action has the right to perform that action. Using local accounts, iLO 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 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 refers to verifying that no one has altered incoming commands or data. iLO incorporates trusted Java™ applets to verify the integrity of data.
- Privacy: iLO MP uses SSL for Web connections, RSL-RC4 encryption for the 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.

Because iLO 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 devices in the security and network audits and should review the access logs daily.

Security Setup

HP generally recommends that iLO management traffic be on a separate 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.

For security reasons, HP 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. You can create local accounts or use directory services to control user access. See “Modifying User Accounts and Default Password” on page 41.

Protecting 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-write and 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 MP has a robust help system.

Accessing Help Using the TUI

To access the help menu if you 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 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 Indicators

All iLO MP functions are available through the server LAN and the local and remote serial ports. This chapter describes the available iLO MP port connectors, pinouts, and LEDs.

This chapter addresses the following topics:

- “Serial Ports” on page 26
- “iLO MP LAN Port” on page 27

Serial Ports

Figure 2-1 shows the serial port connector with numbered labels for each pin.

Figure 2-1 Serial Port Connector

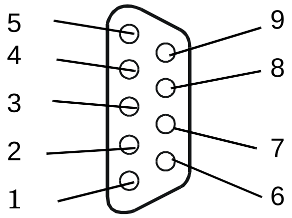


Table 2-1 maps the serial port connector pin number to its signal description.

Table 2-1 Serial Port Pinouts

Pin Number	Signal Description
1	Not applicable
2	Receive data
3	Transmit data
4	Not applicable
5	Ground
6	Not applicable
7	Request to send
8	Clear to send
9	Not applicable

iLO MP LAN Port

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

Figure 2-2 iLO MP LAN Port

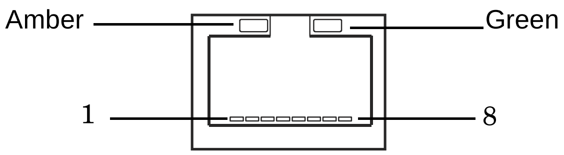


Table 2-2 maps the iLO MP LAN port connector pin number to its signal description.

Table 2-2 iLO 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 MP LAN LEDs (rx4640; rp4410/4440)

The internal iLO MP LAN uses an RJ-45 type connector. This connector has two LEDs (LAN link and LAN activity) that signal status and activity (Figure 2-3).

Figure 2-3 iLO MP LAN LEDs (rx4640; rp4410/4440)

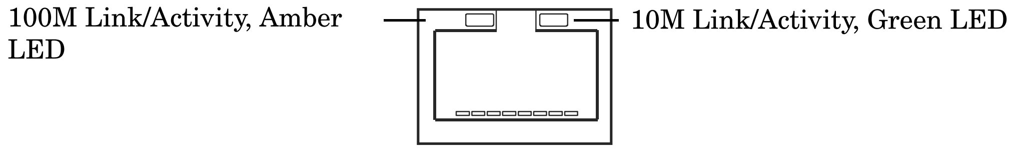


Table 2-3 describes the status of the system when a specific LED condition exists.

Table 2-3 iLO MP LAN LED Status Descriptions (rx4640; rp4410/4440)

LED	Condition	Status
100M amber	Off	Linked at 100 MB/s, no activity
100M amber	On	Linked at 100 MB/s, activity present
10M green	On	Linked at 10MB/s, no activity
10M green	Blinking	Linked at 10MB/s, activity present

iLO MP LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

The iLO MP LAN has four LEDs that signal status and activity (Figure 2-4).

Figure 2-4 iLO MP LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

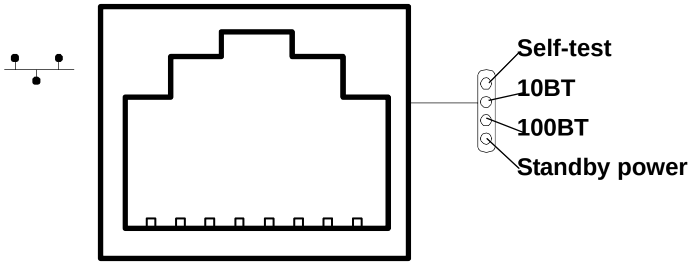


Table 2-4 describes the status of the system when a specific LED condition exists.

Table 2-4 iLO MP LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

LAN LED	Location	Color	State
Self-test	Top	Yellow	iLO MP running selftest or error
		Off	iLO MP has booted
10BT	2nd from top	Green	10BT link established
		Blinking green	10BT activity
		Off	No link or 100BT link
100BT	2nd from bottom	Green	100BT link established
		Blinking green	100BT activity
		Off	No link or 10BT link
Standby Power	Bottom	Green	Standby power on
		Off	Standby power off

iLO MP Reset Button

The iLO MP **Reset** button enables you to reset the iLO MP, and reset the user-specific values to factory default values. A momentary press causes a soft reset of the iLO MP when the button is released. A greater than four second press causes a soft reset of the iLO MP upon release; it also returns user-specific values to factory default values. The following are reset to factory default values:

- serial terminal baud rate settings
- local user accounts and passwords

Resetting Local User Accounts and Passwords to Default Values

If iLO MP user passwords have been lost, or iLO 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:

Step 1. Connect a serial terminal (or serial-cabled laptop with serial emulation, for example) to the iLO MP serial port.

Step 2. Press and hold the iLO MP **Reset** button for > 4 seconds. The iLO MP reboots and displays a prompt that asks if you want to reset the passwords.

Step 3. Respond to the prompt to reset local user accounts and passwords to default values.

3 Console Connection and Setup

Setting up the console involves the following:

- Determining the physical access method to connect cables. There are two physical connections to the Integrity iLO MP: RS-232 and LAN.
- Configuring the Integrity iLO 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
  - — Local RS-232 serial port
  - — Remote/modem port

This chapter addresses the following topics:

Setup Checklist

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

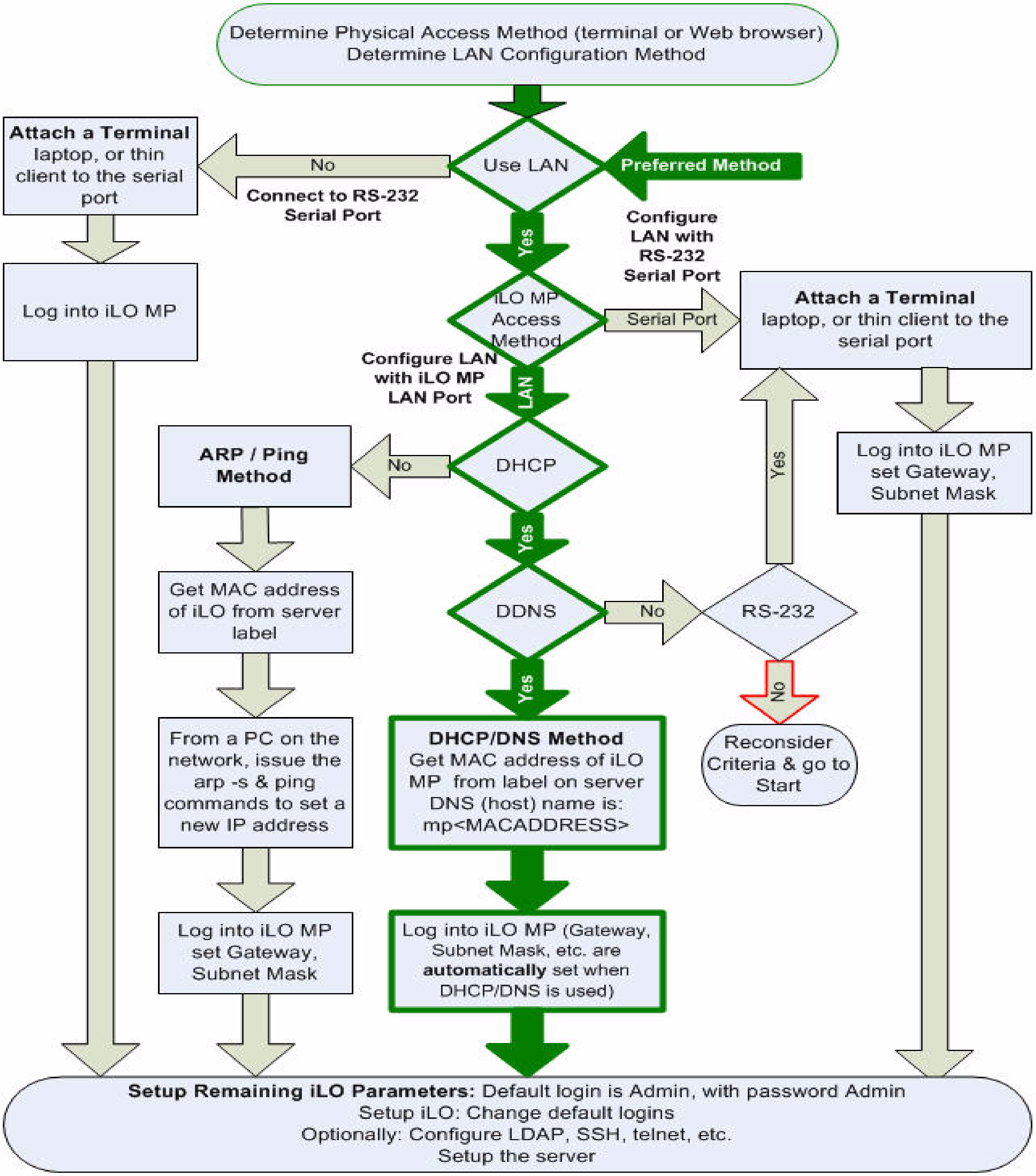
Table 3-1 Setup Checklist

	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 MP LAN	There are three methods to configure the LAN for iLO MP access: • DHCP with DNS • ARP Ping • RS-232 serial port	
3	Log on to the iLO MP	Log in to the iLO 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.	
7	Access the host console	Access the host console using the method of choice.	
	Advanced		
	Activate Advanced Pack Features	Activate advanced features by entering a license key.	

Setup Flowchart

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

Figure 3-1 iLO MP Setup Flowchart


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

Preparation

There are several tasks to perform before you can configure the iLO MP LAN.

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

Determining the Physical iLO MP Access Method

Before you can access the iLO MP, you must first determine the correct physical connection method. The iLO 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 your server installation guide for rear panel console connection port identification and cable connection information.

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

Table 3-2 Console Connection Matrix

Operating System	Console Connection Method	Required Connection Components
HP-UX	Local RS-232 serial port Remote/modem port	1. M-cable: DB25 connector on one end, and three DB-9F connectors on the other end: • Console • Remote • UPS 2. RS-232 DB-9F to DB-9F cable 3. Console device (for example, a laptop or ASCII terminal)
	LAN port	10/100 LAN cable
Linux	Local RS-232 serial port Remote/modem port	1. M-cable: DB25 connector on one end, and three DB-9F connectors on the other end: • Console • Remote • UPS 2. RS-232 DB-9F to DB-9F cable 3. Console device (for example, a laptop or ASCII terminal)
	LAN port	10/100 LAN cable

Table 3-2 Console Connection Matrix (Continued)

Operating System	Console Connection Method	Required Connection Components
OpenVMS	Local RS-232 serial port Remote/modem port	1. M-cable: DB25 connector on one end, and three DB-9F connectors on the other end: • Console • Remote • UPS 2. RS-232 DB-9F to DB-9F cable 3. Console device (for example, a laptop or ASCII terminal)
	LAN Port	10/100 LAN cable
Windows	VGA Port (no iLO MP access; EFI only)	1. Monitor (VGA) 2. Keyboard (USB) 3. Mouse (USB)
	LAN port	10/100 LAN cable

Determining the iLO MP LAN Configuration Method

To access the iLO MP through the iLO MP LAN, the iLO MP must acquire an IP address. The way the iLO 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 MP access, you must determine how you will configure the iLO MP LAN in order to acquire an IP address using the following methods:

- DHCP/DNS
- ARP Ping
- Local S-232 serial port
- Remote/modem port

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	RS-232 Serial Port (MP LC command)	LAN Configuration Method
Yes	Yes	No	DHCP
Yes	Yes	Yes	DHCP, RS-232 serial port, or remote/modem port
No	No	No	ARP Ping

Table 3-3 LAN Configuration Methods (Continued)

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

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

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

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

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.

When you use DHCP and DNS, you can connect to the iLO 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 and the primary DNS server IP address.
- The primary DNS server accepts dynamic DNS (DDNS) updates.
- The primary DNS server IP address has been configured through the DHCP server.

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

Step 1. Obtain the factory-set host name from the iLO 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 MP core I/O board. The core I/O board has a unique MAC address that identifies the hardware on the network.

IMPORTANT Make sure you obtain the MAC address to the core I/O board and not the MAC address to the server core LAN card.

Step 2. Connect the LAN cable from the server to an active network port.

Step 3. Apply ac power to the server.

Step 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 MP Log In** window opens.

Step 5. Log in using the default user name and password.

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

HP strongly recommends you assign user groups and rights before proceeding. See “Modifying User Accounts and Default Password” on page 41.

Configuring the iLO MP LAN Using ARP Ping

The Address Resolution Protocol (ARP) and Packet Internet Grouper (Ping) utility uses ARP packets to ping, or 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.

ARP Ping operational issues:

- You can use ARP Ping regardless of the status of DHCP unless an IP address has ever been acquired using DHCP.
- When ARP Ping is successful, DHCP status is disabled.
- Some DHCP server options can cause the apparent issuance of ARP Ping to the iLO MP which will negate the DHCP/DDNS method.
- 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 MP is booted. This applies to every subsequent boot of the iLO MP until an IP address is obtained by DHCP or has been assigned by using the `LC` command or ARP Ping succeeds.

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, log into it, and 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 MP MAC address. This ARP table entry maps the MAC address of the iLO MP LAN interface to the static IP address designated for that interface.
`ping`	This command tests network connections. It verifies the iLO 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:

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

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

Step 2. Verify that an active LAN cable on the local subnet is connected to the iLO MP LAN port on the server.

Step 3. Access a PC on the same physical subnet as the server.

Step 4. Open a DOS window on the PC.

Step 5. At the DOS prompt, 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 MAC address>
```

Example from Windows

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

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

Step 7. Use this IP address to connect to the iLO MP LAN.

Step 8. Use Web or telnet access to connect to the iLO MP from a host on the local subnet and complete the rest of the LAN parameter (gateway, subnet).

Configuring the iLO MP LAN Using the RS-232 Serial Port

To configure the iLO MP LAN using the RS-232 serial port, 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 server 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 RS-232 serial port or a network connection through the LAN to access the iLO MP and use the `LC` command.

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

Step 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.

Step 2. Use Table 3-2 to determine the required connection components, and the ports used to connect the server to the console device.

Step 3. Connect the cables.

Step 4. Start the emulation software on the console device.

Step 5. Log in to the iLO MP. See “Logging In to the iLO MP” on page 40.

Step 6. At the **MP Main Menu**, enter **`CM`** and press **Enter** to select command mode.

Step 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.

Step 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 MP.

Step 9. Use the `LC` command to enter information for the IP address, host, subnet mask, gateway parameters, and so on.

Step 10. Enter **XD -R** to reset the iLO MP.

Step 11. After the iLO MP resets, log in to the iLO MP again and enter **CM** at the **MP:>** prompt.

Step 12. Enter **LS** to confirm that DHCP is disabled and display a list of updated LAN configuration settings.

Logging In to the iLO MP

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

Step 1. Access the iLO MP using the LAN, RS-232 serial port, telnet, SSH, or Web method. The iLO MP login prompt displays.

Step 2. Log in using the default the iLO 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” on page 41.

Following is the **MP Main Menu**:

```
MP MAIN MENU:
        CO: Console
       VFP: Virtual Front Panel
        CM: Command Menu
        CL: Console Logs
        SL: Show Event Logs
        HE: Main Menu Help
         X: Exit Connection
```

See Chapter 7, “Command Menu Interface Reference,” on page 85 for information on the iLO MP menus and commands.

When logging in using the local or remote RS-232 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 iLO MP prompt (`MP>`).

Additional Setup

This section provides additional information to setup the iLO MP.

Modifying User Accounts and Default Password

The iLO 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 MP user interfaces.

To modify default account configuration settings, follow these steps:

Step 1. Log in as the administrator. You must log in as the administrator in order to modify default user configuration settings

Step 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.

Step 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 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 allows 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” on page 41.

Security Access Settings

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

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

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

- Change the default user name and password. See “Modifying User Accounts and Default Password” on page 41).
- Create local accounts. You can store up to 19 user names and passwords to manage iLO 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 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 8, “Directory Services Installation and Configuration,” on page 99 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 Host Console With the TUI - CO Command" on page 43
- "Interacting with the iLO MP Using the Web GUI" on page 43
- "Accessing the Graphic Console Using VGA" on page 46

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 MP, follow these steps:

Step 1. Log in using your user account name and password at the login page.

Step 2. At the iLO MP login prompt (`MP>`), enter the `CO` command to switch the console terminal from the **MP Main Menu** to mirrored/redirected console mode. All mirrored data is displayed.

Step 3. To return to the iLO MP command interface, type **Ctrl-B**, or **Esc** and **(**.

Interacting with the iLO MP Using the Web GUI

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

The iLO 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 MP LAN and not the MAC address to the server core LAN.

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

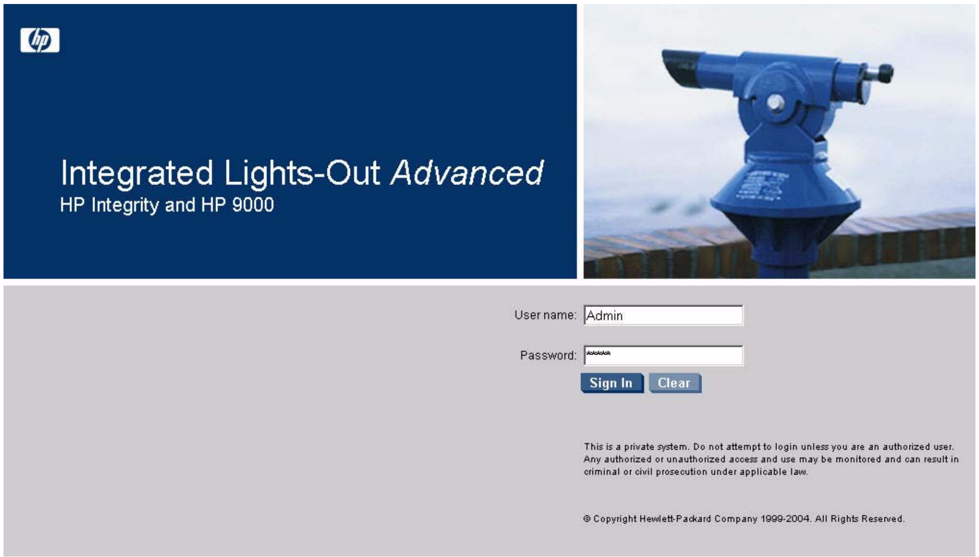
- IP address for the iLO MP LAN
- Host name (this is used when messages are logged or printed)

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

Step 1. Open a Web browser and enter the host name or the IP address for the iLO MP.

Step 2. Log in using your user account name and password at the login page. (Figure 4-1).

Figure 4-1 Web Login Page



Integrated Lights-Out *Advanced*
HP Integrity and HP 9000

User name: Admin

Password: ******

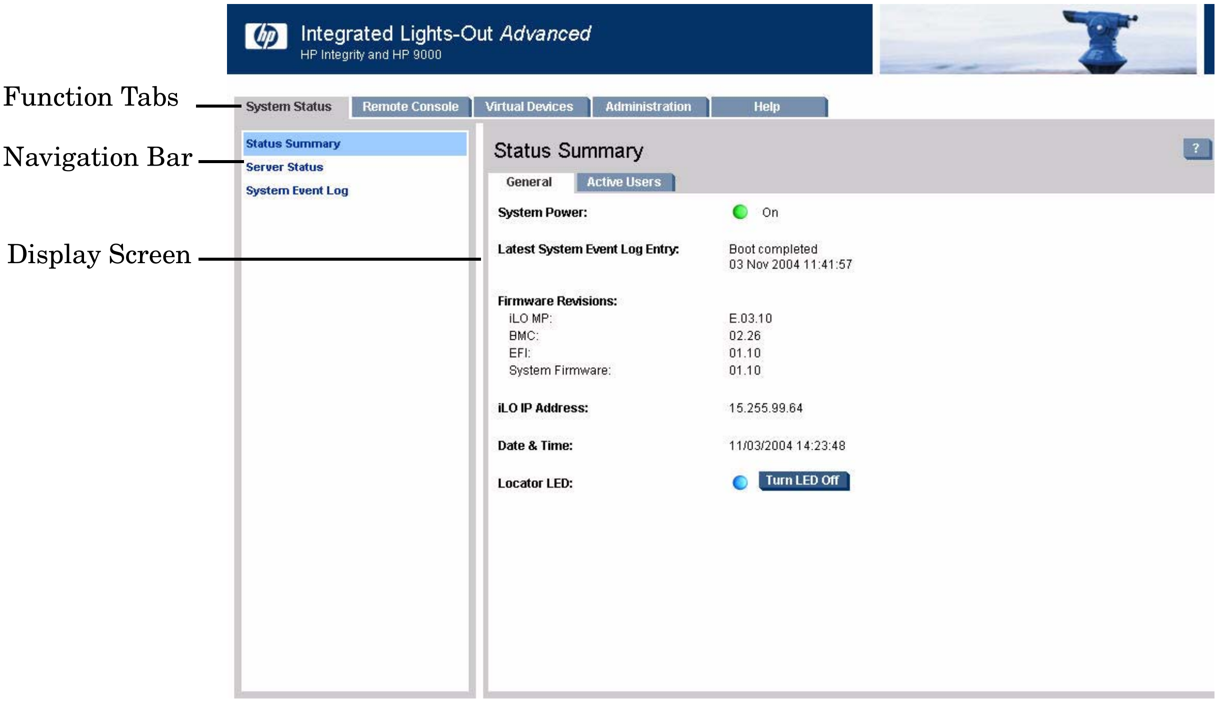
This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

© Copyright Hewlett-Packard Company 1999-2004. All Rights Reserved.

Step 3. Click **Sign In**. The **Status Summary** page (Figure 4-2) displays after login.

NOTE The iLO 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.

Figure 4-2 Status Summary Page



Status Summary

System Power: On

Latest System Event Log Entry: Boot completed
03 Nov 2004 11:41:57

Firmware Revisions:
iLO MP: E.03.10
BMC: 02.26
EFI: 01.10
System Firmware: 01.10

iLO IP Address: 15.255.99.64

Date & Time: 11/03/2004 14:23:48

Locator LED:

Step 1. To select the Web interface functions, click the **Function** tabs at the top of the page. Each function lists options in the **Navigation Bar** on the left side of the page.

Step 2. Click an option link to display data in the **Display** screen; and click **Refresh** to update the display.

Step 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 MP Web interface has a robust help system. To launch iLO 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 Graphic Console Using VGA

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

NOTE You cannot access the iLO 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 RS-232 serial port method to view console output prior to booting to the EFI Shell or to access the iLO MP. See “Configuring the iLO MP LAN Using the RS-232 Serial Port” on page 39.

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

Step 1. Perform preparation tasks.

Step 2. Connect the cables. See your user service guide 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.

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

NOTE The HPUX system name visible through a `uname -a` command is different than the iLO 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 iLO MP `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:

Step 1. At the **MP Main Menu** prompt (`MP>`), enter **`CM`** to select command mode.

Step 2. At the command mode prompt (`MP:CM>`), enter **`DNS`** (for the DNS configuration). The screen displays `current DNS` data.

Step 3. When prompted to enter a parameter name, `A to modify All`, or `Q to Quit`, enter **`A`** to select all parameters. The screen displays the current DHCP for DNS servers status.

Step 4. When prompted, enter **`Enabled`**, or **`Disabled`**. The screen displays the current DHCP for DNS domain name status.

Step 5. When prompted, enter **`Enabled`**, or **`Disabled`**. The screen displays the current register with DDNS server value.

Step 6. When prompted, enter, **`Yes`**, or **`No`**. The screen displays the current DNS domain name.

Step 7. When prompted, enter a new value. The screen displays the primary DNS server IP address.

Step 8. When prompted, enter a new value. The screen displays the optional secondary DNS server IP address.

Step 9. When prompted, enter a new value. The screen displays the optional tertiary DNS server IP address.

Step 10. When prompted, enter a new value.

The DNS configuration is updated as follows:

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

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

Enter parameter(s) to revise, Y to confirm, or [Q] to Quit: Y
-> DNS Configuration has been updated
[mpserver] MP:CM>
```

