HP Integrated Lights-Out User Guide

invent

July 2004 (Sixth Edition)
Part Number 238882-006

© Copyright 2004 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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.

Microsoft, Windows, Windows NT, and MS-DOS are U.S. registered trademarks of Microsoft Corporation. Linux is a U.S. registered trademark of Linus Torvalds. Java is a U.S. trademark of Sun Microsystems, Inc. UNIX is a registered trademark of The Open Group.

HP Integrated Lights-Out User Guide

July 2004 (Sixth Edition)
Part Number 238882-006

Audience Assumptions

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

Contents

Operational Overview 15

Configuring iLO 21

Using iLO 39

Certificate Services 189

Directory-Enabled Remote Management 193

Lights-Out Directories Migration Utilities 205

Insight Manager 7 Integration 223

Systems Insight Manager Integration 233

Group Administration and iLO Scripting 241

Operational Overview

In This Section

New in This Version

- Secure Shell (on page 123)
- Virtual Media Scripting (on page 79)
- iLO Shared Network Port (on page 125)
- Command Line Interface (on page 130)
- ProLiant BL p-Class Configuration (on page 31)
- Telnet Simple Command Set (on page 117)
- Updated Web interface screens:
  - Global Settings (on page 89)
  - Network Settings (on page 91)
- New and updated RIBCL commands:
  - RIBCL RACK_INFO commands (on page 36)
  - MOD_GLOBAL_SETTINGS (on page 294)
  - MOD_NETWORK_SETTINGS (on page 289)
  - GET_EVENT_LOG (iLO Event Log)
  - INSERT_VIRTUAL_MEDIA (on page 325)
  - EJECT_VIRTUAL_MEDIA (on page 327)

- GET_VM_STATUS (on page 328)
- SET_VM_STATUS (on page 329)

Usage Model

The common usage model for iLO is a client PC running a supported browser using DHCP and DNS protocols connected to one or more iLO devices. To use iLO, plug in the power of the host server and connect an Ethernet cable to the dedicated iLO management port of the server. You can then use your Web browser to connect to iLO over an SSL connection. When logged in, you can remotely control the server from your client desktop.

Graphical Remote Console (on page 52), Virtual Media (on page 64), Terminal Services Pass-through Option (on page 109), and Directory Services (on page 143) are advanced functions that must be enabled by licensing the optional iLO Advanced Pack.

Linux customers might prefer connecting to iLO using the SSH interface instead of a browser.

Network Connection Overview

There are three general network connection scenarios. iLO can be connected on:

- A corporate network with both ports connected to the corporate network. In this configuration, the server has two network ports (one server NIC, and one iLO NIC) connected to a corporate network. This connection enables access to iLO from anywhere on the network. On a corporate network, however, network traffic can hinder iLO performance.

  A coroporate network configuration reduces the amount of networking hardware and infrastructure required to support iLO because iLO uses existing DNS and DHCP servers and routers.

- A dedicated management network with the iLO port on a separate network. A separate network improves performance and security, and provides redundant access to the server when a hardware failure occurs on the corporate network. In this configuration, iLO cannot be accessed directly from the corporate network.

A separate network increases the security of the management network because you can physically control which workstations are connected to the network.

- An iLO Shared Network Port using the server's NIC instead of the dedicated iLO management NIC for server management. This configuration simplifies the network and reduces total network cost. Fewer cables, hubs, and switches are needed because both regular and iLO network traffic comes through the system NIC.

  The main disadvantage of using the iLO Shared Network Port for iLO server management is the lack of speed compared to the dedicated iLO management NIC. As a result, not all iLO management features are available through the iLO Shared Network Port configuration.

Supported Server Operating System Software

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.

Graceful host operating system shutdown, Insight Manager 7, and Systems Insight Manager integration require Health Drivers and Management Agents or remote console access.

iLO provides two interface drivers:

- iLO Advanced Server Management Controller Driver (Health Driver)—This driver provides system management support, including monitoring of server components, event logging, and support for the Management Agents.
- iLO Management Interface Driver—This driver enables system software and SNMP Insight Agents to communicate with the iLO.