Configuring LDAP Extended Schema

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

NOTE The LDAP connection has an inactivity timeout of 30 minutes.

To configure using the Web interface, see “Administration > Directory Settings > LDAP Parameters” on page 79.

NOTE You can only use the LDAP feature if you have iLO MP Advanced Pack licensing.

Step 1. At the **MP Main Menu** prompt (`MP>`), enter **`CM`** to select command mode.

Step 2. At the command mode prompt (`MP:CM>`), enter **`LDAP`** (for the LDAP configuration).

Step 3. Enter **`D`** to select **Directory Settings**. The screen displays the current LDAP directory settings.

Step 4. Enter **`A`** to select all parameters. The screen displays the current LDAP directory authentication status.

Step 5. 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 MP user accounts database status. If enabled, the local iLO MP user database is used if there is an authentication failure using the LDAP Directory.

Step 6. 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.

Step 7. Enter the IP address of the LDAP server. The screen displays the current LDAP server port address.

Step 8. Enter a new port number. The screen displays the current object distinguished name. This specifies the full distinguished name of the iLO MP device object in the directory service. For example, CN=RILOE2OBJECT, CN=Users, DC=HP, DC=com. Distinguished names are limited to 255 characters plus one for the terminating NULL character.

Step 9. Enter a new name. The screen displays the current user search context 1.

Step 10. 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 plus one for the terminating NULL character each.

Step 11. Enter a new search setting. The screen displays the current user search context 3.

Step 12. 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 the iLO MPs. The iLO 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 MP. The iLO MP accesses the directory service to determine which roles are available for that user login. The iLO MP first uses the credentials to access the iLO 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 MP device object and the role object, the iLO MP determines the role object's distinguished name and the associated user privileges. The iLO MP then calculates the current user privileges based on those roles and grants them to that user.

Configuring LDAP Lite Default Schema

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

NOTE You can only use the LDAP feature if you have iLO MP Advanced Pack licensing.

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

- Easy implementation without schema extensions - iLO MP schema-free integration is configured from any iLO MP user interface (browser, command line or script).
- Minimal administration and maintenance:
  - after initial setup, only groups and permissions require maintenance support on iLO MPs; typically group and permission changes occur infrequently
  - the schema-free approach does not require updating directory databases with new iLO MP devices objects

- Reliable security - iLO MP schema-free does not affect standard directory attributes avoiding conflicting use of attributes that might result over time.
- Complements two-factor authentication - iLO MP schema-free integration can be used in conjunction with iLO 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 MP schema at this time.

To configure LDAP Lite you need to:

1. Follow the procedure for configuring "Configuring LDAP Extended Schema" on page 50 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 procedures describes how to set up directory security groups in LDAP Lite using the iLO MP text interface. To configure using the Web interface, see "Administration > Directory Settings > Group Administration" on page 81.

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.

Step 1. At the command mode prompt (MP:CM>), 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
```

Step 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:
```

Step 3. Enter the number for the group you want to view or modify. The screen displays the current LDAP group settings.

Step 4. Set up a group distinguished name.

Step 5. Select rights for the group.

Step 6. Enter **`Y`** to confirm.

Login Process Using Directory Services without Schema Extensions

You can control access to the iLO MP using directories without requiring schema extensions. The iLO MP acquires the user's name to determine group membership from the directory. The iLO MP then cross-references the group names with its locally-stored names to determine user privilege level. The iLO MP must be configured with the appropriate group names and their associated privileges. You can accomplish this configuration through one of the following options:

- Web interface: use the **Administration > Directory Settings > Group Administration** page.
- iLO MP text interface: use the `LDAP` command.

6 Web Graphical User Interface

One of the methods available to access the iLO 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 MP Advanced Pack license. For more information on the iLO MP Advanced Pack license, see “Advanced Pack License” on page 20, 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 log in to the iLO MP Web GUI.

See “Interacting with the iLO MP Using the Web GUI” on page 43 for information on how to access the iLO MP Web interface.

This chapter addresses the following topics:

- “System Status” on page 56
- “Remote Console” on page 62
- “Virtual Devices” on page 65
- “Administration” on page 67
- “Help” on page 84

System Status

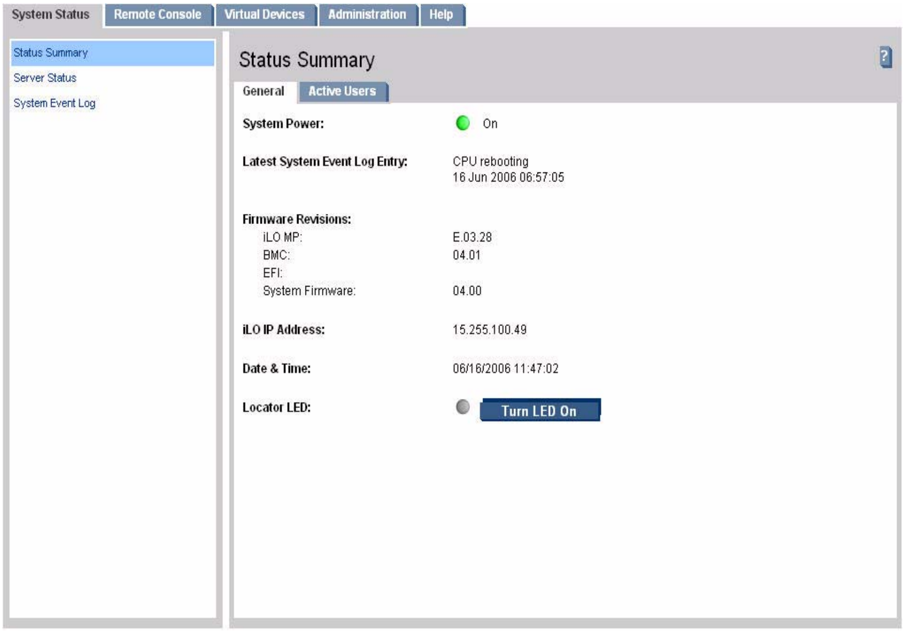
The **System Status** tab enables you to access the following pages:

- 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 6-1) displays a brief status summary of the system.

Figure 6-1 System Status Summary General Page



Status Summary

System Power:	● On
Latest System Event Log Entry:	CPU rebooting 16 Jun 2006 06:57:05
Firmware Revisions:	
iLO MP:	E.03.28
BMC:	04.01
EFI:	
System Firmware:	04.00
iLO IP Address:	15.255.100.49
Date & Time:	06/16/2006 11:47:02
Locator LED:	● Turn LED On

Fields and descriptions are as follows:

Table 6-1 Status Summary General Page Description

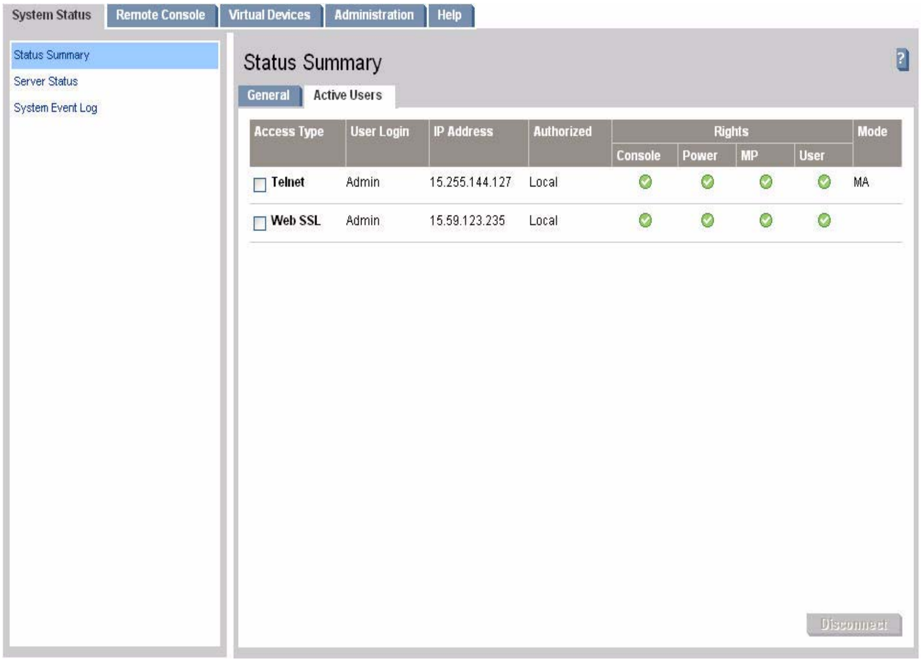
Fields	Description
System Power	The current power state (ON/OFF/STANDBY) of the system along with the corresponding power LED state.
Latest System Event Log Entry	The most recent entry in the System Event Log (SEL).
Firmware Revisions	The current revisions of firmware (iLO MP , BMC, system firmware).
iLO MP IP Address	The IP address of the iLO MP subsystem.
Date & Time	Displays the date and time as known to the iLO MP.
Locator LED	The status of the (Blue) Locator or Unit Identifier (UID) LED and enables you to turn the Locator LED on or off.

System Status > Status Summary > Active Users

The **Active Users** page (Figure 6-2) displays information about the users currently logged in to the iLO MP.

The **Disconnect** button enables a user with sufficient privileges to disconnect users of a certain access type.

Figure 6-2 System Status Summary Active Users Page



Access Type	User Login	IP Address	Authorized	Rights				Mode
				Console	Power	MP	User	
□ Telnet	Admin	15.255.144.127	Local	✓	✓	✓	✓	MA
□ Web SSL	Admin	15.59.123.235	Local	✓	✓	✓	✓	

Fields and descriptions are as follows:

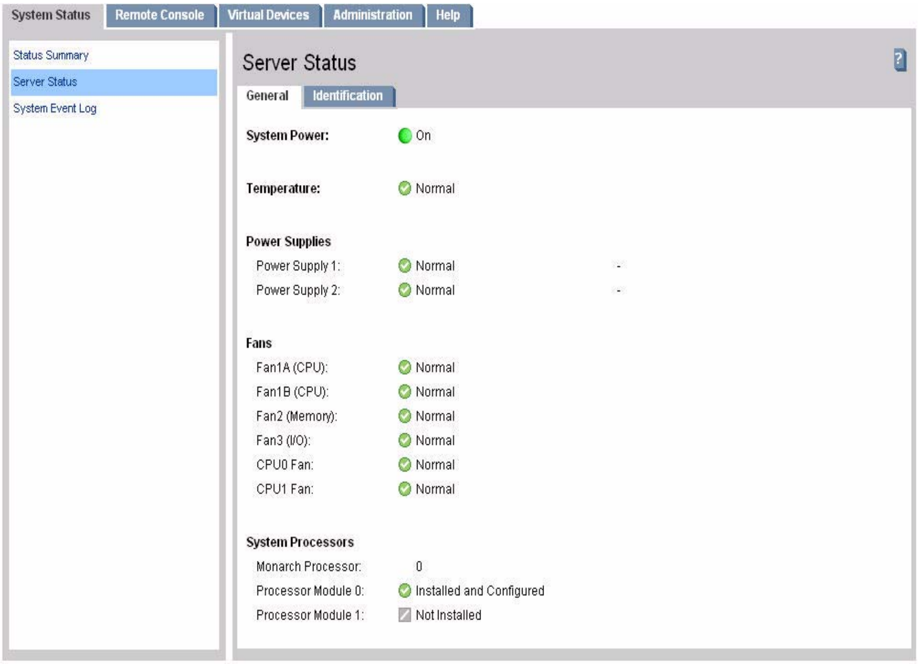
Table 6-2 Active Users Page Description

Field	Description
Access Type	There are multiple access methods: Serial, telnet, SSH, SSL, or Web.
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 MP user accounts (Local).
Rights	Rights control the iLO MP functions a user can perform. There are four user access rights: console access, iLO MP configuration, power control, and user administration. A user can be configured to have some, none, or all the access rights.
Mode	Current iLO MP mode that the user is in. Text user interface modes are: MA, main MP 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 6-3) 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 6-3 System Status > Server Status General Page



System Power: ● On

Temperature: ✓ Normal

Power Supplies
Power Supply 1: ✓ Normal -
Power Supply 2: ✓ Normal -

Fans
Fan1A (CPU): ✓ Normal
Fan1B (CPU): ✓ Normal
Fan2 (Memory): ✓ Normal
Fan3 (I/O): ✓ Normal
CPU0 Fan: ✓ Normal
CPU1 Fan: ✓ Normal

System Processors
Monarch Processor: 0
Processor Module 0: ✓ Installed and Configured
Processor Module 1: ▨ Not Installed

Fields and descriptions are as follows:

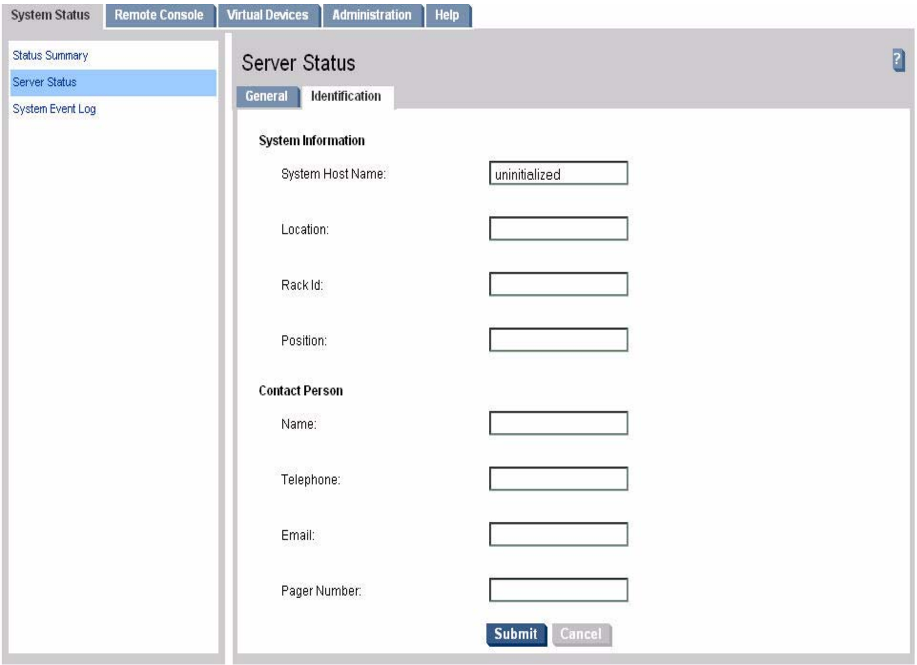
Table 6-3 Server Status General Page Description

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.

System Status > Server Status > Identification

The **Identification** page (Figure 6-4) enables you to configure system information for identifying the server.

Figure 6-4 System Status > Server Status Identification Page



System Information

System Host Name: uninitialized

Location:

Rack Id:

Position:

Contact Person

Name:

Telephone:

Email:

Pager Number:

Enter the default host name. Obtain the factory-set host name from the 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 Media Access Protocol (MAC) (example: mp0014c29c064f). This address is assigned to the iLO MP hardware. This unique MAC address identifies the iLO MP hardware on the network.

IMPORTANT Make sure you obtain the MAC address to the iLO MP hardware and not the MAC address to the server core LAN card. See your server user guide for information on where the label is located.

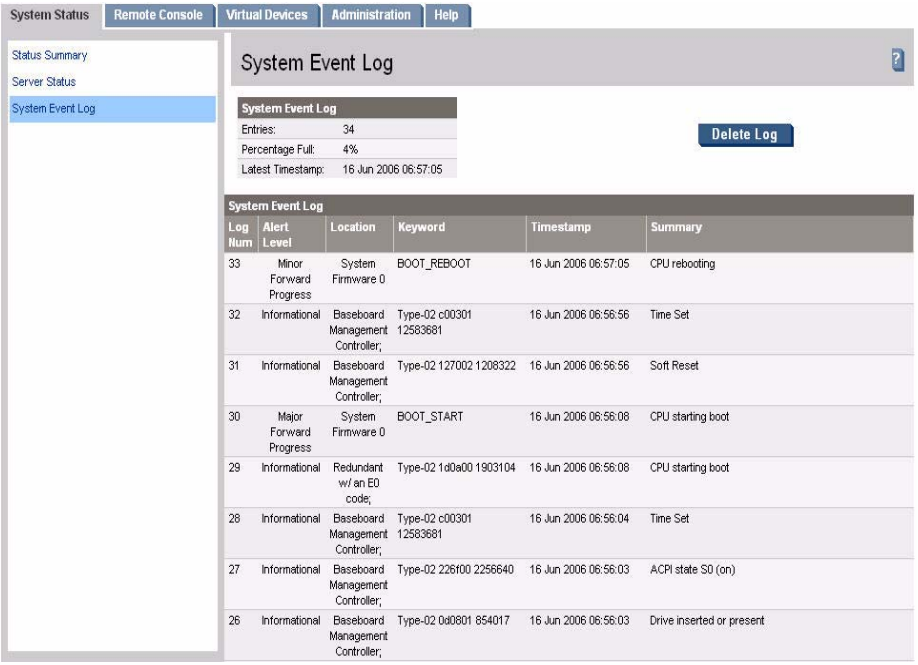
Enter the relevant details like location, rack id, position, contact person name, telephone number, e-mail, and pager number.