These drivers and agents are available for the following network operating systems:

- Microsoft®
  - Windows NT® 4.0 Server
  - Windows NT® 4.0, Enterprise Edition

  - Windows® 2000 Server
  - Windows® 2000 Advanced Server
  - Windows® Server 2003
- Linux
  - Red Hat Linux 7.2
  - Red Hat Linux 7.3
  - Red Hat Linux 8.0
  - Red Hat Enterprise Linux AS 2.1
  - Red Hat Enterprise Linux 3
  - SuSE Linux Enterprise Server 7.0
  - SuSE Linux Enterprise Server 9.0
  - UnitedLinux 1.0
- Novell
  - NetWare 6
  - NetWare 6.5

Supported Browsers

- Microsoft® Internet Explorer
  - Minimum—Microsoft® Internet Explorer 6 with Service Pack 1 or later for Windows® 2000 or Windows® XP. If using single-cursor mode in Remote Console, Java™ 1.3.1_02 or greater, JVM is required.
  - Recommended—Microsoft® Internet Explorer 6.0 or later and Java™ 1.4.X JVM for Windows® 2000 or Windows® XP. To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvml).
- Linux
  - Netscape 7.10

- Mozilla 1.60

  Mozilla 1.60 is not supported on United Linux 1.0. Please use Mozilla 1.70. Linux, Netscape, and Mozilla require Java™ 1.4.2 JVM. To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvml).

Certain browsers and operating system combinations might not work correctly depending on their implementations of the required browser technologies.

Linux Browser Configuration

iLO firmware supports Mozilla 1.46 and Netscape 7.10 to access iLO.

Linux-based browsers have the following limitations:

- Only the KDE desktop is supported.
- A known issue prevents the use of links in the pop-up tab menus when the browser window does not have focus. If a clickable item is behind the pop-up menu, the click event is handled as if you had clicked that item. Otherwise, the mouse click will have no effect.

The font configuration of the desktop and browser can affect the placement of pop-up tab menus. A fixed font of 12 points is required for proper placement. If the pop-up menus are not in their proper position, you will find it difficult to move the mouse from the tab to the pop-up menu before the menu can "pop down." In this situation, the user should select the desired tab and use the menu window to select the desired page. Alternatively, you can change the font size in the browser. Refer to "Configuring Linux Font Size (on page 19)" for information.

Configuring Linux Font Size

To change font size:

1. Open the KDE Control Center panel and set the fonts.
2. Start Mozilla or Netscape and configure the fonts using the Fonts—Control Center. Set the minimum font size to 12.

Configuring iLO

In This Section

iLO Configuration Options

iLO comes preconfigured with default factory settings, including a default user account and password. If iLO is connected to a network running DNS or DHCP, you can use it immediately without changing any settings. For greater security and reliability, you can connect iLO to a separate dedicated management network.

Some advanced features require the operating system ("Supported Server Operating System Software" on page 17) drivers be installed.

iLO offers several configuration options:

- iLO RBSU (on page 22)
- Browser-based setup (on page 23)
- Remote scripted setup (on page 24) using CPQLOCFG
- Local scripted deployment using CPQLODOS (on page 252)
- Local on-line scripted setup using HPONCFG ("HPONCFG Online Configuration Utility" on page 261)

iLO RBSU

HP recommends iLO RBSU to initially set up iLO and initially configure iLO network parameters for environments that do not use DHCP and DNS or WINS. RBSU provides the basic tools to configure iLO network settings and user accounts to get iLO onto the network.

iLO RBSU is designed to assist you with setting up iLO on a network. iLO is not intended for continued administration. RBSU is available every time the server is booted and can be run remotely using the iLO Remote Console. You can use RBSU to configure network parameters, directory settings, global settings, and user accounts.

iLO RBSU can be disabled in the Global Settings preferences. Disabling iLO RBSU prevents reconfiguration from the host unless the iLO Security Override Switch is set.