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

System Status > System Event Log

The **System Event Log** page (Figure 6-5) enables a user 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 configuration access right can clear the logs.

Figure 6-5 System Status > System Event Log Page



System Event Log	
Entries:	34
Percentage Full:	4%
Latest Timestamp:	16 Jun 2006 06:57:05

System Event Log

Log Num	Alert Level	Location	Keyword	Timestamp	Summary
33	Minor Forward Progress	System Firmware 0	BOOT_REBOOT	16 Jun 2006 06:57:05	CPU rebooting
32	Informational	Baseboard Management Controller;	Type-02 c00301 12583681	16 Jun 2006 06:56:56	Time Set
31	Informational	Baseboard Management Controller;	Type-02 127002 1208322	16 Jun 2006 06:56:56	Soft Reset
30	Major Forward Progress	System Firmware 0	BOOT_START	16 Jun 2006 06:56:08	CPU starting boot
29	Informational	Redundant w/ an E0 code;	Type-02 1d0a00 1903104	16 Jun 2006 06:56:08	CPU starting boot
28	Informational	Baseboard Management Controller;	Type-02 c00301 12583681	16 Jun 2006 06:56:04	Time Set
27	Informational	Baseboard Management Controller;	Type-02 226f00 2256640	16 Jun 2006 06:56:03	ACPI state S0 (on)
26	Informational	Baseboard Management Controller;	Type-02 0d0801 854017	16 Jun 2006 06:56:03	Drive inserted or present

The system event log contains the following errors and priority events.

Table 6-4 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	All events. 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”.
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 into the iLO 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 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

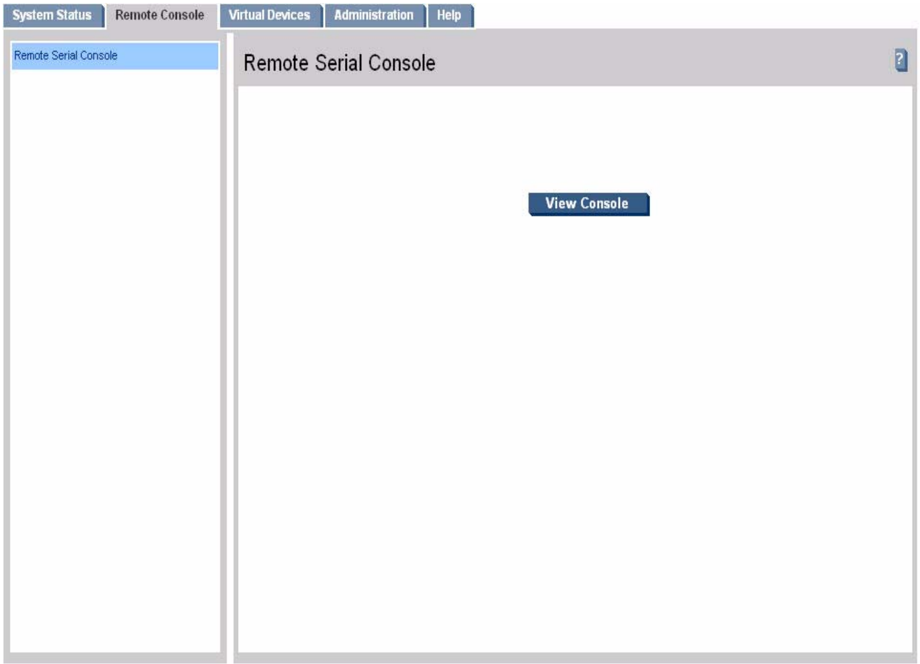
7: Fatal

Remote Console

Remote Console > Remote Serial Console

The **Remote Serial Console** page (Figure 6-6) enables you to securely view and manage a remote server. Only a user with console access right can use this feature.

Figure 6-6 Remote Console > Remote Serial Console



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. This port is configurable 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 MP.

NOTE Pop-up blocking applications will prevent remote serial console from running. Disable any pop-up blocking applications before starting remote serial console.

The iLO MP mirrors the system console to the iLO 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 MP terminal setting in the applet is correct.

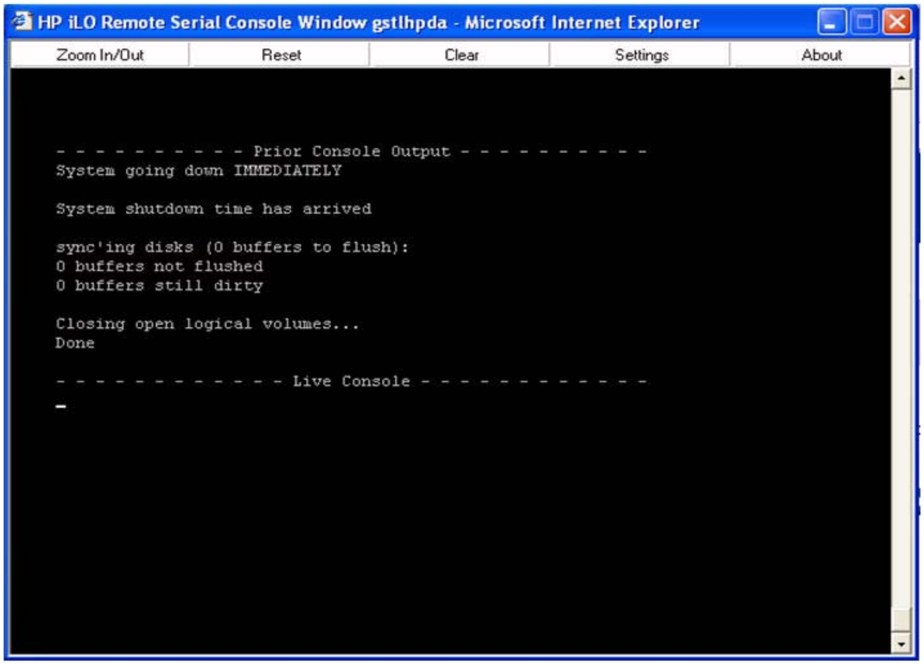
- The operating system environment settings and your client terminal type are set properly.
- All mirrored consoles are of the same terminal type for proper operation. Supported terminal types are:
  — VT100
  — VT100+ (default terminal type)
  — VT-UTF8

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

To connect to the system console (Figure 6-7), click **Launch**.

NOTE If the **Launch** button is disabled, the user does not have console access rights. See the **User Administration** page under the **Administration** tab to add this access right.

Figure 6-7 Remote Console > Remote Serial Console > View Console


HP iLO Remote Serial Console Window gstlhpda - Microsoft Internet Explorer
Zoom In/Out
Reset
Clear
Settings
About

```
- - - - - - - - - - Prior Console Output - - - - - - - - - -
System going down IMMEDIATELY

System shutdown time has arrived

sync'ing disks (0 buffers to flush):
0 buffers not flushed
0 buffers still dirty

Closing open logical volumes...
Done

- - - - - - - - - - - - Live Console - - - - - - - - - - - -
_
```

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.

As long as the remote serial console window is open, the iLO MP Web interface does not timeout. The remote serial console window remains open until you sign out of the iLO MP interface using the provided link in the banner, leave the iLO MP site, or refresh the entire page.

The remote serial console provides the console, and the GUI provides the iLO MP 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 option relies on the virtual serial port.

Virtual Serial Port

The iLO 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 MP. The iLO MP converts the serial data stream to be available remotely through the remote serial console. 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 the iLO MP, an administrator can access a console application such as Windows EMS remotely over the network. The iLO MP contains the functional equivalent of the standard serial port (16550 UART) register set, and the iLO MP firmware provides a Java applet that connects to the server serial port. If the serial redirection feature is enabled on the host server, the iLO MP intercepts the data coming from the serial port, encrypts it, and sends it to the Web browser applet.

For Linux users, the iLO MP 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 MP virtual serial port feature to remotely login to the Linux operating system over the network.

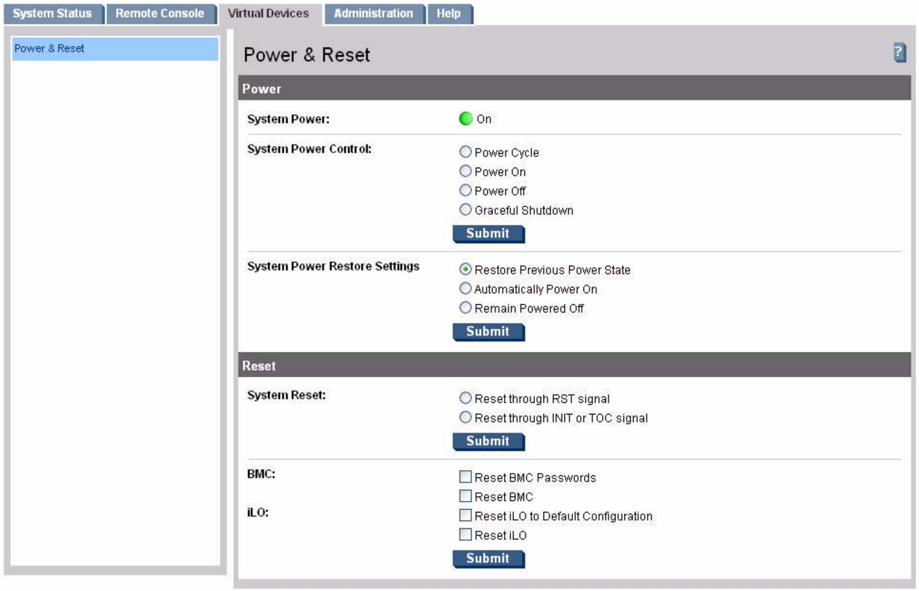
For more information on using the virtual serial port, see *Integrated Lights-Out Virtual Serial Port configuration and operation HOW TO*, at:
`http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00263709/c00263709.pdf`

Virtual Devices

The **Virtual Devices** tab enables you to access the **Power & Reset** page.

The **Power & Reset** page (Figure 6-8) enables you to view and control the power state of the server. It also provides you with options to reset the system, the BMC, or iLO MP.

Figure 6-8 Virtual Devices > Power & Reset Page



Power & Reset

Power

System Power: ● On

System Power Control:
○ Power Cycle
○ Power On
○ Power Off
○ Graceful Shutdown

System Power Restore Settings
● Restore Previous Power State
○ Automatically Power On
○ Remain Powered Off

Reset

System Reset:
○ Reset through RST signal
○ Reset through INIT or TOC signal

BMC:
□ Reset BMC Passwords
□ Reset BMC

iLO:
□ Reset iLO to Default Configuration
□ Reset iLO

Fields and descriptions are as follows:

Table 6-5 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.

Table 6-5 Power & Reset Page Description (Continued)

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

Administration

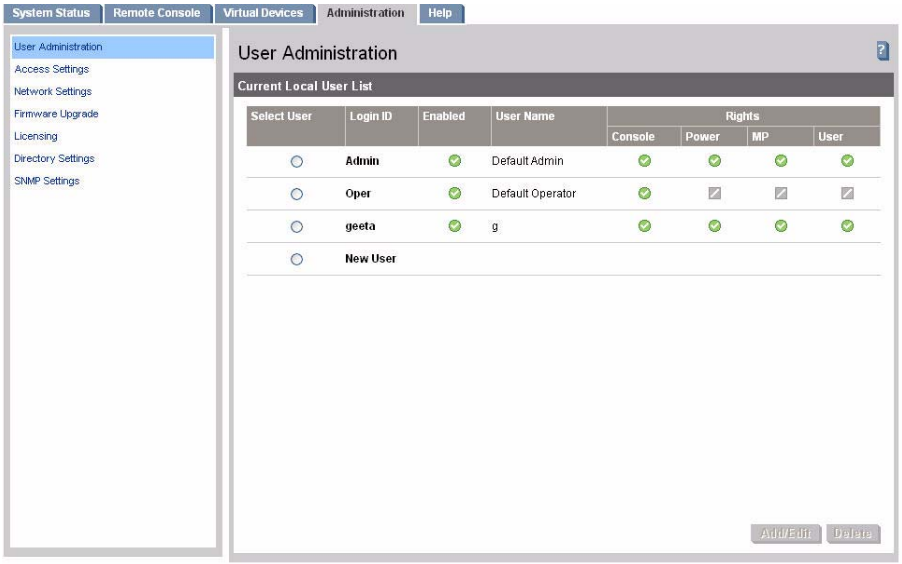
The **Administration** tab enables you to access the following pages:

- User Administration
- Access Settings: LAN, Serial, and Login Options
- Network Settings: Standard and Domain Name Server
- Firmware Upgrade
- Licensing
- Directory Settings: LDAP Parameters and Group Administration
- SNMP Settings
- Help

Administration >User Administration

The **User Administration** page (Figure 6-9) 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 MP, add new users assign rights, and modify or delete existing users. Only a user with administration access right can use this feature.

Figure 6-9 User Administration Page



User Administration

Current Local User List

Select User	Login ID	Enabled	User Name	Rights			
				Console	Power	MP	User
○	Admin	✓	Default Admin	✓	✓	✓	✓
○	Oper	✓	Default Operator	✓	▨	▨	▨
○	geeta	✓	g	✓	✓	✓	✓
○	New User						

There are two default users:

1. Admin: The Admin user has all four rights (console access, power control, MP configuration, user administration).
2. Oper: The Oper user has the login and console access rights by default.

Fields and descriptions are as follows:

Table 6-6 User Administration 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.

NOTE The HP System's Insight Manager group actions feature for iLO MP utilizes the **Admin** user account, modifying or removing the **Admin** user could cause a problem.

Administration > Access Settings

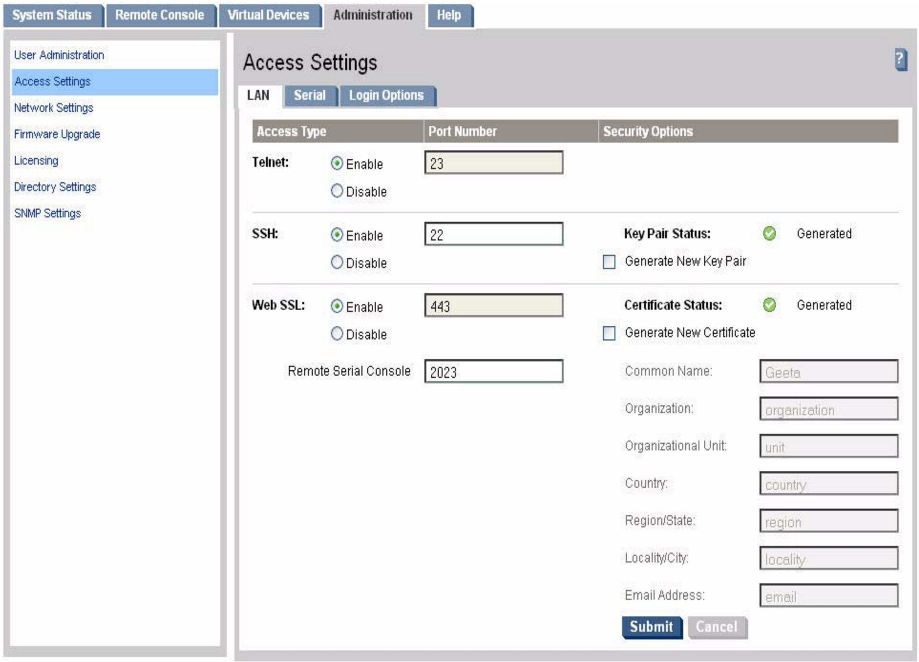
The **Access Settings** tab enables you to access the following pages:

- LAN
- Serial
- Login Options

Administration > Access Settings > LAN

The **LAN** page (Figure 6-10) enables you to modify the LAN settings. Only a user with configuration access right can use this feature.

Figure 6-10 Administration > Access Settings > LAN Page



Access Settings

Access Type		Port Number	Security Options	
Telnet:	● Enable ○ Disable	23		
SSH:	● Enable ○ Disable	22	Key Pair Status: □ Generate New Key Pair	✓ Generated
Web SSL:	● Enable ○ Disable	443	Certificate Status: □ Generate New Certificate	✓ Generated
Remote Serial Console		2023	Common Name:	Geeta
			Organization:	organization
			Organizational Unit:	unit
			Country:	country
			Region/State:	region
			Locality/City:	locality
			Email Address:	email

Use the following options to modify the LAN settings:

Table 6-7 LAN Page Description

Fields and Buttons	Description
Telnet	These options are used to enable or disable telnet access to the iLO MP.

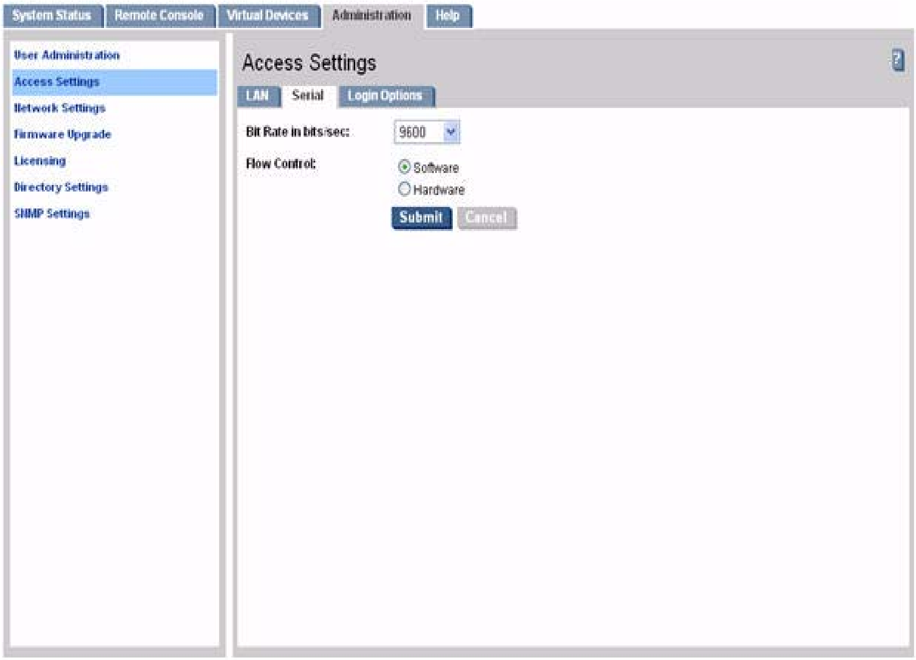
Table 6-7 LAN Page Description (Continued)

Fields and Buttons	Description
SSH	An industry-standard client-server connectivity protocol that provides a secure remote connection. The iLO MP supports: • SSH2 implementation • Authentication algorithms RSA and DSA • Encryption algorithms 3DES-CBC and AES128-CBC • Integrity algorithms HMAC-SHA1 and MD5 The iLO MP Advanced Pack license is required for this feature.
Web SSL	You can enable or disable the Web SSL access to the iLO 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 > Access Settings > Serial

The **Serial** page (Figure 6-11) enables you to set the serial port parameters. Only a user with configuration access right can use this feature.

Figure 6-11 Administration > Access Settings > Serial Page



Bit Rate in bits/sec: 9600

Flow Control: ● Software ○ Hardware

Fields and descriptions are as follows:

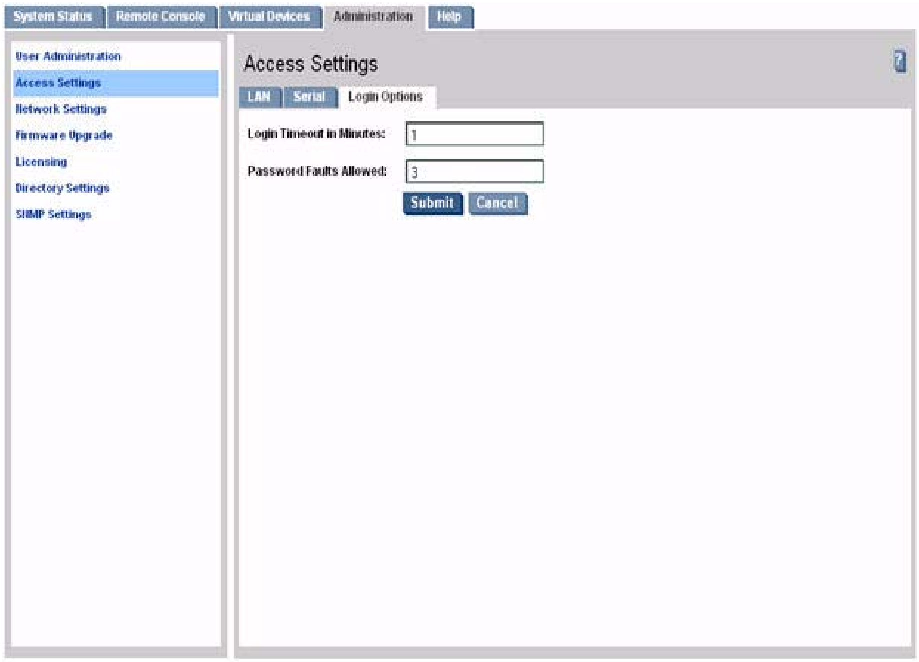
Table 6-8 Serial Page Description

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 > Access Settings > Login Options

The **Login Options** page (Figure 6-12)enables you to modify the security options of the iLO MP. Only a user with configuration access right can use this feature.

Figure 6-12 Administration > Access Settings > Login Options Page



Login Timeout in Minutes: 1

Password Faults Allowed: 3

Fields and descriptions are as follows.

Table 6-9 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 into the iLO MP. The default number of password faults allowed is three
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

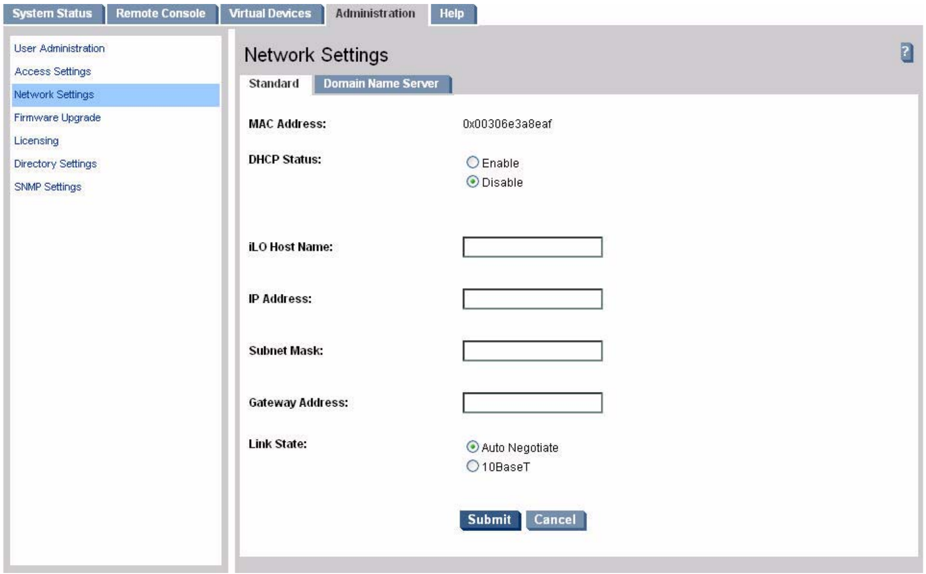
IMPORTANT If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, the iLO MP automatically resets once you confirm the change. The automatic reset occurs only after a warning displays before you commit the changes. If you enter `-nc`, no warning displays and the iLO 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 MP alerts you to manually reset the iLO MP. A warning about dropped network connections is sent prior to committing the change. The warning does not display if you enter `-nc`.

Administration > Network Settings > Standard

The **Standard** page (Figure 6-13) enables you to configure the network settings. Only a user with configuration access right can configure the network settings.

Figure 6-13 Administration > Network Settings > Standard Page



Network Settings

MAC Address: 0x00306e3a8eaf

DHCP Status: ○ Enable ● Disable

iLO Host Name:

IP Address:

Subnet Mask:

Gateway Address:

Link State: ● Auto Negotiate ○ 10BaseT

Fields and descriptions are as follows:

Table 6-10 Standard Page Description

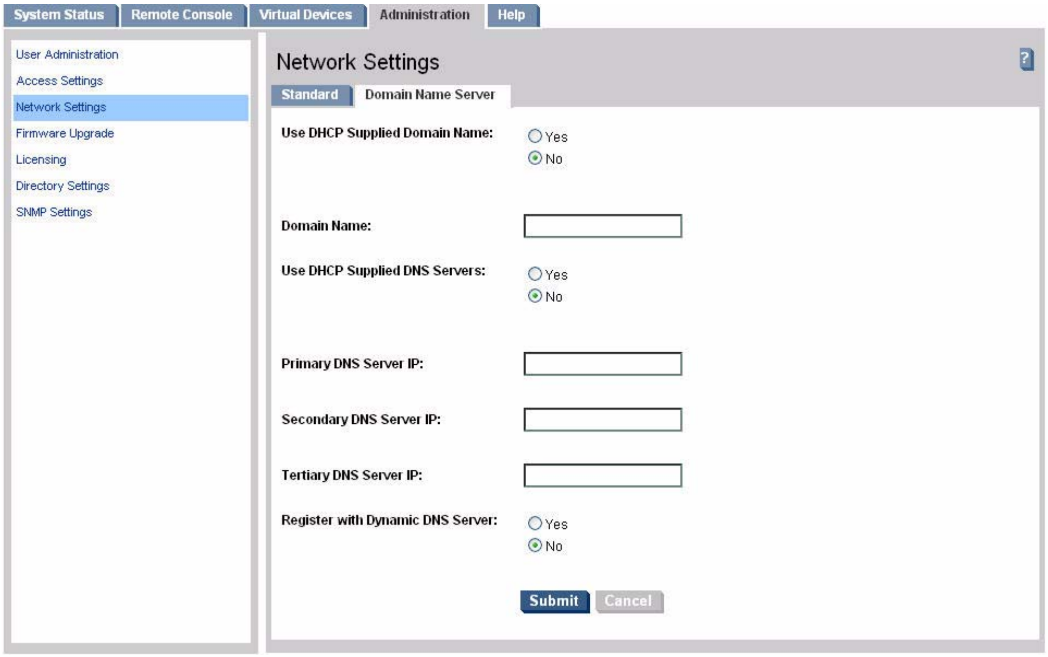
Fields and Buttons	Description
MAC Address	The 12 digit (hexadecimal) MAC address.
DHCP Status	Enable or Disable.
iLO MP Host Name	The host name set here is displayed at the iLO MP Command interface prompt.
IP Address	The iLO MP IP address. If DHCP is being used, the IP address is automatically supplied.
Subnet Mask	The subnet mask for the iLO 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 10BaseT option.
Submit	Submits the information.
Cancel	Cancels the action.

Administration > Network Settings > Domain Name Service

The **Domain Name Service** page (Figure 6-14) enables you to configure the DNS server settings, the domain name, and up to three DNS servers either manually or automatically through DHCP. Only a user with configuration access right can use this feature.

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

Figure 6-14 Administration > Network Settings > Domain Name Service Page



Use DHCP Supplied Domain Name: ○ Yes ● No

Domain Name:

Use DHCP Supplied DNS Servers: ○ Yes ● No

Primary DNS Server IP:

Secondary DNS Server IP:

Tertiary DNS Server IP:

Register with Dynamic DNS Server: ○ Yes ● No

Fields and descriptions are as follows:

Table 6-11 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.

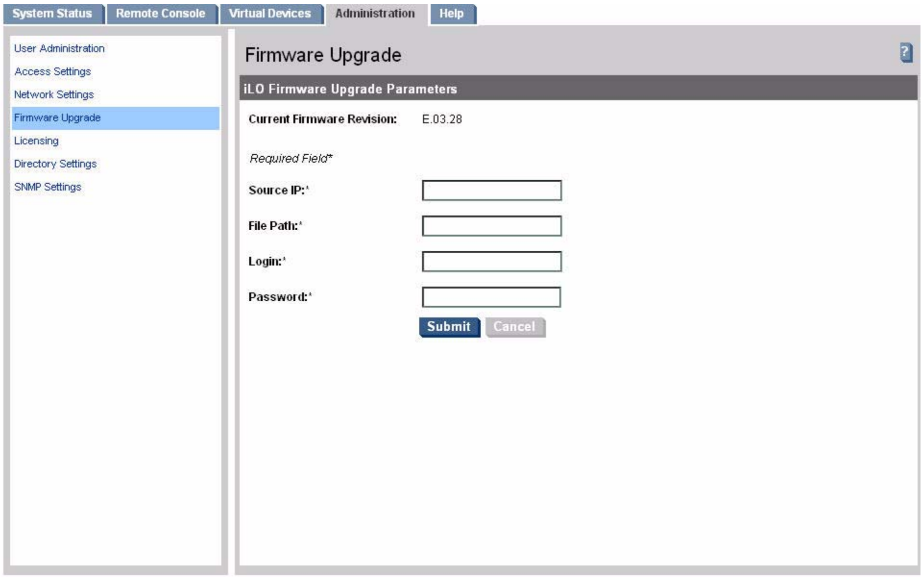
Administration > Firmware Upgrade

The **Firmware Upgrade** page (Figure 6-15) enables you to remotely upgrade the firmware from an FTP source. Only a user with configuration access right can use this feature.

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

IMPORTANT This firmware upgrade upgrades iLO MP firmware only. It does not affect server operation. You do not need to shut down the OS to perform this upgrade.

Figure 6-15 Administration > Firmware Upgrade Page



Firmware Upgrade

iLO Firmware Upgrade Parameters

Current Firmware Revision: E.03.28

*Required Field**

Source IP:*

File Path:*

Login:*

Password:*

To perform a firmware upgrade, follow these steps:

Step 1. Download the firmware from the HP Web site at: **`http://www.hp.com/go/bizsupport`** for IPF firmware and follow the directions.

Step 2. Copy the firmware image file onto your own FTP server.

Step 3. Enter the following mandatory parameters:

Table 6-12 Firmware Upgrade Parameters

Field	Action
Current Firmware Revision	**The version of iLO MP firmware displays.**
Source IP	**Enter the IP address of the FTP server where the firmware image file resides.**

Table 6-12 Firmware Upgrade Parameters (Continued)

Field	Action
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 MP reboots using the new firmware. If the upgrade fails, the iLO 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 6-16) is used to enter a license key to enable the iLO MP Advanced Pack features.

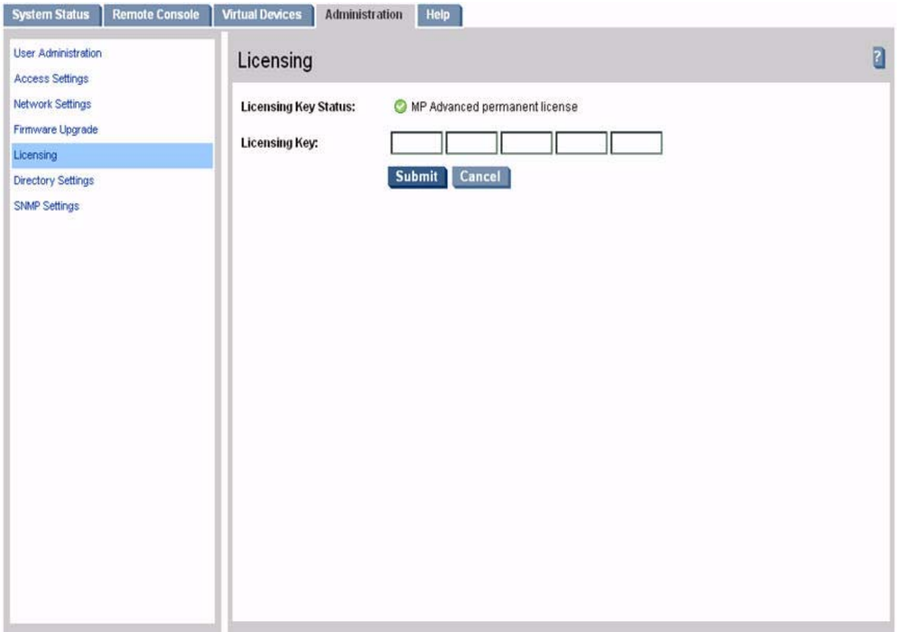
The iLO MP offers some advanced features, which can be used only with the iLO MP Advanced Pack license:

- Directory-based authentication and authorization using LDAP.
- SSH access.
- Group actions through HP Systems Insight Manager (HPSIM).
- LDAP Lite

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

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

Figure 6-16 User Administration > Licensing Page



Licensing Key Status: MP Advanced permanent license

Licensing Key:

Fields and descriptions are as follows:

Table 6-13 Licensing Page Description

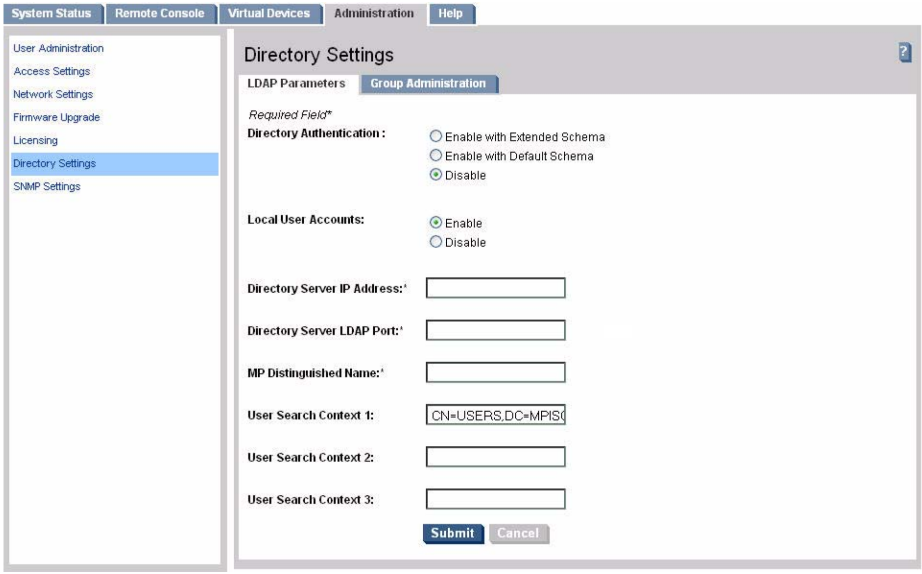
Fields and Buttons	Description
Licensing Key Status	The status of the license - inactive if no license has been installed, the type of the license (Evaluation or Permanent), and the number of days remaining if the license installed is an Evaluation license.
Licensing Key	Enter the 25-character license key used to enable the iLO MP Advanced Pack features. Fields are case sensitive.
Submit	Submits the key for activation.
Cancel	Cancels the action.

Administration > Directory Settings > LDAP Parameters

The **LDAP Parameters** page (Figure 6-17) enables you to edit LDAP parameters. Only a user with configuration access right can use this feature.

NOTE This functionality will only display if you have the iLO MP Advanced Pack license. For more information on the iLO MP Advanced Pack license, see Chapter , “Advanced Pack License,” on page 20.

Figure 6-17 Administration > Directory Settings > LDAP Parameters Page



Directory Settings

*Required Field**

Directory Authentication : ○ Enable with Extended Schema ○ Enable with Default Schema ● Disable

Local User Accounts: ● Enable ○ Disable

Directory Server IP Address:*

Directory Server LDAP Port:*

MP Distinguished Name:*

User Search Context 1: CN=USERS,DC=MPIS(

User Search Context 2:

User Search Context 3:

Fields and descriptions are as follows:

Table 6-14 LDAP Parameters Page Description

Field	Description
Directory Authentication	Choosing enable or disable, activates or deactivates directory support on the iLO 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 Ad ministration** page must be configured after this option is selected.

Table 6-14 LDAP Parameters Page Description (Continued)

Field	Description
Local User Accounts	Includes or excludes access to local iLO 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 into the iLO 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.
Distinguished Name	Distinguished Name of the iLO MP, specifies where this iLO 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 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 MP.
Submit	Submits the information.
Cancel	Cancels the action.

Administration > Directory Settings > Group Administration

The **Group Administration** page (Figure 6-18) 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. This page utilizes Lightweight Directory Access Protocol Light (LDAP Lite), which provides user authentication for access to the iLO MP without extending the schema on the LDAP server or snap-in installation on the client.

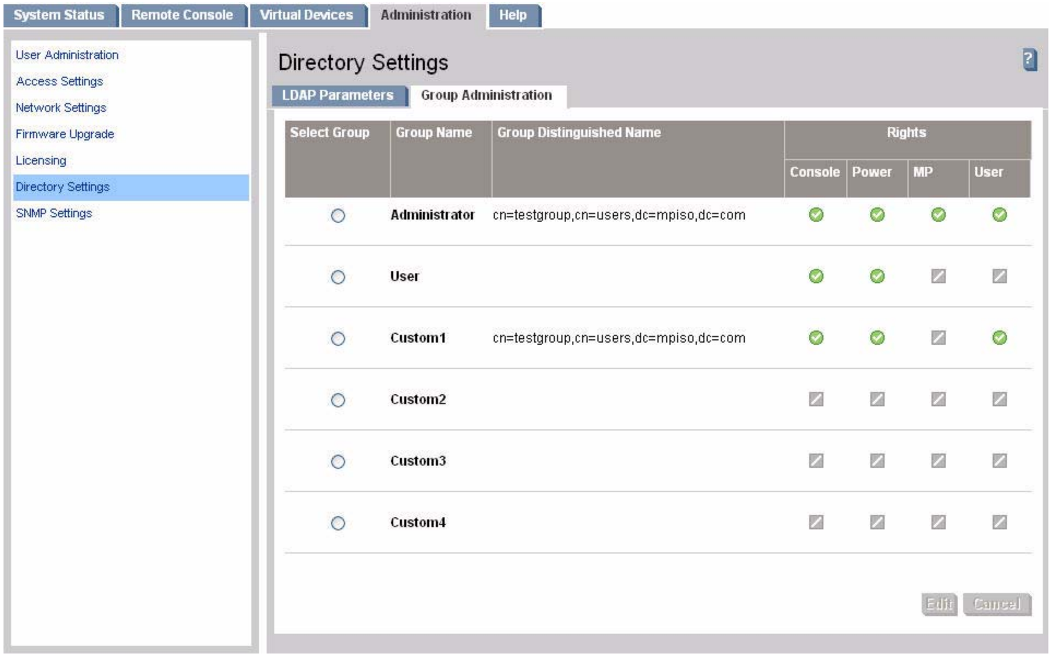
Not extending the schema on the directory server means the directory server will not know anything about the iLO MP object or iLO MP privileges, and the only thing the iLO MP queries from the directory server is to authenticate the user name and password.

NOTE This functionality will only display if you have the iLO MP Advanced Pack license. For more information on the iLO MP Advanced Pack license, see Chapter , “Advanced Pack License,” on page 20.