To run iLO RBSU:

1. Restart or power up the server.
2. Press the **F8** key when prompted during POST. The iLO RBSU runs.
3. If prompted, enter a valid iLO user ID and password with the appropriate iLO privileges (**Administer User Accounts>Configure iLO Settings**). Default account information is located on the iLO Default Network Settings tag attached to the server containing the iLO management processor. If iLO has not been configured to present a login challenge to the RBSU. No prompt will appear.
4. Make and save any necessary changes to the iLO configuration.
5. Exit iLO RBSU.

HP recommends using DNS or DHCP with iLO to simplify installation. If DNS/DHCP cannot be used, use the following procedure to disable DNS and DHCP and configure the IP address and the subnet mask:

1. Restart or power up the server.
2. Press the **F8** key when prompted during POST. The iLO RBSU runs.

3. Enter a valid iLO user ID and password with the appropriate iLO privileges (**Administer User Accounts>Configure iLO Settings**). Default account information is located on the iLO Default Network Settings tag.
4. Select **Network>DNS/DHCP**, press the **Enter** key, and then select **DHCP Enable**. Press the spacebar to turn off DHCP. Be sure that DHCP Enable is set to Off, and save the changes.
5. Select **Network>NIC>TCP/IP**, press the **Enter** key, and enter the appropriate information in the IP Address, Subnet Mask, and Gateway IP Address fields.
6. Save the changes.
7. Exit iLO RBSU. The changes take effect when you exit iLO RBSU.

Browser-Based Setup

Use the browser-based setup method if you can connect to iLO on the network using a browser. You can also use this method to reconfigure a previously configured iLO.

1. Access iLO from a remote network client using a supported Web browser, and provide the default DNS name, user name, and password. Default DNS name and account information is located on the iLO Network Settings tag attached to the server containing the iLO management processor.

   When you successfully log onto iLO, you can change the default values of the network, user, and SNMP alerting settings through the Web browser interface.

2. Enter the activation key to enable iLO Advanced features.

   If the iLO Advanced features are licensed, you can deploy your operating system using the Virtual Floppy Drive and install operating system drivers and Insight Manager agents on the remote host server using the graphical Remote Console.

   For ProLiant BL p-Class servers, iLO Advanced functionality is already enabled and cannot be disabled.

Scripted Setup

Scripts can initially configure an iLO system. The configuration scripts are text files written in a style of XML called RIBCL. You can use RIBCL scripts to configure iLO on the network, during initial deployment, or from an already deployed host. RIBCL is sent across the network in a script file. iLO scripting enables you to configure User Administration, Global Settings, Network Settings, SNMP/Insight Manager Settings, Upgrade iLO Firmware, Licensing, and ProLiant BL p-Class Rack Settings. The iLO management processor supports several scripting solutions for configuration and control of the iLO and the host server.

- CPQLOCFG is a Windows® utility that sends RIBCL scripts to iLO over the network.
- CPQLODOS ("Lights-Out DOS Utility" on page 249) is a DOS deployment utility (part of the SmartStart scripting toolkit) that runs on the host during SmartStart or RDP deployment.
- Perl ("Perl Scripting" on page 255) is a scripting language that can be used from Linux clients to send RIBCL scripts to iLO over the network.
- HPONCFG is a utility that runs on the host and passes RIBCL scripts to the local iLO. There are Windows® and Linux versions of this utility, which requires the HP iLO Management Interface Driver.

Scripting can be integrated with the SmartStart Scripting Toolkit. Scripting can also be launched with:

- Windows® client
- ProLiant Essentials Rapid Deployment Pack
- Insight Manager 7
- Systems Insight Manager

Installing iLO Device Drivers

The SmartStart Software Maintenance CD contains all of the necessary support for your server, or you can download all the necessary iLO support drivers from the HP website (http://www.hp.com/servers/lights-out).

To download the drivers:

1. Click the iLO graphic.
2. Select **Software and Drivers.**

The iLO Management Interface Driver allows system software like SNMP Insight Agents and Terminal Services pass-through service to communicate with iLO.