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

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

Figure 6-18 Administration > Directory Settings > Group Administration Page



Directory Settings

Select Group	Group Name	Group Distinguished Name	Rights			
			Console	Power	MP	User
○	Administrator	cn=testgroup,cn=users,dc=mpiso,dc=com	✓	✓	✓	✓
○	User		✓	✓	▨	▨
○	Custom1	cn=testgroup,cn=users,dc=mpiso,dc=com	✓	✓	▨	✓
○	Custom2		▨	▨	▨	▨
○	Custom3		▨	▨	▨	▨
○	Custom4		▨	▨	▨	▨

Fields and descriptions are as follows:

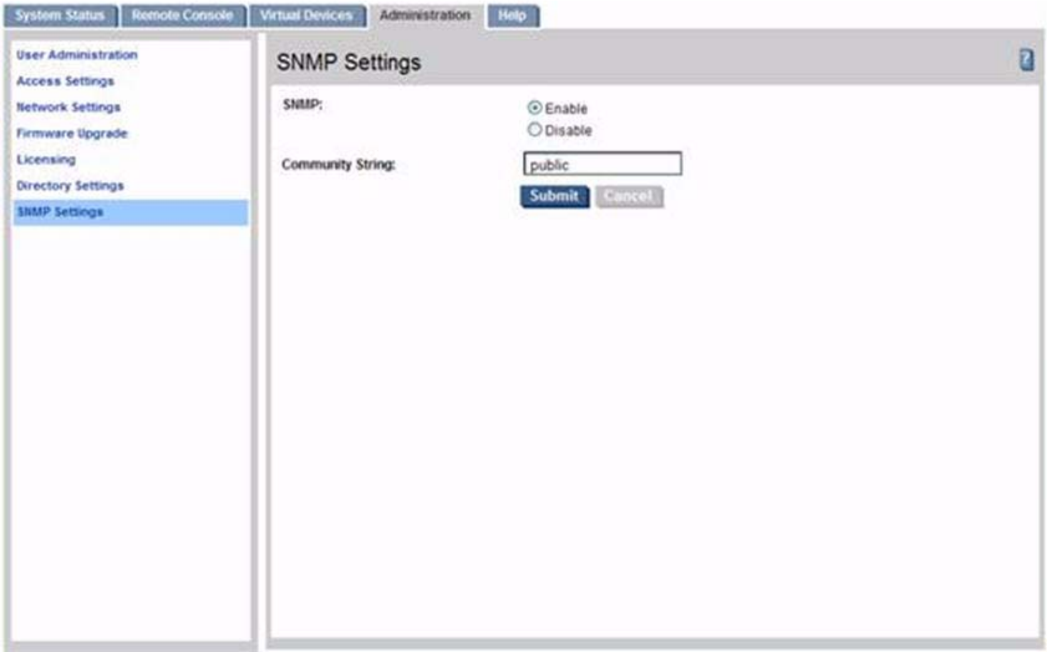
Table 6-15 Group Administration Page Description

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 > SNMP Settings

The **SNMP Settings** page (Figure 6-19) enables you to edit SNMP feature settings. Only a user with configuration access right can use this feature.

Figure 6-19 Administration > SNMP Settings Page



SNMP Settings

SNMP: ● Enable ○ Disable

Community String: public

Fields and descriptions are as follows:

Table 6-16 SNMP Settings Page Description

Field	Description
SNMP	Choosing **Enable** or **Disable**, activates or deactivates the SNMP feature support on this iLO MP.
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.
```

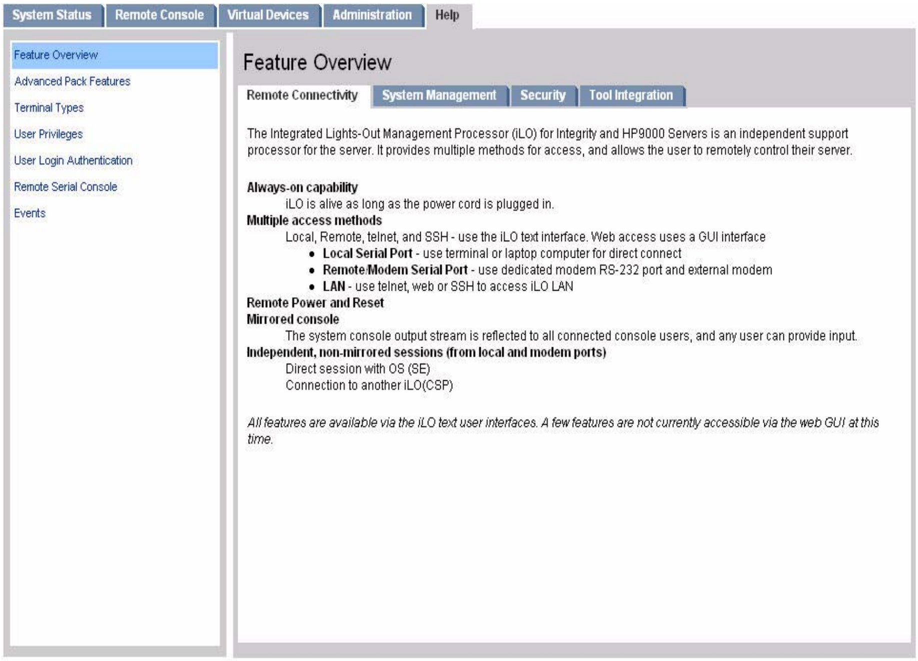
Click **OK** and reset the iLO MP.

Help

The iLO MP has a robust help system.

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

Figure 6-20 Help Page



Feature Overview

The Integrated Lights-Out Management Processor (iLO) for Integrity and HP9000 Servers is an independent support processor for the server. It provides multiple methods for access, and allows the user to remotely control their server.

Always-on capability
iLO is alive as long as the power cord is plugged in.
Multiple access methods
Local, Remote, telnet, and SSH - use the iLO text interface. Web access uses a GUI interface
- **Local Serial Port** - use terminal or laptop computer for direct connect
- **Remote/Modem Serial Port** - use dedicated modem RS-232 port and external modem
- **LAN** - use telnet, web or SSH to access iLO LAN

Remote Power and Reset
Mirrored console
The system console output stream is reflected to all connected console users, and any user can provide input.
Independent, non-mirrored sessions (from local and modem ports)
Direct session with OS (SE)
Connection to another iLO(CSP)

All features are available via the iLO text user interfaces. A few features are not currently accessible via the web GUI at this time.

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.

7 Command Menu Interface Reference

There are several options from which commands can be executed in the iLO MP:

MP Main Menu — The **MP Main Menu** command line interface (CLI) supports the basic MP commands for server control and the iLO MP configuration, such as setting up the iLO MP LAN, retrieving events, resetting and powering on control of the server, switching to the console, and so on.

Command Menu — The **Command** menu switches the console terminal from the **MP Main Menu** to mirrored command interface mode.

This chapter addresses the following topics:

- "MP Main Menu Commands" on page 86
- "Command Menu Commands" on page 88

MP Main Menu Commands

The **MP Main Menu** commands are listed in Table 7-1 and described below.

Table 7-1 MP Main Menu Commands and Descriptions

Command	Description
`CO`	Select console mode
`VFP`	Display virtual front panel
`CM`	Enter command mode
`CL`	View console log
`SL`	Show event logs
`HE`	Display help for menu or command
`X`	Exit

NOTE The list of commands displayed on the screen can be different depending on the method of access to the iLO MP.

MP Main Menu Command Summary

`CO`: Console—leave command mode and enter console mode

This command switches the console terminal from the **MP Main Menu** to mirrored/redirected console mode. All mirrored data is displayed. Type either **Ctrl-B**, or **Esc** and **(** to return to the iLO MP command interface.

`VFP`: Display virtual front panel

This command presents a summary of the system by using direct console addressing. If the terminal is not recognized by the iLO MP, VFP mode is rejected. Each individual user gets this summary in order to avoid issues related to terminal type and screen display mode.

`CM`: Command Mode—enter command mode

This command switches the console terminal from the **MP Main Menu** to mirrored command interface mode. If a command is in progress, a message is displayed warning the new user of system status.

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

This command displays up to 60 KB of console data (about 60 pages of display in text mode) sent from the SPU 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: Display contents of the system status logs

This command displays the contents of the event logs that have been stored in nonvolatile memory.

- System event log (SEL)—Events (filtered by alert level) and errors.
- Forward progress—All events.
- Current 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 indicator of the system LED (flashing amber light). 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.

Navigate within the logs as follows:

- + — 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).
- ? — Display this help menu.
- Ctrl-B — Exit command, and return to the **MP Main Menu**.

Table 7-2 defines alert (or severity) levels.

Table 7-2 Alert Levels

Severity	Definition
0	Minor forward progress
1	Major forward progress
2	Informational
3	Warning

Table 7-2 Alert Levels (Continued)

Severity	Definition
5	Critical
7	Fatal

HE: Display help for menu or command

This command displays the iLO 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 MP, and those commands available in the **MP Main Menu**. If executed in command mode, this command displays a list of command interface commands available to the user. It also displays detailed help information in response to a topic or command at the help prompt.

X: Exit iLO 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 MP session.

Command Menu Commands

The **Command Menu** commands are listed in Table 7-3 and described below.

Table 7-3 Command Menu Commands and Descriptions

Command	Description
BP	Reset BMC passwords
CA	Configure async or serial ports
DATE	Display the current date
DC	Default configuration
DF	Display field replaceable unit (FRU) information
DI	Disconnect remote or LAN console
DNS	Set DNS configuration
FW	Upgrade iLO MP firmware
HE	Display help for menu or command
ID	Display or modify system information
IT	Modify iLO MP inactivity timeouts
LC	LAN configuration
LDAP	LDAP configuration

Table 7-3 Command Menu Commands and Descriptions (Continued)

Command	Description
`LM`	License management
`LOC`	Display and configure locator LED
`LS`	LAN status
`MR`	Modem reset
`MS`	Modem status
`PC`	Remote power control
`PG`	Paging parameter setup
`PR`	Configure power restore policy
`PS`	Power management module status
`RB`	Reset BMC
`RS`	Reset 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
`VDP`	Display virtual diagnostic panel LEDs
`WHO`	Display connected iLO MP users
`XD`	Diagnostics or reset of the iLO MP

Command Menu Command Summary

BP: Reset BMC passwords

This command resets baseboard management controller (BMC) (EFI Shell) passwords.

CA: Configure asynchronous local and remote serial port parameters

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.

Set up the remote serial port parameters as follows:

- MODEM PROTOCOL: Bell or CCITT. (CCITT is a European standard; RTS/CTS signaling is used, as well as the Ring signal. Bell is a U.S. or simple mode.)
- BAUD RATES: Input and output data rates are the same — 4800, 9600, 19200, 38400 bit/sec.
- FLOW CONTROL: Hardware uses RTS/CTS; software uses Xon/Xoff.
- TRANSMIT CONFIGURATION STRINGS: Disable this setting whenever the modem being used is not compatible with the supported modem (MT5634ZBA).
- MODEM PRESENCE: When the modem might not always be connected, set this parameter to “not always connected.”

  Example: A modem attached through a switch. In mode “not always connected,” no dial-out functions are allowed: DIAL-BACK is disabled, and PAGING is not possible.

The iLO MP mirrors the system console to the iLO MP local, remote/modem, 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 might see unexpected results.

DATE: Display the current date

This command displays the current date, as best known to the iLO MP. The usual source for the date is from the BMC, but if the BMC date is not available, the iLO MP real-time clock is used. The real-time clock is only used when the iLO MP is first powered on or rebooted, until it can obtain the correct date from the BMC.

DC: Default configuration—reset all iLO MP parameters to the default configuration

This command sets all iLO MP all parameters back to their default values. The following parameters are reset:

```
To restore specific configurations to their defaults use the following commands:
Remote Console Serial Port Modem configuration: CA -all DEFAULT
MP IP configuration                           : LC -all DEFAULT
Remote Access Configuration                   : SA -all DEFAULT
Command Interface configuration               : IT -all DEFAULT
MP Security configuration                     : SO -all DEFAULT
MP Session configuration                      : IT -all DEFAULT
MP User configuration                         : UC -all DEFAULT
SNAP Configuration                            : SNMP -all DEFAULT
```

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

- In the UC command, change individual users or reset all users to default values.
- Reset passwords by pressing the **MP reset** button on the back panel of your HP server. After the iLO 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.

DF: Display FRUID information

This command displays FRUID information from the BMC for FRU devices. Information provided includes serial number, part number, model designation, name and version number, and manufacturer.

`DI`: Disconnect remote/Modem or LAN/Remote Serial Console

This command disconnects (hangs up) remote/modem, telnet, Web SSL, or SSH users from the iLO MP. It does not disable the ports. The remote console is no longer mirrored.

`DNS`: Set DNS configuration

This command enables you to configure the DNS server settings, whether DHCP is enabled or disabled.

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.

`FW`: Activates firmware upgrade mode

This command performs two functions:

- Upgrades iLO MP firmware. This firmware upgrade will not affect server operation if it is for iLO 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.

NOTE This functionality is not available on all systems. On current entry-class systems only the MP iLO firmware update is available through the iLO MP

This command is only available from the iLO MP LAN port and the local serial port.

To perform a firmware upgrade, follow these steps:

Step 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.

Step 2. Copy the firmware image file onto your own FTP server.

Step 3. Establish a telnet or SSH session with the iLO MP.

Step 4. Logon to the iLO MP using the **Admin** password.

Step 5. At the **MP Main Menu** prompt, type **`CM`** to enter the **Command Menu**.

Step 6. Type **`FW`** to enter firmware upgrade mode.

Step 7. At the **Source IP** prompt, enter the IP address of the FTP server where the firmware image file resides and press **Enter**.

Step 8. At the **File Path** prompt, enter the directory and path where the firmware is located. (example, /firmware/rx4640/example/)

Example command line usage:

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

Step 9. At the **Enter Login** prompt, enter your username on the FTP server.

Step 10. At the **Enter Password** prompt, enter your password on the FTP server.

Step 11. When you are prompted to confirm, enter **`Y`** to confirm. The firmware will be upgraded and the iLO MP automatically resets.

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

Step 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 MP firmware displays at the top of the main help menu.

CAUTION If the upgrade process is interrupted at any time, the core I/O may need to be repaired or replaced.

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

```
New Firmware Upgrade Parameters
   * I - Source IP : 192.0.2.1
   * 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
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 - Web and telnet connections will
      be dropped. MP will now reset . . . .
```

`HE`: Display help for menu or command

This command displays the iLO MP hardware and firmware version identity, and the date and time of firmware generation. If executed from the **MP Main Menu**, this command displays general information about the iLO MP, and those commands available in the **MP Main Menu**. If executed in command mode, this command displays a list of command interface commands available to the user. It also displays detailed help information in response to a topic or command at the help prompt.

`ID`: Display or modify system information

This command enables the user to display and modify the following:

- SNMP contact information
- SNMP server information
- SPU host name

NOTE The SPU host name information is not retained across iLO MP reboots.

IT: Modify iLO MP inactivity timers

The session inactivity timeout prevents sessions on the system from being inadvertently left open. You can start a session by dialing into the modem port if it is configured for O/S SESSION. An open session can prevent users from logging in to the iLO MP through the port and can also prevent system applications from initiating an outbound connection. The inactivity timeout also prevents a session from being locked indefinitely if the system session is hung or if the system OS is hung. You cannot deactivate the session inactivity timeout.

When a user initiates an iLO 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.

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:

- Session inactivity timeout: 1 to 1440 minutes (default is 60 minutes).
- iLO MP inactivity timeout: 1 to 30 minutes (default is 3 minutes).
- Flow control timeout: 0 to 60 minutes. If the flow control timeout is set to 0, no timeout is applied. A mirroring flow control condition ceases when no flow control condition exists on any port.

LC: LAN configuration (IP address, and so on)

This command displays and enables modification of the LAN configuration. Configurable parameters include:

- iLO 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 MP host name:
  - The iLO MP host name set in this command is displayed at the iLO MP Command mode prompt. Its primary purpose is to identify the iLO MP LAN interface in a DNS database.
  - If you change the iLO 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 hostname* are sent to the DDNS server.
- Subnet mask.
- Gateway IP address.
- Remote Serial Console Port.
- Link state.
- SSH access port number.

LDAP: LDAP configuration

LDAP directory settings is an iLO MP Advanced Pack license feature that enables centralized user account administration using directory services.

This command displays and enables modification of the following LDAP directory settings:

- Directory Authentication: Choosing enable or disable, activates or deactivates directory support on the iLO 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 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 Ad ministration** 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.
- Local User Accounts: Includes or excludes access to local iLO MP user accounts. If local user accounts are enabled, you may log into the iLO 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.
- Distinguished Name: Distinguished Name of the iLO MP, specifies where this iLO 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 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 MP.

LDAP: LDAP group administration

The **Group Administration** page 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 MP, the iLO MP reads that user’s directory name in the directory to determine the groups the user is a member of. The iLO 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 into the iLO MP without having to do any schema extension on the directory server or snap-in installation on the client. See “Configuring LDAP Lite Default Schema” on page 51 for information on configuring LDAP Lite.

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

This command displays the current license status. Use it to enter a license key to enable the following features:

- Directory-based authentication and authorization.
- SSH (secure shell).
- Group actions through Systems Insight Manager.

LOC: Locator LED status

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

LS: LAN status

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

MR: Modem reset

This command makes the iLO MP send an `at z` command to the modem, which resets it. Any modem connections are lost. You can view the initialization results by using the `MS` command.

MS: Modem status—display modem status

This command displays the state of the modem lines connected to the remote or modem serial port. Update the display by pressing **Enter**. The `MS` command displays the current state of the status signals DCD, CTS, DSR, RI, and the last state of the control signals DTR, and RTS set by the firmware.

PC: Power control—turn system power on and off

This command enables you to switch the system power on or off. A power cycle option is available that provides a 30-second delay between system power on and power off.

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

IMPORTANT This 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.

PG: Paging parameter setup

This command enables you to configure the pagers and set triggering events.

A string description of the triggering event is sent with the page.

PR: Power restore policy configuration

Use this command to configure the power restore policy. The power restore policy determines how the system or chassis 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 ac was removed or lost.

PS: Power status

This command displays the system power state and temperature and the status of the power supplies and fans.

RB: Reset BMC

This command resets the BMC.

RS: Reset system through RST signal

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

This command causes the system (except iLO 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.

SA: Set access options

This command configures access for LAN telnet, SSH, IPMI over LAN, remote/modem ports, and Web SSL.

If remote/modem, 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.

SNMP: Configure SNMP parameters

This command enables you to update, enable or disable the SNMP feature. In addition, you can configure the community string, thereby securing the access to the MIB object.

To enable or disable SNMP, follow these steps:

Step 1. At the `MP:CM>` prompt, enter **SNMP**.

Step 2. Enter **N** to change the SNMP status. Enabled is the default.

Step 3. Enter **E** to enable or **D** to disable SNMP status. The screen displays the new SNMP configuration settings.

SO: Configure security options and access control

This command monitors and changes systemwide security parameters.

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.
- Number of Password Faults allowed: one to 10. This parameter defines the number of times a console can attempt to login before being rejected and having its connection closed.
- Web based to use SSL: Enabled/Disabled.
- Firmware upgrade: enables firmware upgrade from the EFI console of the server.

- iLO MP reset: enables an iLO MP reset through IPMI (from BMC, system, or IPMI over LAN).
- iLO MP password reset: enables iLO MP password reset through IPMI (from BMC, system, or IPMI over LAN).

SS: Displays the status of the system processors

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

SYSREV: Display all firmware revisions

This command displays current revisions of firmware in the system.

The following is an example of the `SYSREV` command output:

```
MP:CM> SYSREV

Current firmware revisions
MP  FW    : E.03.13
BMC FW    : 01.20
EFI FW    : 01.22
System FW : 01.40
```

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

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

This command causes 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.

TE: Tell—send a message to other terminals

You can type a message of up to 255 characters. The message is broadcast to the other mirrored clients.

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

UC: User Configuration—controls user access

This command is used to enable an administrator 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
- Modem Dial-back
- Modem Dial-back Phone

All users have the right to log in to the iLO 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 MP or the system.

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

An iLO 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 MP Configuration Access: Right to configure all iLO 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`, `MR`, `PG`, `RB`, `SA`, `SO`, `XD`

`VDP`: Display virtual diagnostics panel LEDs

This command monitors the LEDs on the diagnostics panel.

NOTE This command is restricted to rx4640 and rp4440 systems.

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

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

For LAN and Remote Serial Console clients, the command displays the remote 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.

`XD`: Diagnostics or reset of the iLO MP

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

- iLO MP Parameter Checksum
- Verify I2C connection (get BMC Device ID)
- LAN connectivity test using the `ping` command
- Modem selftest

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

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

8 Directory Services Installation and Configuration

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

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

This chapter addresses the following topics:

- "Directory Services" on page 100
- "Directory Services for Active Directory" on page 106
- "Directory Services for eDirectory" on page 119
- "User Login Using Directory Services" on page 131
- "Certificate Services" on page 132
- "Directory-Enabled Management" on page 133
- "Directory Services Schema (LDAP)" on page 139

Directory Services

The following are benefits of directory integration:

- Scalability: The directory can be leveraged to support thousands of users on thousands of iLOs.
- 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 iLO 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 iLO MP users.
- Immediacy: A single change in the directory rolls out immediately to associated iLO 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 MP.
- Flexibility: You can create a single role for a single user on a single iLO MP, you can create a single role for multiple users on multiple iLOs, or you can use a combination of roles — whatever is suitable for your enterprise.
- Compatibility: iLO MP directory integration applies to iLO MP products. The integration supports the popular directories Active Directory and eDirectory.
- Standards: iLO MP directory support builds on the LDAP 2.0 standard for secure directory access.

Features Supported by Directory Integration

iLO 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 MP and iLO MP users.

Installing Directory Services for the iLO 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 Integrated Lights-Out Advanced Pack license.
- Configure LDAP.

Installing Directory Services

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

Step 1. Plan

Review the following sections:

- "Directory Services" on page 100.
- "Directory Services Schema (LDAP)" on page 139.
- "Directory-Enabled Management" on page 133.

Step 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" on page 103) once to extend the schema.

c. Run the management snap-in installer ("Management Snap-In Installer" on page 105) and install the appropriate snap-in for your directory service on one or more management workstations.

Step 3. Update

a. Flash the ROM (upgrade iLO MP firmware) on the iLO MP with the directory-enabled firmware.

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

Step 4. Manage

a. Create a management device object and a role object ("Directory Services Objects" on page 112) 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" on page 133. Examples are available in "Directory Services for Active Directory" on page 106 and "Directory Services for eDirectory" on page 119.

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)" on page 139.

Directory Services Support

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

- Windows 2000 family
- Windows Server 2003 family

The iLO 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 MP uses LDAP over SSL to communicate with the directory servers. The iLO 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 (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 MP requires extending the eDirectory schema. An administrator must complete extending the schema.

Schema Required Software

The iLO MP requires specific software, which extends the schema and provides snap-ins to manage the iLO MP 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.

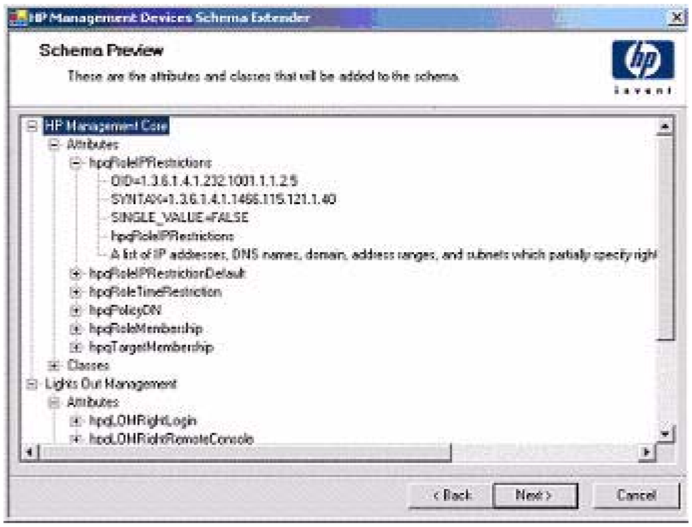
The installer includes three important screens:

- Schema Preview
- Setup
- Results

Schema Preview

The **Schema Preview** screen (Figure 8-1) 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 8-1 Schema Preview Screen



HP Management Devices Schema Extender

Schema Preview

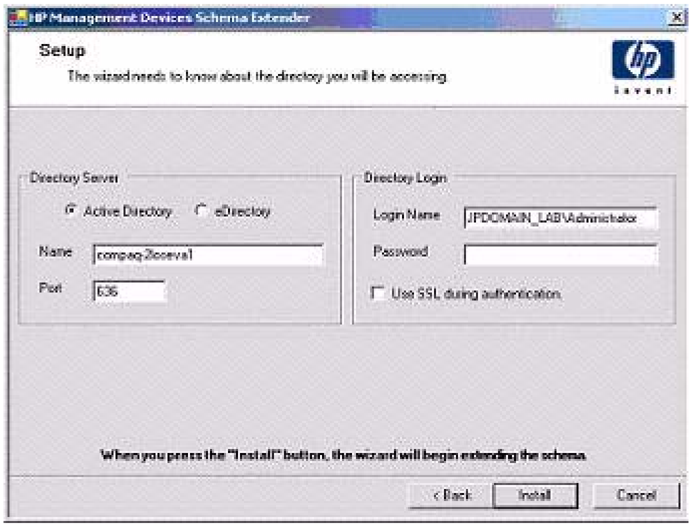
These are the attributes and classes that will be added to the schema.

```
HP Management Core
  Attributes
    hpqRoleIPRestrictions
      OID=1.3.6.1.4.1.232.1001.1.1.2.5
      SYNTAX=1.3.6.1.4.1.1466.115.121.1.40
      SINGLE_VALUE=FALSE
      hpqRoleIPRestrictions
      A list of IP addresses, DNS names, domain, address ranges, and subnets which partially specify righ
    hpqRoleIPRestrictionDefault
    hpqRoleTimeRestriction
    hpqPolicyDN
    hpqRoleMembership
    hpqTargetMembership
  Classes
Lights Out Management
  Attributes
    hpqLOMRightLogin
    hpqLOMRightRemoteConsole
```

Setup

Use the **Setup** screen (Figure 8-2) to enter the appropriate information before extending the schema.

Figure 8-2 Schema Setup Screen



Setup

The wizard needs to know about the directory you will be accessing

Directory Server

● Active Directory ○ eDirectory

Name: compaq-2kceval1

Port: 636

Directory Login

Login Name: JPDOMAIN_LAB\Administrator

Password:

□ Use SSL during authentication

When you press the "Install" button, the wizard will begin extending the schema.

The Directory Server section of the **Setup** screen enables you to select whether to use Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

IMPORTANT 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.

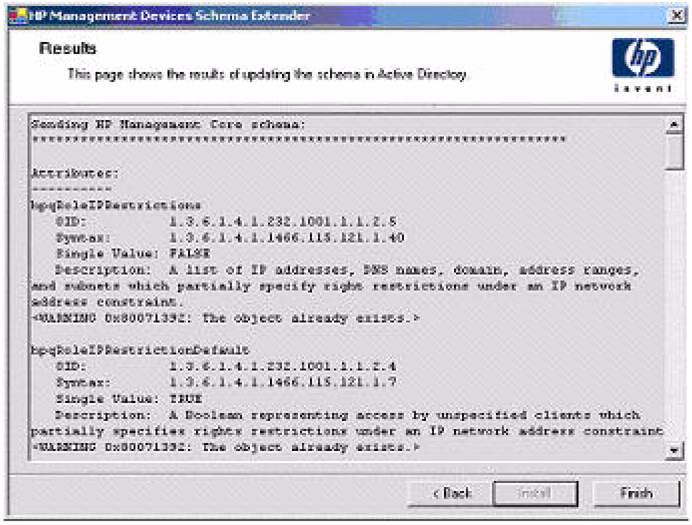
To get write access to the schema on Windows 2000 requires a change to the registry safety interlock. If you select the Active Directory option, the schema extender attempts to make the registry change. It will only succeed if you have rights to do this. Write access to the schema is automatically enabled 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 8-3) displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Figure 8-3 Schema Results Screen



HP Management Devices Schema Extender

Results

This page shows the results of updating the schema in Active Directory.

```
Sending HP Management Core schema:
******************************************************************

Attributes:
----------
hpqRoleIPRestrictions
   OID:          1.3.6.1.4.1.232.1001.1.1.2.5
   Syntax:       1.3.6.1.4.1.1466.115.121.1.40
   Single Value: FALSE
   Description:  A list of IP addresses, DNS names, domain, address ranges,
and subnets which partially specify right restrictions under an IP network
address constraint.
<WARNING 0x80071392: The object already exists.>