Microsoft Windows NT, Windows 2000, and Windows Server 2003 Driver Support

The device drivers that support the iLO are part of the PSP that is located on the HP website (http://www.hp.com/support) or on the SmartStart CD. Before you install the Windows® drivers, obtain the Windows® documentation and the latest Windows® Service Pack.

iLO Pre-requisite Files for Microsoft®

The CPQCIDRV.SYS file provides the iLO Management Interface Driver support.

The CPQASM2.SYS, SYSMGMT.SYS, SYSDOWN.SYS files provide the iLO Advanced Server Management Controller Driver support.

Installing or Updating the iLO Drivers for Microsoft®

The PSP for Microsoft® Windows® products includes an installer that analyzes system requirements and installs all drivers.

The PSP is available on the HP website (http://www.hp.com/support) or on the SmartStart CD.

> **NOTE:** If you are updating the iLO drivers, be sure that the iLO is running the latest version of the iLO firmware. The latest version can be obtained as a Smart Component from the HP website (http://www.hp.com/servers/lights-out).

To install the drivers in the PSP, download the PSP from the HP website (http://www.hp.com/support), run the SETUP.EXE file included in the download, and follow the installation instructions. For additional information about the PSP installation, read the text file included in the PSP download.

Novell NetWare Server Driver Support

The device drivers required to support iLO are part of the PSP that is located on the SmartStart CD and the HP website (http://www.hp.com/support).

iLO Pre-Requisite Files for NetWare

The CPQHLTH.NLM file provides the Health Driver for NetWare.

The CPQCI.NLM file provides the iLO Management Interface Driver support.

Installing or Updating iLO Drivers for NetWare

The PSP for Novell NetWare includes an installer that analyzes system requirements and installs all drivers. The PSP is available on the HP website (http://www.hp.com/support) and on the SmartStart CD.

When updating iLO drivers, be sure iLO is running the latest version of the iLO firmware. The latest version can be obtained as a Smart Component from the HP website (http://www.hp.com/servers/lights-out).

To install the drivers, download the PSP from the HP website (http://www.hp.com/support) to a NetWare server. After the PSP has been downloaded, follow the NetWare component installation instructions to complete the installation. For additional information about the PSP installation, read the text file included in the PSP download.

When using NetWare 6.X, a RAGE-XL video driver is provided by the operating system and should be used for best results.

Red Hat Linux and SuSE Linux Server Driver Support

The device drivers required to support iLO for Red Hat Linux and SuSE Linux are located on the SmartStart CD, Management CD, or on the HP website (http://www.hp.com/support).

iLO Pre-requisite Files for Red Hat and SuSE Linux Files

You can download the PSP files containing the iLO driver, the foundation agents, and health agents from the HP website (http://www.hp.com/support). The instructions on how to install or update the iLO driver are available on the website. The HP Management Agents for Linux are:

- ASM package (hpasm) which combines the health driver, IML viewer, foundation agents, health agent, and standard equipment agent into one package.
- RSM package (hprsm) which combines the RIB driver, rack daemon, RIB agent, and rack agent into one package.

Instaling or Updating iLO Linux and SuSE Drivers

If necessary, uninstall earlier agents. To uninstall earlier agents, execute the following:

- `rpm –e cpqci`
- `rpm –e cpqriisd` (for BL p-Class servers)
- `rpm –e cmanic`
- `rpm –e cmastor`
- `rpm –e cmasvr`
- `rpm –e cmafdtn`
- `rpm –e cpqhealth`

To load the Health and iLO driver packages use the following commands :

```
rpm –ivh hpasm-d.vv.v-pp.Linux_version.i386.rpm
rpm –ivh hprsm-d.vv.v-pp.Linux_version.i386.rpm
```

where: *d* is the Linux distribution and version and

vv.v-pp are version numbers.

For additional information, refer to the Software and Drivers website (http://www.hp.com/support).

To remove the Health and iLO drivers use the following commands:

```
rpm –e hprsm
rpm –e hpasm
```

For additional information, refer to the Software and Drivers website (http://www.hp.com/support).