hpqRoleIPRestrictionDefault
   OID:          1.3.6.1.4.1.232.1001.1.1.2.4
   Syntax:       1.3.6.1.4.1.1466.115.121.1.7
   Single Value: TRUE
   Description:  A Boolean representing access by unspecified clients which
partially specifies rights restrictions under an IP network address constraint
<WARNING 0x80071392: The object already exists.>
```

Management Snap-In Installer

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

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

- Create and manage iLO MP and role objects.
- Make the associations between iLO 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 Management Processors 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 MP to connect securely over the network.
- The active directory must have the schema extended to describe iLO MP object classes and properties.
- The iLO MP firmware must be Version E.03.01 or later.
- iLO MP Advanced Pack features must be licensed.

Directory Services for the iLO 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 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 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 iLOs, follow these steps:

Step 1. Install Active Directory. For more information, see Installing Active Directory in the Microsoft Windows 2000 Server Resource Kit.

Step 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.

Step 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.

Step 4. Create a certificate or install certificate services. This step is necessary to create a certificate or install certificate services because the iLO MP communicates with active directory using SSL. Install active directory before installing certificate services.

Step 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.

Step 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`**.

Step 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:

Step 1. Run the snap-in installation application to install the snap-ins.

Step 2. Configure the directory service to have the appropriate objects and relationships for iLO MP management:

a. Use the management snap-ins from HP to create iLO MP, Policy, Admin, and User Role objects.

b. Use the management snap-ins from HP to build associations between the iLO MP object, the policy object, and the role object.

c. Point the iLO MP object to the Admin and User role objects (Admin and User roles automatically point back to the iLO MP object).

For more information on iLO MP objects, see “Directory Services Objects” on page 112.

At a minimum, create:

- One Role object that contains one or more users and one or more iLO MP objects.
- One iLO MP object corresponding to each iLO MP that is using the directory.

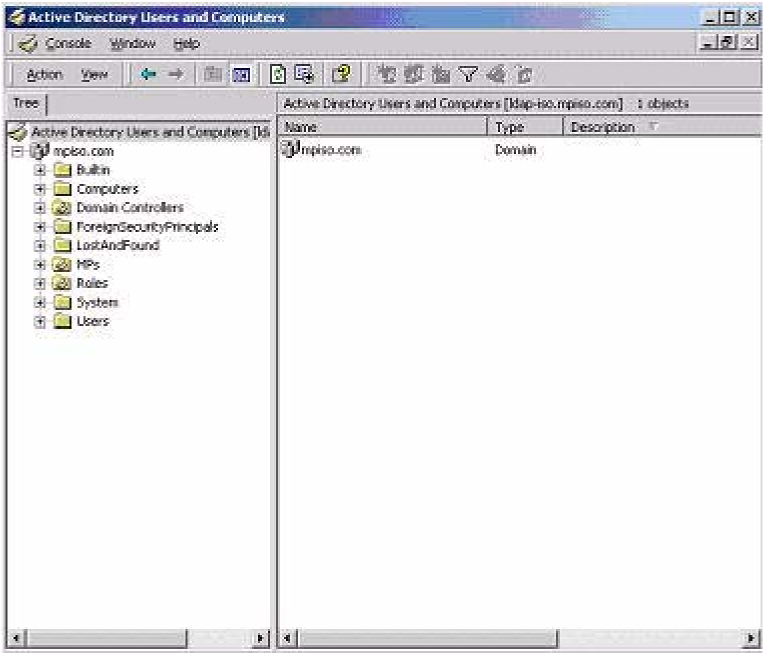
Example: Creating and Configuring Directory Objects for Use with iLO MP in Active Directory

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 8-4.

Figure 8-4 Directory Example



Active Directory Users and Computers [ldap-iso.mpiso.com] 1 objects

Name	Type	Description
mpiso.com	Domain	

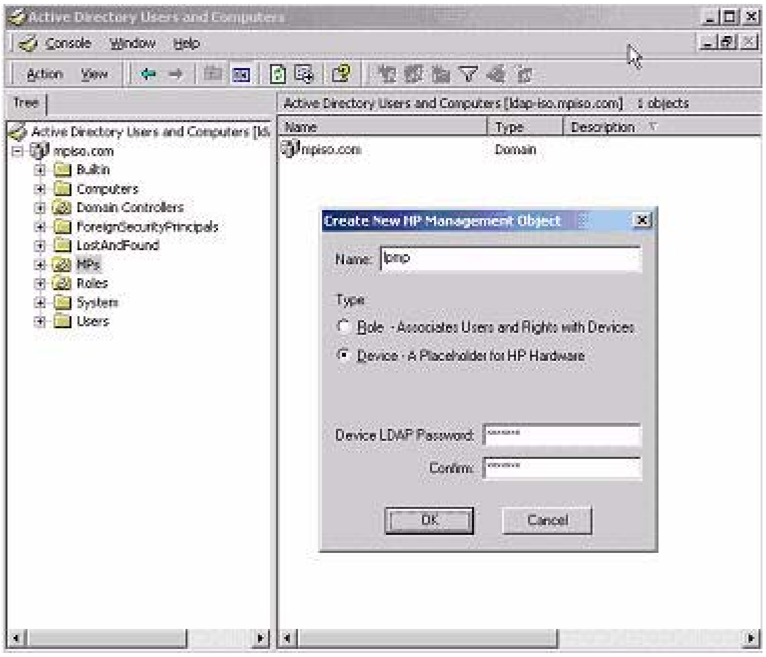
Step 1. Create an organizational unit to contain the iLO MP devices managed by the domain. In this example, two organizational units are created, called Roles and MPs.

Step 2. Use the HP provided Active Directory Users and Computers snap-ins to create iLO MP objects in the MPs organizational unit for several iLO MP 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 8-5).

Figure 8-5 Create New HP Management Object Dialog Box


Active Directory Users and Computers
Console Window Help
Action View
Tree
Active Directory Users and Computers [ld
mpiso.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
MPs
Roles
System
Users
Active Directory Users and Computers [ldap-iso.mpiso.com] 1 objects
Name
Type
Description
mpiso.com
Domain
OK
Cancel

Create New HP Management Object

Name: lpmp

Type

○ Role - Associates Users and Rights with Devices

● Device - A Placeholder for HP Hardware

Device LDAP Password: ******

Confirm: ******

c. Enter an appropriate name in the **Name** field of the dialog box. In this example, the DNS host name of the iLO MP device, lpmp, is used as the name of the iLO MP object, and the surname is iLO MP.

d. Enter and confirm a password in the **Device LDAP Password** and **Confirm** fields (this is optional).

e. Click **OK**.

Step 3. Use the HP provided Active Directory Users and Computers snap-ins to create HP Role objects in the Roles organizational unit.

Step 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**.

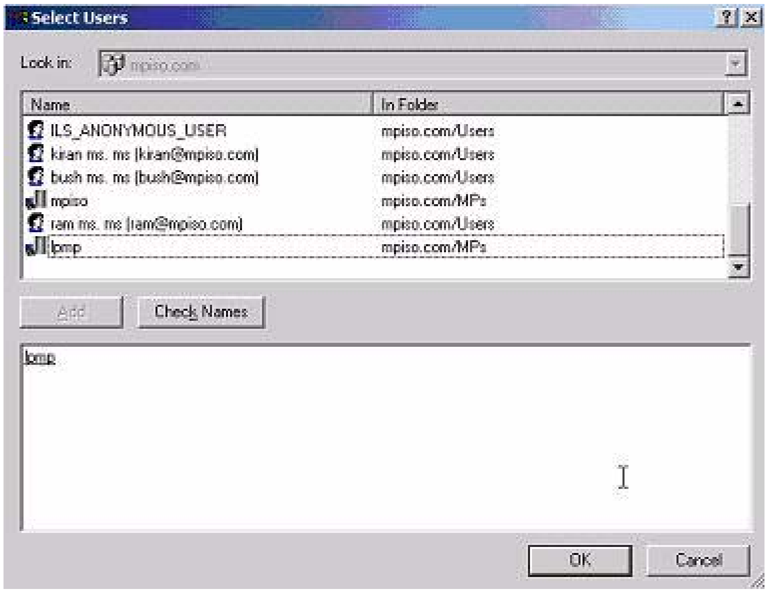
Step 5. Use the HP provided Active Directory Users and Computers snap-ins to assign the roles rights, and associate the roles with users and devices.

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 8-6), select the iLO MP object created in step 2: **lpmp** in folder mpiso.com/MPs. Click **OK** to close the dialog.

Figure 8-6 Select Users Dialog Box



Look in: mpiso.com

Name	In Folder
ILS_ANONYMOUS_USER	mpiso.com/Users
kiran ms. ms (kiran@mpiso.com)	mpiso.com/Users
bush ms. ms (bush@mpiso.com)	mpiso.com/Users
mpiso	mpiso.com/MPs
ram ms. ms (ram@mpiso.com)	mpiso.com/Users
lpmp	mpiso.com/MPs

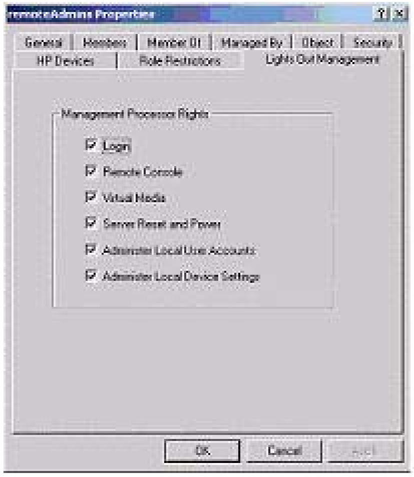
lpmp

d. 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.

Step 6. Use the **Lights Out Management** tab (Figure 8-7) 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 MP devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the iLO MP functionality. Click the checkboxes next to each right and click **Apply**.

Figure 8-7 Lights-Out Management Tab



Management Processor Rights

☑ Login
☑ Remote Console
☑ Virtual Media
☑ Server Reset and Power
☑ Administer Local User Accounts
☑ Administer Local Device Settings

Step 7. Click **OK** to close the property sheet.

Step 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.

Step 9. On the **Lights Out Management** tab, click the **Login** checkbox.

Step 10. Click **Apply** and **OK**. Members of the **remoteMonitors** role are able to authenticate and view the server status.

User rights to any iLO MP are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and the iLO MP 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 the iLO MP and associate it with an iLO MP object used in this example, use settings similar to the following on the iLO MP directory settings test 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 MP. He would enter `mpiso\moorem`, or `moorem@mpiso.com`, or `Mel Moore`, in the **Login Name** field of the iLO MP 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 the iLO MP requires three basic objects in the directory service:

- iLO MP 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 MP objects and iLO MP roles in the directory. Using the **Users and Computers** tool, you can:

- Create iLO MP and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

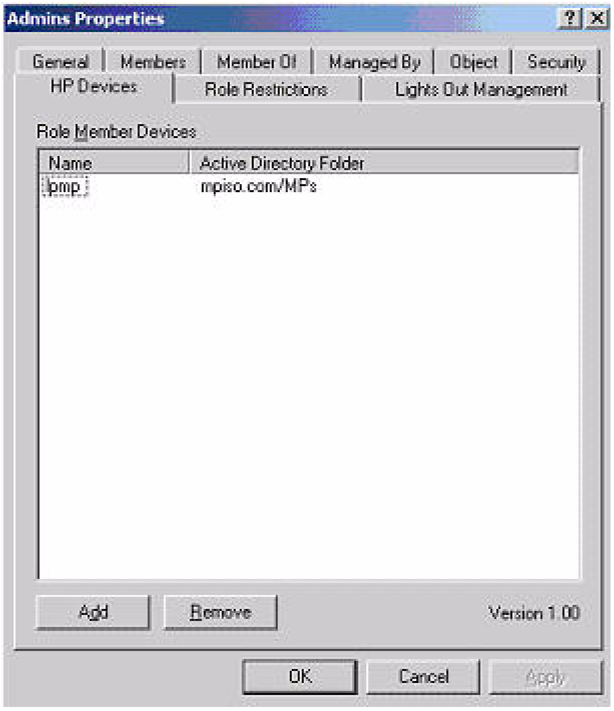
Active Directory Snap-Ins

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 8-8) to add the HP devices to be managed within a role.

Figure 8-8 HP Devices Tab



Role Member Devices

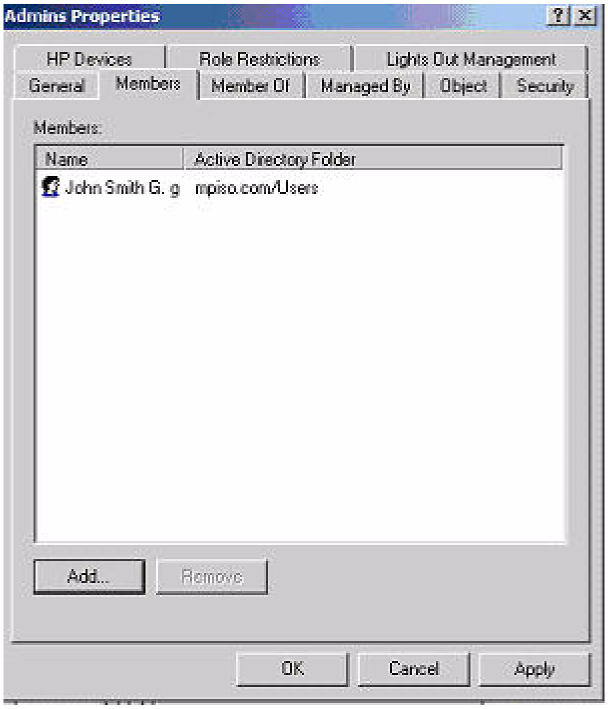
Name	Active Directory Folder
pmp	mpiso.com/MPs

- To browse to a specific HP device and add it to the list of member devices, click **Add**.
- To browse to a specific HP device and remove it from the list of member devices, click **Remove**.

Managing Users Within a Role

After user objects are created, use the **Members** tab (Figure 8-9) to manage the users within the role.

Figure 8-9 Members Tab



Members:

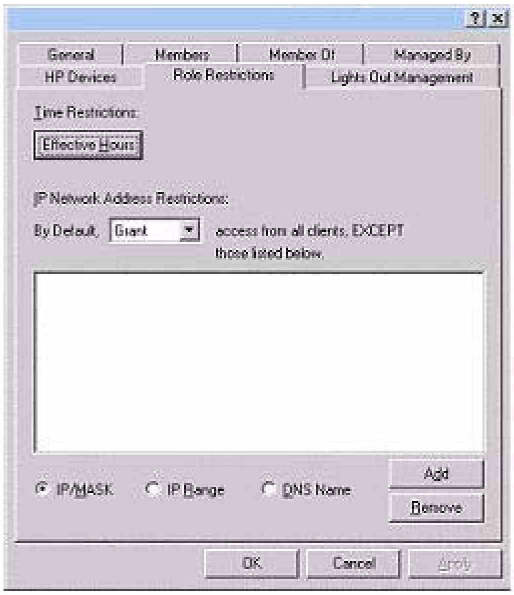
Name	Active Directory Folder
John Smith G. g	mpiso.com/Users

- 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 **Remove**.

Setting Login Restrictions

The **Role Restrictions** subtab (Figure 8-10) enables you to set login restrictions for the role. These restrictions include:

Figure 8-10 Role Restrictions Subtab



Time Restrictions:

IP Network Address Restrictions:

By Default, Grant access from all clients, EXCEPT those listed below.

● IP/MASK ○ IP Range ○ DNS Name

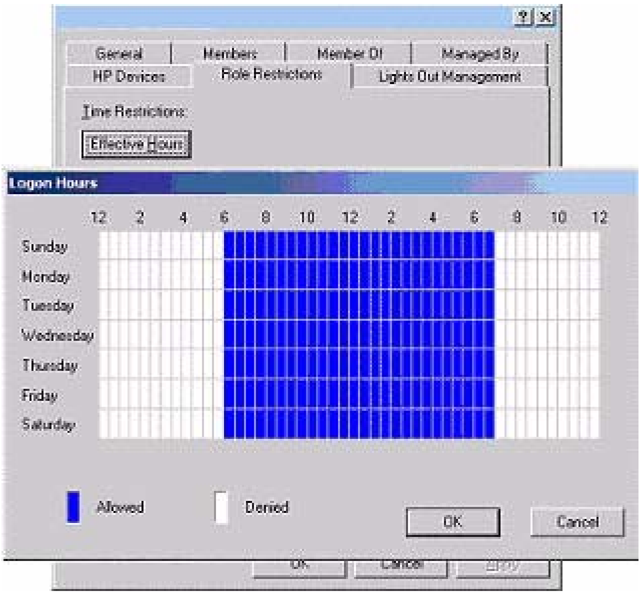
- Time Restrictions
- IP Network Address Restrictions
  - — IP/Mask
  - — IP Range
  - — DNS Name

Setting Time Restrictions

You can set the following time restrictions from the **Role Restrictions** tab.

- 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 8-11). 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 8-11 Logon Hours Pop-Up Window



- Use the default setting to allow access at all times.

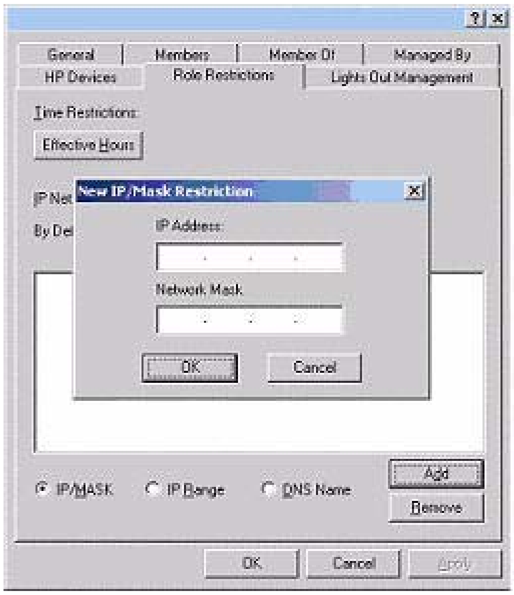
Defining Client IP Address or DNS Name Access

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

In the **By Default** dropdown menu, select whether to grant or deny access from all addresses except the specified IP addresses, IP address ranges, and DNS names.

Step 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 8-12).

Figure 8-12 New IP/Mask Pop-Up Window



Step 2. In the **New IP/Mask Restriction** pop-up window, enter the information and click **OK**.

Step 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.

Step 4. Enter the information and click **OK**.

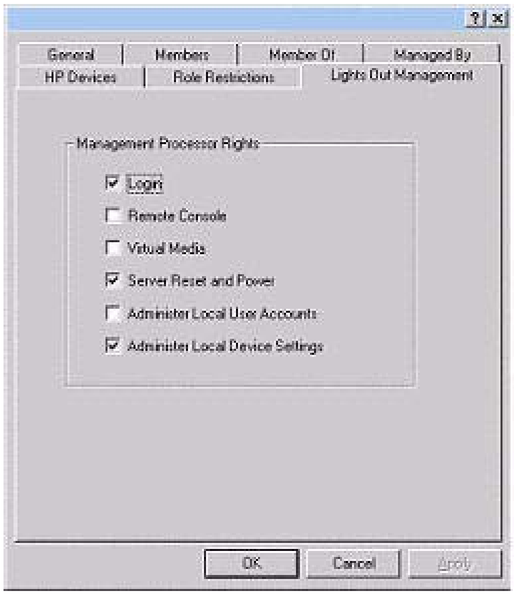
Step 5. Click **OK** to save the changes.

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 8-13) to manage rights.

Figure 8-13 Lights Out Management Tab



Management Processor Rights

☑ Login
☐ Remote Console
☐ Virtual Media
☑ Server Reset and Power
☐ Administer Local User Accounts
☑ Administer Local Device Settings

Table 8-1 lists the available rights.

Table 8-1 Group Role Rights

Right	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 MP or the system.
Remote Console	This option enables you to access the system console (the host OS)
Virtual Media	This option is currently not supported.
Server Reset and Power	This option enables you to execute iLO 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 MP user accounts.
Administer Local Device Settings	This option enables you to configure all iLO MP settings, as well as reboot iLO MP and update iLO MP firmware.

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” on page 108 for more information on using the snap-in installation application.

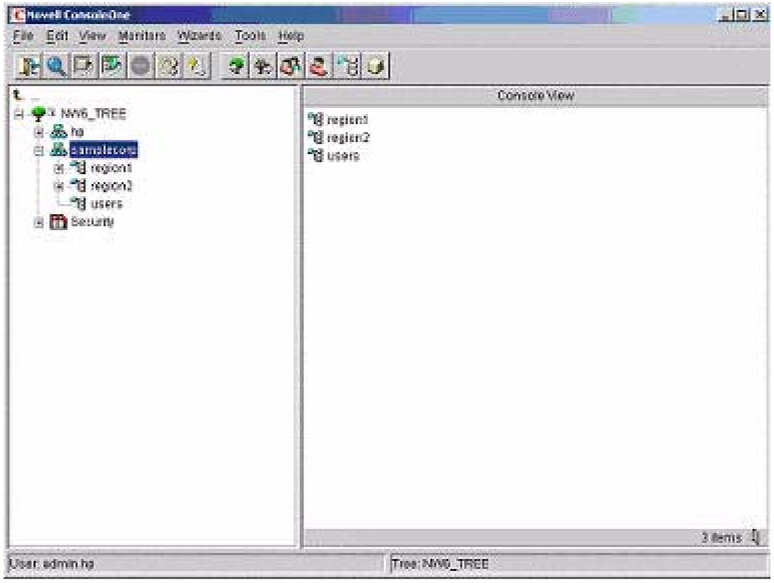
NOTE After you install snap-ins, restart ConsoleOne and MMC to show the new entries.

Example: Creating and Configuring Directory Objects for Use with iLO MP Devices in eDirectory

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

Assume samplecorp has an enterprise directory arranged according to the Figure 8-14.

Figure 8-14 Roles and Devices Example



Begin by creating organizational units in each region to contain the iLO 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

Follow these steps to create iLO MP objects:

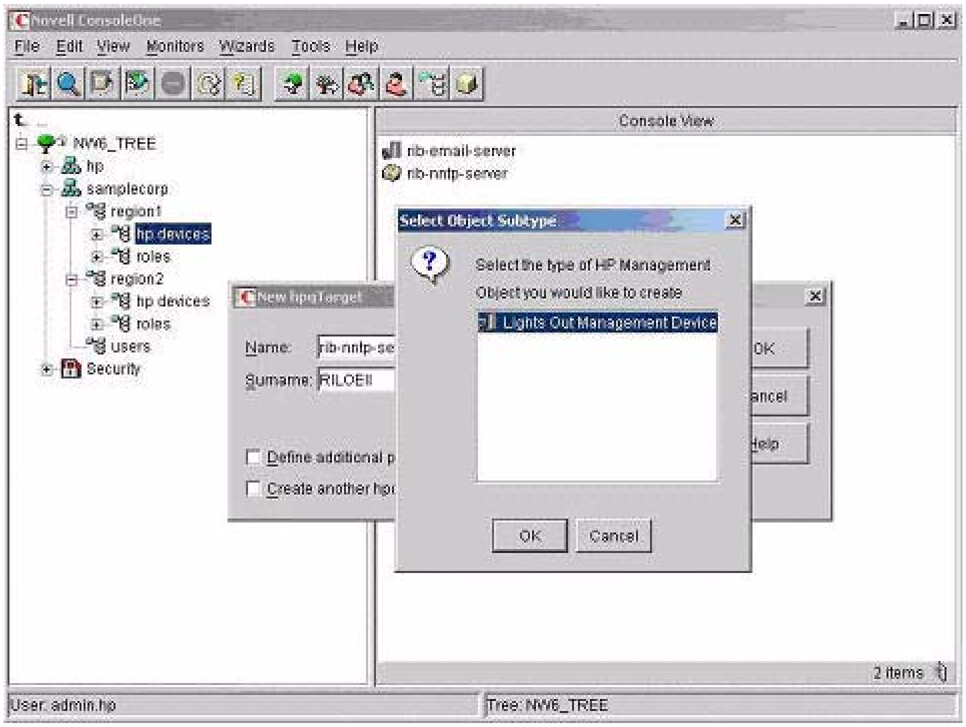
Step 1. Use the HP provided ConsoleOne snap-ins to create iLO MP objects in the **hp devices** organizational unit for several iLO MP devices.

Step 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 MP device, rib-email-server is used as the name of the iLO MP object, and the surname is RILOEII (iLO MP). Click **OK**. The **Select Object Subtype** dialog box (Figure 8-15) opens.

Figure 8-15 Select Object Subtype Dialog Box



Select the type of HP Management Object you would like to create

Lights Out Management Device

Name: rib-nntp-se

Surname: RILOEII

□ Define additional p

□ Create another hpq

User: admin.hp

Tree: NW6_TREE

c. Select **Lights Out Management Device** from the list, and click **OK**.

d. Repeat the process for several more iLO 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

Follow these steps to create roles:

Step 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**.

Step 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.

Step 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**.

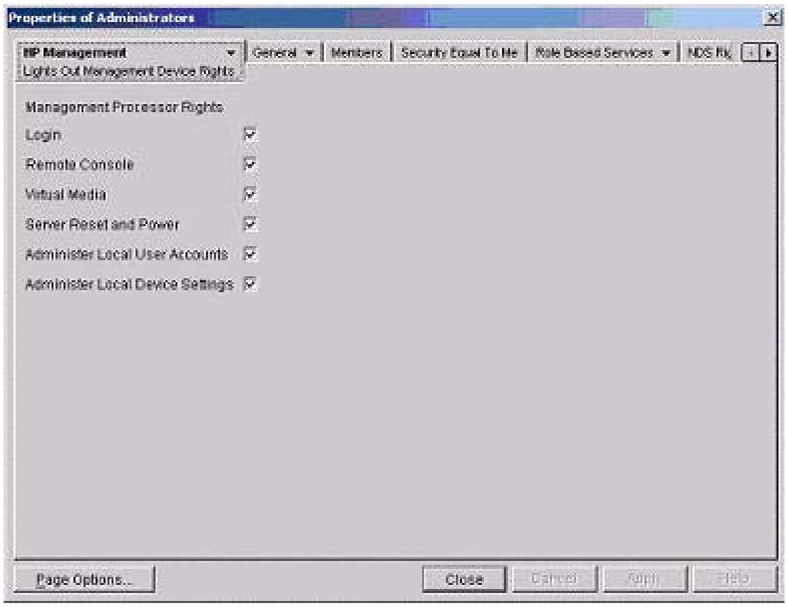
b. Select the **Role Managed Devices** subtab of the **HP Management** tab, and click **Add**.

c. Using the **Select Objects** dialog box, browse to the **hp devices** organizational unit in the region1 organizational unit. Select the three iLO 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 8-16) to set the rights for the role. All users within a role will have the rights assigned to the role on all of the iLO MP devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the iLO MP functionality. Select the boxes next to each right, and click **Apply**. Click **Close** to close the property sheet.

Figure 8-16 Setting Role Rights



Lights Out Management Device Rights

Management Processor Rights

- Login ☑
- Remote Console ☑
- Virtual Media ☑
- Server Reset and Power ☑
- Administer Local User Accounts ☑
- Administer Local Device Settings ☑

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

a. Add the three iLO 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 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 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 MP device and associate it with an iLO MP object used in this example, use settings similar to the following on the iLO 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 MP. He would type csmith (case insensitive) in the **Login Name** field of the iLO MP login and use his eDirectory password in the **Password** field to gain access.

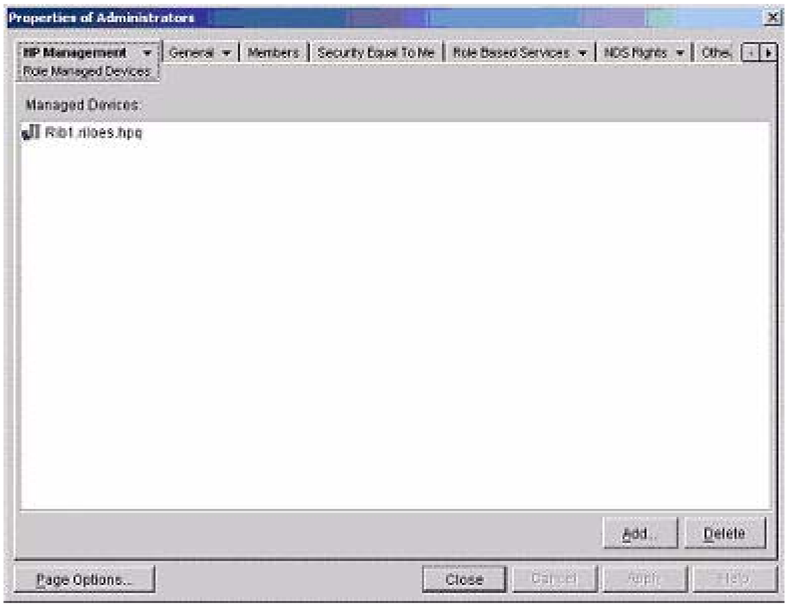
Directory Services Objects for eDirectory

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 8-17) to add the HP devices to be managed within a role. To browse to the specific HP device and add it as a managed device, click **Add**.

Figure 8-17 Role Managed Devices Subtab



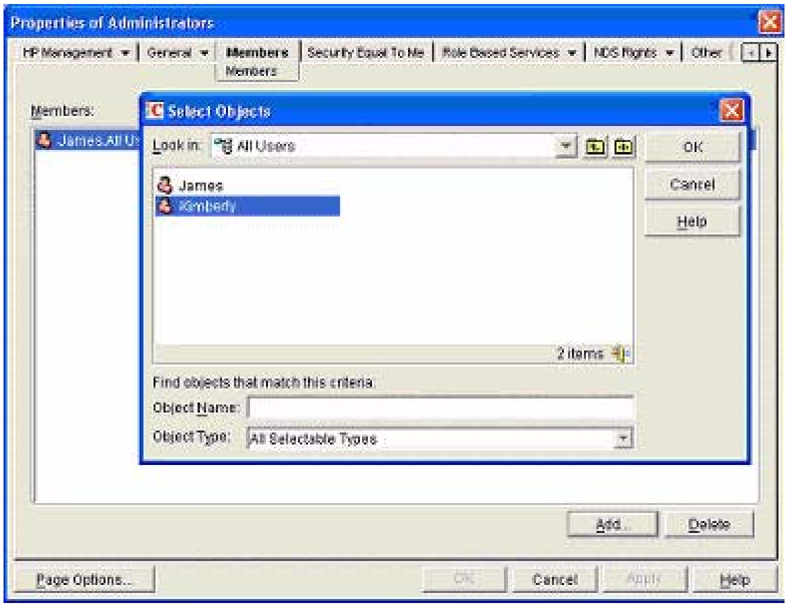
Managed Devices:

Rib1.riloes.hpq

Adding Members

After you create user objects, use the **Members** tab to manage the users within the role. 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**.

Figure 8-18 Members Tab (eDirectory)



Members: James.All Us

Look in: All Users

James
Kimberly

2 items

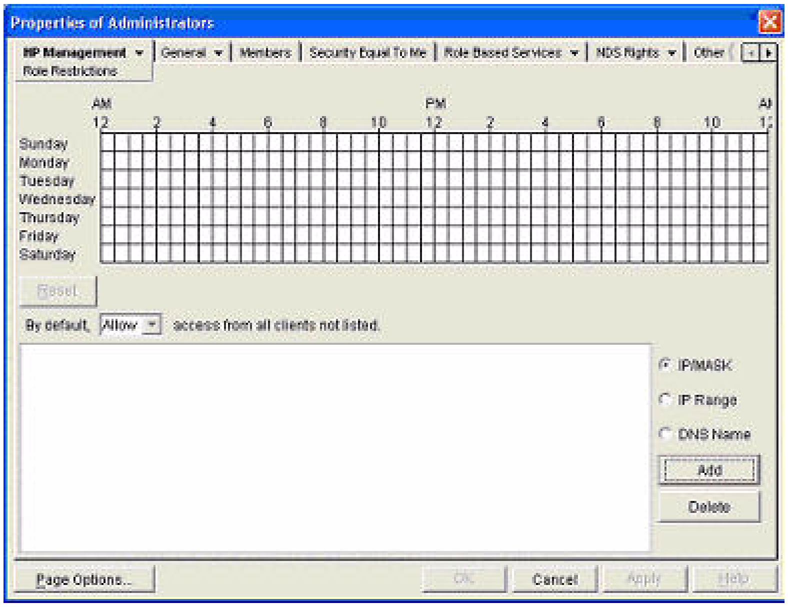
Find objects that match this criteria:
Object Name:
Object Type: All Selectable Types

Setting Role Restrictions

The **Role Restrictions** subtab (Figure 8-19) 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 8-19 Role Restrictions Subtab (eDirectory)



By default, Allow access from all clients not listed.

● 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 8-19). 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

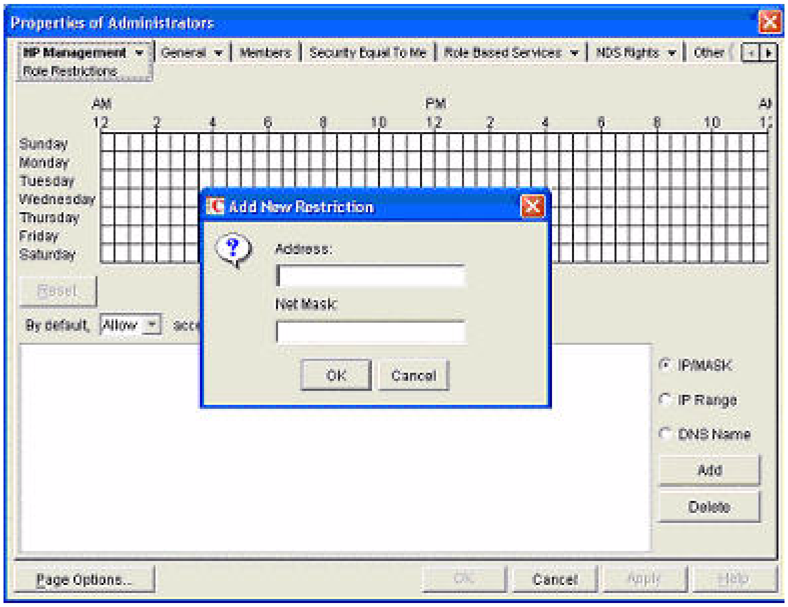
You can grant or deny access to an IP address, IP address range, or DNS names.

In the **By Default** dropdown menu, select whether to allow or deny access from all addresses except the specified IP addresses, IP address ranges, and DNS names.

Step 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.

Step 2. In the **Add New Restriction** pop-up window (Figure 8-20), enter the information, and click **OK**.

Figure 8-20 Add New Restriction Pop-Up Window



Step 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.

Step 4. Enter the information and click **OK.**

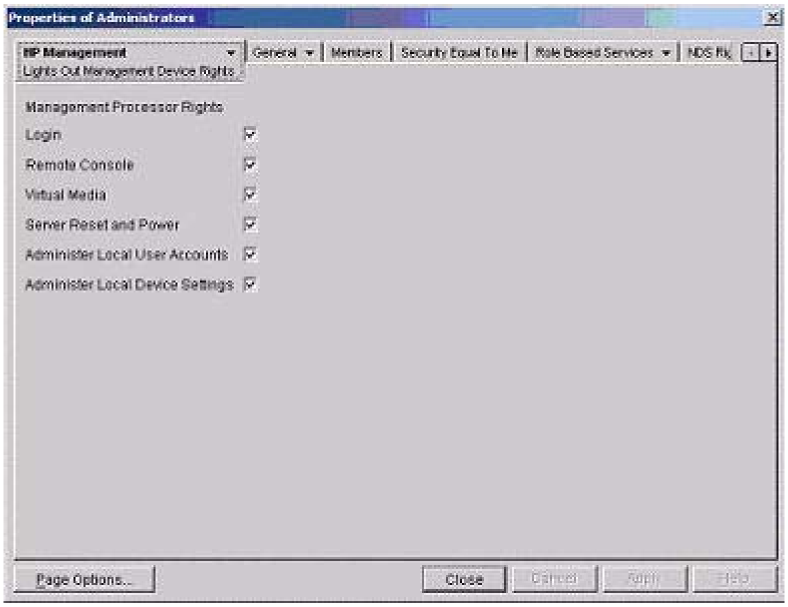
Step 5. Click **Apply** to save the changes.

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 8-21) to manage rights.

Figure 8-21 Lights-Out Management Device Rights Tab



Management Processor Rights

- Login ☑
- Remote Console ☑
- Virtual Media ☑
- Server Reset and Power ☑
- Administer Local User Accounts ☑
- Administer Local Device Settings ☑

The available rights are:

Table 8-2 Lights-Out Management Device Rights

Right	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 MP or the system.
Remote Console	This option enables you to access the system console (the host OS).
Virtual Media	This option is currently not supported.
Server Reset and Power	This option enables you to execute iLO 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 MP user accounts.
Administer Local Device Settings	This option enables you to configure all iLO MP settings, as well as reboot iLO and update iLO 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 MP devices (created using the 'hpqTarget' class), and iLO MP Admins and Monitors (created using the 'hpqRole' class). These objects support the Login Authentication utility to the iLO MP device and enable iLO 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:

Step 1. To determine the Java version, execute the following command:

```
# java -version
```

The Java version installed on your system is displayed.

Step 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.

Step 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
```

Step 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.sh` file is executed.

NOTE The `hpdsse.sh` file is obtained when the `Schema.tar` tarball is extracted. This process is explained in the Schema Extension section. You can download schema extensions from the link **`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:

Step 1. Download the tar file to the Linux system on which eDirectory is installed.

Step 2. Extract the tar file to obtain the `hpdsse.sh` file by executing the following command:

```
# tar -xvf Schema. tar
```

Step 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.

Step 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:

Step 1. Launch **ConsoleOne** and log on to the tree.

Step 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 iLO MP (LDAP Command)

Use the **LDAP Command Menu** to configure in the iLO MP CLI to configure iLO 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: 15.255.1.1
-> 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 : 15.255.1.1
 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 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:

Step 1. Select **Start>Settings>Control Panel**.

Step 2. Double-click **Add/Remove Programs**.

Step 3. Click **Add/Remove Windows Components** to start the Windows Components wizard.

Step 4. Select the **Certificate Services** checkbox. Click **Next**.

Step 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.

Step 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**.

Step 7. Accept the default locations of the certificate database and the database log. Click **Next**.

Step 8. Browse to the `c:\I386` folder when prompted for the Windows 2000 Advanced Server CD.

Step 9. Click **Finish** to close the wizard.

Verifying Directory Services

Because the iLO 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:

Step 1. Select **Start>Run**, and enter **`mmc`**.

Step 2. Click **Add**.

Step 3. Select **Group Policy**, and click **Add** to add the snap-in to the MMC.

Step 4. Click **Browse**, and select the **Default Domain Policy** object. Click **OK**.

Step 5. Select **Finish>Close>OK**.

Step 6. Expand **Computer Configuration>Windows Settings>Security Settings>Public Key Policies**.

Step 7. Right-click **Automatic Certificate Requests Settings**, and select **New>Automatic Certificate Request**.

Step 8. Click **Next** when the Automatic Certificate Request Setup wizard starts.

Step 9. Select the **Domain Controller** template, and click **Next**.

Step 10. Select the certificate authority listed. (It is the same CA defined during the Certificate Services installation.) Click **Next**.

Step 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 MP product. See “Directory Services” on page 100 to familiarize yourself. Make sure you understand the examples and are comfortable with setting up.

Directory-enabled remote management enables you to:

- Create iLO MP objects

  Create one iLO MP device object to represent each device that will use the directory service to authenticate and authorize users. See “Directory Services” on page 100 for additional information on creating iLO MP device objects for Active Directory (“Directory Services for Active Directory” on page 106) and eDirectory (“Directory Services for eDirectory” on page 119). In general, you can use the HP provided snap-ins to create objects. It is useful to give the iLO MP device objects meaningful names, such as the device's network address, DNS name, host server name, or serial number.

- Configure iLO MP devices

  Every iLO 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 iLO MP (LDAP Command)” on page 129 for details on the specific directory settings. In general, you configure each device with the appropriate directory server address, iLO 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 MP role objects. When the devices are associated with the role objects, you can control access to the iLO 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 MP object representing the iLO MP device. Some environments require the same trustees of a role to also be read trustees of the iLO MP object to successfully authenticate users.

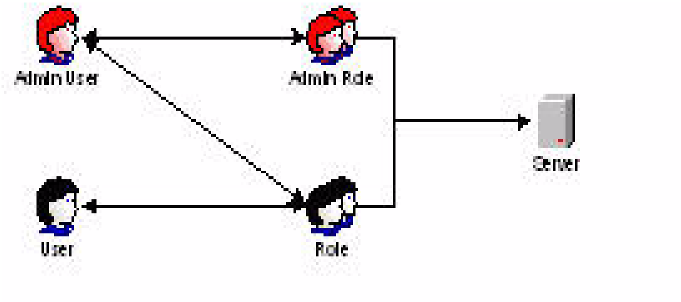
Using Multiple Roles

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.

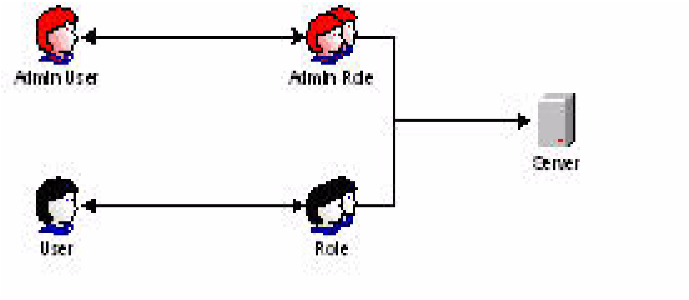
Typically, a directory administrator creates a base role with the minimum number of rights assigned and creates additional roles to add additional rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization can have two types of users: administrators of the iLO MP device or host server and users of the iLO 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 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” on page 125 or “Setting Time Restrictions” on page 125.

Role Time Restrictions

You can place time restrictions on iLO MP roles. Users are granted the rights specified for the iLO MP devices listed in the role, only if they are members of the role and meet the time restrictions for that role.

iLO MP devices use local host time to enforce time restrictions. If the iLO 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 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 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 MP firmware, can cause the iLO MP device clock to not be set. Also, the host time must be correct for the iLO 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.

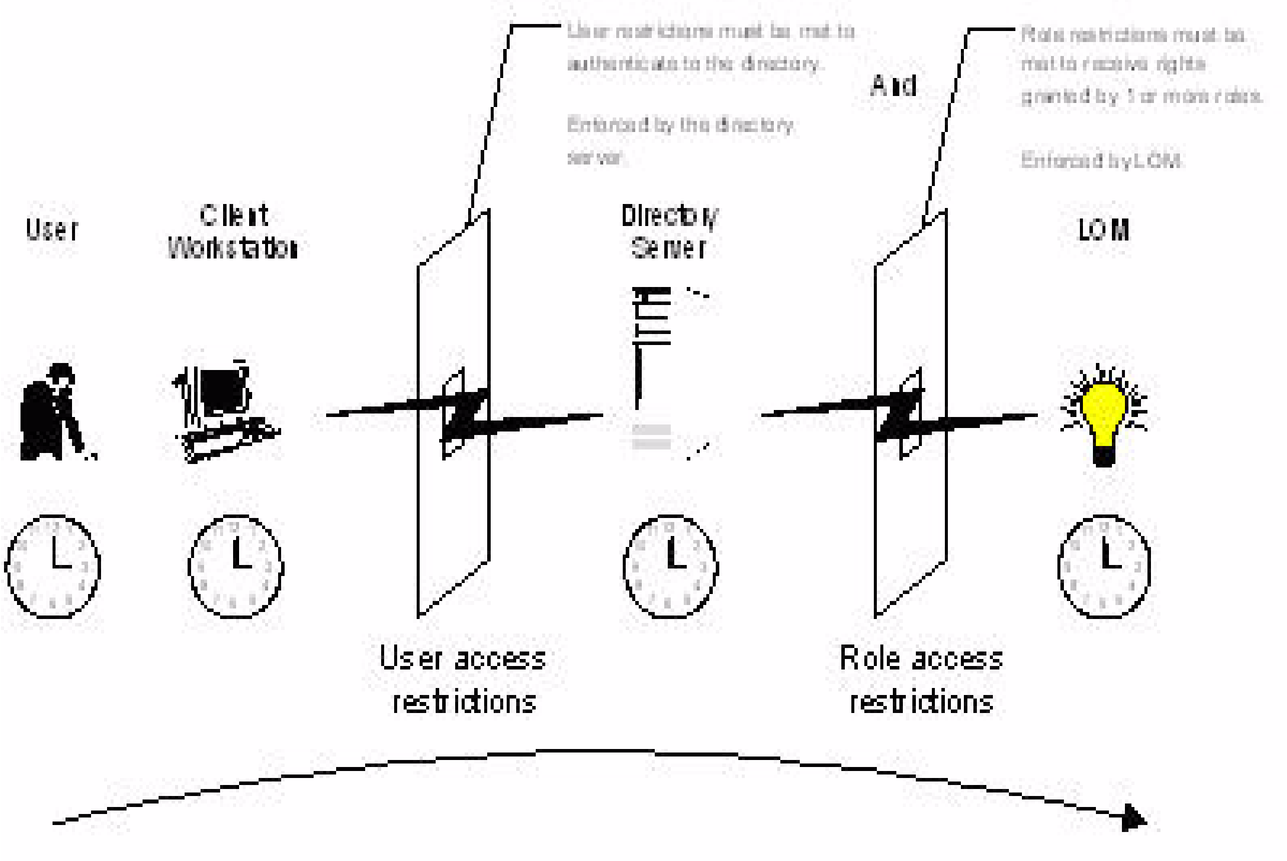
Role Address Restrictions

Role address restrictions are enforced by the iLO 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

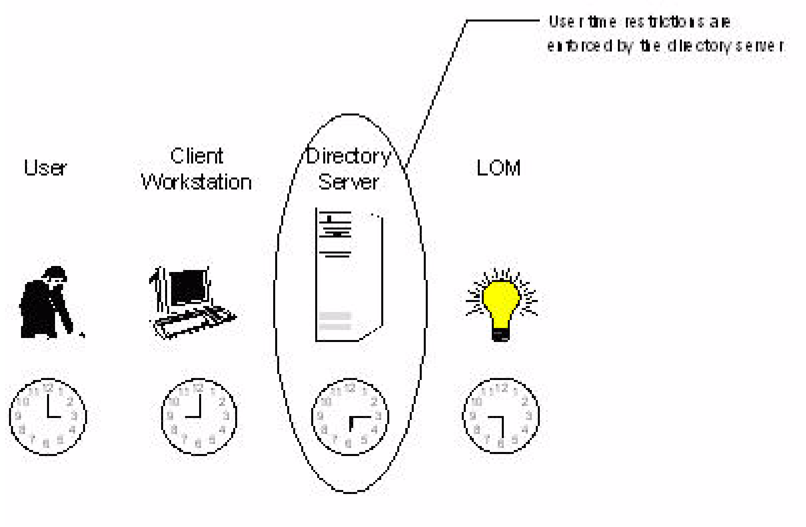
The following figure shows how two sets of restrictions potentially limit a directory user's access to iLO MP devices. User access restrictions limit a user's access to authenticate to the directory. Role access restrictions limit an authenticated user's ability to receive iLO MP privileges based on rights specified in one or more roles.


User restrictions must be met to authenticate to the directory.
Enforced by the directory server.
And
Role restrictions must be met to receive rights granted by 1 or more roles.
Enforced by LOM.
User
Client Workstation
Directory Server
LOM
User access restrictions
Role access restrictions

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 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 MP device as a directory user, the iLO 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 MP device. However, because the user is proxied at the iLO MP device, the network address of the authentication attempt is that of the iLO MP device, not that of the client workstation.

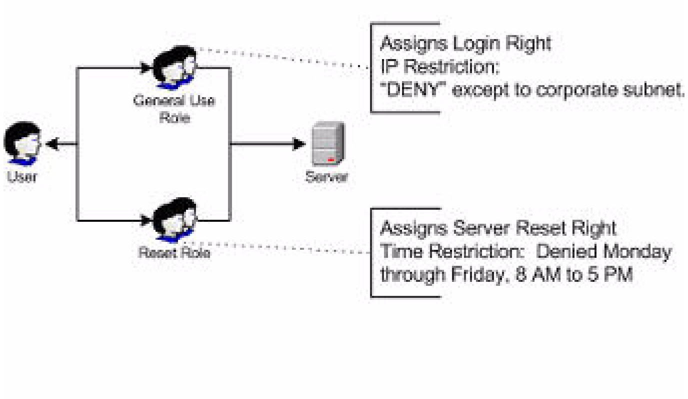
Creating Multiple Restrictions and Roles

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 MP administrators are allowed to use the iLO MP device from within the corporate network but are only able to reset the server outside of regular business hours.

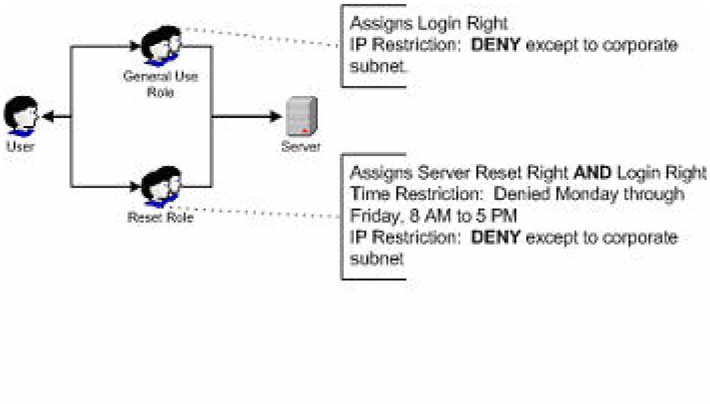
Directory administrators may be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to an after-hours application may allow administrators outside the corporate network to reset the server, 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.


Assigns Login Right
IP Restriction:
"DENY" except to corporate subnet.
General Use Role
User
Server
Reset Role
Assigns Server Reset Right
Time Restriction: Denied Monday through Friday, 8 AM to 5 PM

Alternatively, the directory administrator could create a role that grants the login right and restrict it to the corporate network, create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration can create another role that grants users from addresses outside the corporate network the login right, which could unintentionally grant the iLO 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.


Assigns Login Right
IP Restriction: **DENY** except to corporate subnet.
General Use Role
User
Server
Reset Role
Assigns Server Reset Right **AND** Login Right
Time Restriction: Denied Monday through Friday, 8 AM to 5 PM
IP Restriction: **DENY** except to corporate subnet

Directory Services Schema (LDAP)

A directory schema specifies the types of objects that a directory may have and the mandatory and optional attributes of each object type. The following sections describe both the HP management core, and the iLO 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 8-3 lists the core LDAP OID classes.

Table 8-3 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

Core Attributes

Table 8-4 lists the core LDAP OID attributes.

Table 8-4 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
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core Class Definitions

Table 8-5, Table 8-6, and Table 8-7 define the HP Management core classes.

hpqTarget

Table 8-5 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—1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2
Remarks	None

hpqRole

Table 8-6 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—1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Remarks	None

hpqPolicy

Table 8-7 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

Table 8-7 hpqPolicy (Continued)

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Remarks	None

Core Attribute Definitions

Table 8-8 through Table 8-13 define the HP Management core class attributes.

hpqPolicyDN

Table 8-8 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 8-9 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 8-10 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 8-11 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 8-12 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
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 8-13 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 MP-Specific LDAP OID Classes and Attributes

The schema attributes and classes in Table 8-14 and Table 8-15 may depend on attributes or classes defined in the HP Management core classes and attributes.

iLO MP Classes

Table 8-14 iLO MP Classes

Class Name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

iLO MP Attributes

Table 8-15 iLO 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 8-15 iLO 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 MP Class Definitions

Table 8-16 defines the iLO MP core class.

hpqLOMv100

Table 8-16 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 products.
Class Type	Auxiliary
SuperClasses	None
Attributes	hpqLOMRightConfigureSettings—1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin—1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin—1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole—1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset—1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia—1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

iLO MP Attribute Definitions

Table 8-17 through Table 8-21 define the iLO MP core class attributes.

hpqLOMRightLogin

Table 8-17 hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Login Right for HP iLO 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 8-18 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Remote console right for iLO 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.

hpqLOMRightServerReset

Table 8-19 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 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 8-20 hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Local User Database Administration Right for HP iLO 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 8-21 hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Configure Devices Settings Right for HP iLO MP products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued

Table 8-21 hpqLOMRightConfigureSettings (Continued)

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

Glossary

A

Address In networking, a unique code that identifies a node in the network. Names such as **host1.hp.com** are translated to dotted-quad addresses like **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

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.

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).

C

Command Line Interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

D

DDNS Short for dynamic Domain Name System, its the way iLO can automatically get its name registered by the Domain Name System, so when iLO gets its new IP address from DHCP, users can connect to the new iLO using the host name, rather than the new IP number.

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.

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.

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 ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.

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

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.

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) A 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, 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

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

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.

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 might 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.

SNMP Simple Network Management Protocol. A set of protocols for managing complex networks.

SSH Secure Shell. A UNIX shell program and network protocol that enables secure and encrypted log in and execution of commands on a remote system over an insecure network.

SSL Secure Sockets Layer. A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a Web server and a Web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

Subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

Subnet Mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an **address mask**.

System Event Log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

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, modems, and printers, to the computer system.

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 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 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 Name A combination of letters, and possibly numbers, that identifies a user to the system.

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