Enabling iLO Advanced Functionality

The optional iLO Advanced Pack extends the standard Lights-Out functionality to include:

- Graphical Remote Console (on page 52)
- Virtual Media (on page 64) (including Virtual Floppy and Virtual CD)
- Directory-based authentication and authorization ("Directory-Enabled Remote Management" on page 193)
- Terminal Services pass-through option (on page 109)

Advanced functionality is enabled by licensing the optional iLO Advanced Pack. The iLO Advanced Pack contains an activation key that you must enter into iLO to enable advanced functionality. The advanced features can be evaluated using a 30-day evaluation key which you can download for free from the HP website (http://www.hp.com/servers/lights-out). For more information, refer to the "iLO Advanced Evaluation License (on page 29)" section.

The iLO Advanced Pack license key can be installed using RIBCL scripts or using a browser.

iLO Advanced Evaluation License

A free 30-day evaluation license is available for download on the HP website (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html). The evaluation license will activate and access iLO Advanced features. Only one evaluation license can be installed per iLO. After the evaluation period, an iLO Advanced license is required to continue using the advanced features. iLO Advanced features automatically deactivate when the evaluation license key expires.

The evaluation license key can be installed using a browser or using RIBCL scripts.

iLO Advanced License Options

In addition to the standard single-server iLO Advanced, two other licensing options are available:

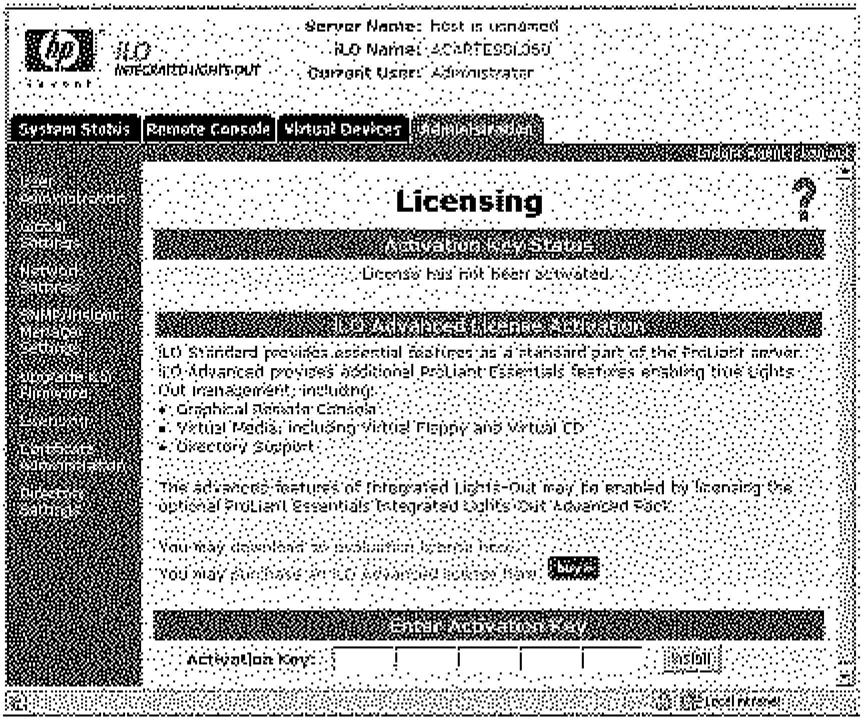
- The Flexible Quantity License Kit allows customers to purchase a single software package, one copy of the documentation, and a single license key to activate the exact number of licenses requested.
- The MLA is available for customers who want a single key for licenses of a value pack product that they plan to purchase incrementally over time.

For additional information, refer the HP website (http://h18004.www1.hp.com/products/servers/proliantessentials/valuepack/licensing.html).

Activating iLO Advanced Features Using a Browser

1. Log on to iLO through a supported Web browser.
2. Select the **Administration** tab.

3. Click **Licensing** to display the iLO Advanced license activation screen.



Server Name: host is unnamed
iLO Name: ACARTESOIL050
Current User: Administrator

Licensing

Activation Key Status

License has not been activated.

iLO Advanced License Activation

iLO Standard provides essential features as a standard part of the ProLiant server. iLO Advanced provides additional ProLiant Essentials features enabling true Lights-Out management, including:

- Graphical Remote Console
- Virtual Media, including Virtual Floppy and Virtual CD
- Directory Support

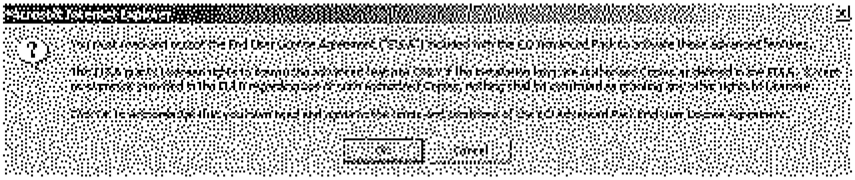
The advanced features of Integrated Lights-Out may be enabled by licensing the optional ProLiant Essentials Integrated Lights-Out Advanced Pack.

You may download an evaluation license here.
You may purchase an iLO Advanced license here. [Here]

Enter Activation Key

Activation Key: ____ ____ ____ ____ ____ [Install]

4. Enter the activation key in the space provided. The EULA confirmation appears. The EULA details are available on the HP website (http://www.hp.com/servers/lights-out) and with the Advanced Pack License kit.



You must read and accept the End User License Agreement ("EULA") included with the iLO Advanced Pack to activate these advanced features.

[illegible]

Click OK to acknowledge that you have read and agree to the terms and conditions of the iLO Advanced Pack End User License Agreement.

5. Click **OK.**

The advanced features of iLO are now enabled.

Activating iLO Advanced Using Scripting

To activate iLO Advanced using CPQLODOS:

1. Add the following statements in the XML script file. The script is saved by CPQLODOS as iLO.xml.

   ```
   <SET_LICENSE>
   <LICENSE_KEY VALUE="1234567890ABCDEFGHIJKLMNO" />
   </SET_LICENSE>
   ```

2. Execute the following CPQLODOS command to activate the iLO license key:

   ```
   cpqlodos /load_xml =iLO.xml
   ```

Refer to the "Lights-Out DOS Utility (on page 249)" section, for more information on using CPQLODOS.

To activate iLO Advanced using CPQLOCFG or HPONCFG:

Use the following RIBCL sample script with CPQLOCFG and HPONCFG to install an iLO Advanced license key:

```
<RIBCL version="2.0">
<LOGIN  USER_LOGIN="Administrator" PASSWORD =
"password">
   <RIB_INFO MODE="w" >
   <LICENSE>
      <ACTIVATE KEY="1234567890ABCDEFGHIJKLMNO" />
   </LICENSE>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

ProLiant BL p-Class Configuration

ProLiant BL p-Class servers can be accessed and configured through the iLO Diagnostic Port on the front of the server. You can also use the "Browser-Based Setup (on page 23)" to initially configure the system through the iLO Diagnostic Port.

On select p-Class blades in enclosures with updated management backplanes that support BL30P (high density) blades, iLO can be used for initial enclosure static IP configuration. Initial configuration of the blade in bay 1 allows all subsequent iLOs in the enclosure to receive predetermined static IP assignments. This feature is supported in iLO 1.55 and later.

Static IP Bay Configuration

Static IP bay configuration, implemented using the new Static IP Bay Settings on the BL p-Class tab, eases the initial deployment of an entire enclosure or the subsequent deployment of blades within an existing enclosure. While the preferred method for assigning IP addresses the iLO to each blade is through DHCP and DNS, these protocols are not always available on non-production networks.

Static IP bay configuration automates the first step of BL p-Class blade deployment by enabling the iLO management processor in each blade slot to obtain a predefined IP address without relying on DHCP. iLO is immediately accessible for server deployment using Virtual Media and other remote administration functions.

Static IP bay configuration uses the Static IP Bay Configuration addressing method which enables you to assign IP addresses to each iLO based on slot location in the respective server enclosure. By providing a set of IP addresses in the enclosure, you gain the advantages of a static IP bay configuration, without requiring each individual iLO to be configured locally.

Using iLO static IP bay configuration:

- Helps avoid the costs of a DHCP infrastructure to support the blade environment
- Provides easier setup with automatic iLO address generation for all or a few selected bays

ProLiant BL p-Class User Requirements

- Users must have the Configure iLO Settings privilege.
- A network connection to iLO must be available and functioning properly.

Configuring a ProLiant BL p-Class Blade Enclosure

To configure a BL p-Class blade enclosure using static IP bay addressing:

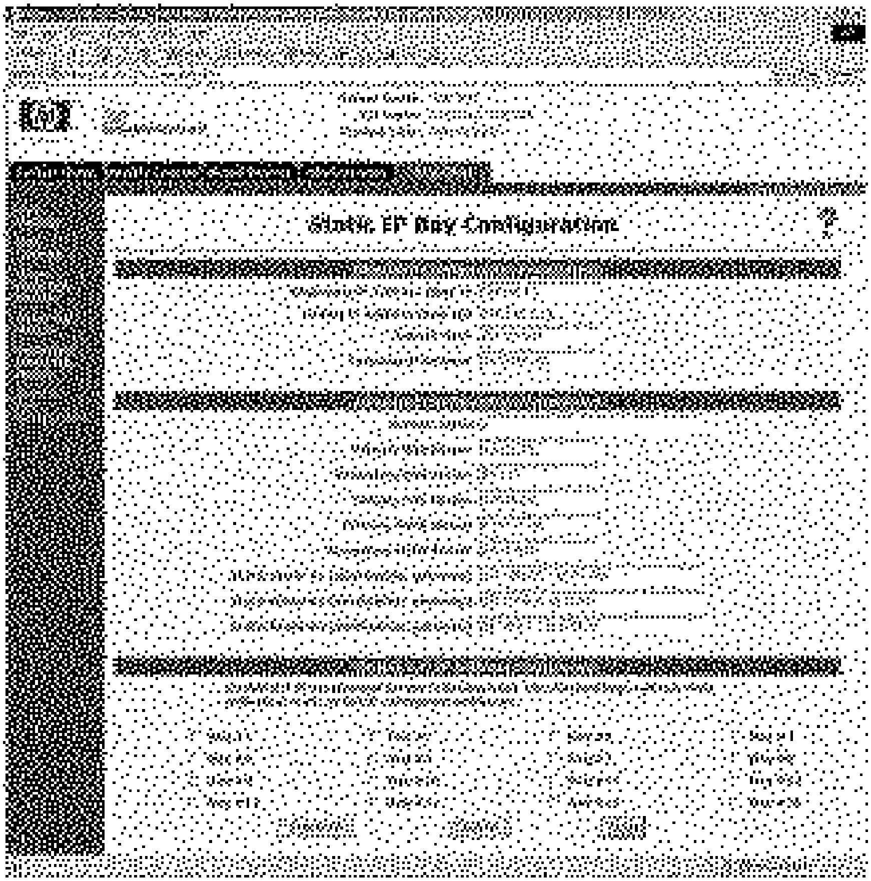
1. Install a server blade in bay 1 of the BL p-Class enclosure. The server blade does not need to be configured or have an operating system installed. The server blade must be configured before installing any additional blades in the enclosure.
2. Connect a client device to the front-panel iLO port of the blade using the local I/O cable. The local I/O cable connects to the I/O port on the front of the server blade. This connection enables the static IP 192.168.1.1 for the iLO Web interface.
3. Configure the enclosure setting. Using the iLO Web interface, select the BL p-Class tab to access the Enclosure Static IP Settings. The BL p-Class tab provides a user interface for configuring the enclosure-level static IP addresses.
4. Select a reasonable starting IP address, with the last digit(s) of the address corresponding to the bay number of each blade (example: 192.168.100.1 through 192.168.100.16), to build an easy-to-remember numbering system.
5. Reset bay #1, if necessary. The blade in bay #1 must only be reset if you intend the blade to use a Static IP bay Configuration address by marking the feature enable mask for bay #1. Before resetting the blade, browse to the Network Settings page, select **Enable Static IP Settings** and click **Apply** to force the blade to reboot and use the newly assigned enclosure static IP.

If multiple enclosures are deployed at the same time, the process can be repeated easily by moving a single blade to bay #1 of each enclosure to perform the configuration.

Configuring Static IP Bay Settings

Static IP bay settings available on the BL p-Class tab, enable you to configure and deploy the blade server.

The Enable Static IP Bay Configuration Settings checkbox, available on the Network Settings tab (not shown), allows you to enable or disable Static IP Bay Configuration. The new Enable Static IP Bay Configuration Settings option is only available on blade servers. When Static IP Bay Configuration is enabled, all fields except iLO Subsystem Name are disabled. Only Static IP Bay Configuration or DHCP can be enabled at one time. Disabling both Static IP Bay Configuration and DHCP signals iLO to use a user defined IP address. The Enable Static IP Bay Configuration Settings option remains disabled if the infrastructure does not support Static IP Bay Configuration.



ProLiant BL p-Class Standard Configuration Parameters

Beginning IP Address (Bay 1)—Assigns the starting IP address. All IP addresses must be valid addresses.

Ending IP Address (Bay 16)—Assigns the ending IP address. All IP addresses must be valid addresses.

Subnet Mask—Assigns the subnet mask for the default gateway. This field may be filled in if either Static IP Bay Configuration or DHCP is enabled. The entire IP address range must conform to the subnet mask.

Gateway IP Address—Assigns the IP address of the network router that connects the Remote Insight subnet to another subnet where the management PC resides. This field may be filled in if either Static IP Bay Configuration or DHCP is enabled.

ProLiant BL p-Class Advanced Configuration Parameters

Domain Name—Enables you to assign the name of the domain in which the iLO will participate.

Primary DNS Server—Assigns a unique DNS server IP address on your network.

Secondary DNS Server—Assigns a unique DNS server IP address on your network.

Tertiary DNS Server—Assigns a unique DNS server IP address on your network.

Primary WINS Server—Assigns a unique WINS server IP address on your network.

Secondary WINS Server—Assigns a unique WINS server IP address on your network.

Static Route #1, #2, and #3 (destination gateway)—Assigns the appropriate static route destination and gateway IP address on your network (the default IP values are 0.0.0.0 and 0.0.0.0, where the first IP address corresponds to the destination IP, and the second IP address corresponds to the gateway IP).

Enable iLO IP Address Assignment

The bay #1 through bay #16 checkboxes allow you to select which BL p-Class blade servers will be configured. You can Enable All, Clear All, or Apply your selection.

RIBCL RACK_INFO Commands

Several new XML commands have been added to the RIBCL structure to support reading and writing of Static IP Bay Configuration in scripting. The new RIBCL commands must be scripted within a RACK_INFO (on page 310) command block. The new attributes are:

- MOD_ENCLOSURE_IP_SETTINGS—Modifies the Static IP Bay Configuration settings. This command is only valid inside a RACK_INFO block. The logged-in user must have the configure iLO privilege. This attribute must appear inside the RACK_INFO command block with MODE = "write."
- BAY_ENABLEMASK—Enables the use of Static IP Bay Configuration addressing. The attribute MASK is a 16-bit number. Each bit represents a slot in the enclosure. If the bit is set, that particular slot is assigned to use the Static IP Bay Configuration settings. The LSB represents slot 1. For example, the MASK="0x0001" only allows slot 1 to use Static IP Bay Configuration. This number can be either a hexadecimal number or a decimal number. This command must appear inside the MOD_ENCLOSURE_IP_SETTINGS block.
- ENCLOSURE_IP_ENABLE—Enables or disables the use of Static IP Bay Configuration. This attribute must appear inside the MOD_NETWORK_SETTINGS command block. The possible values are "Y" or "N." It is case-insensitive. This attribute is only applicable on blade servers.

- GET_ENCLOSURE_IP_SETTINGS—Requests the respective iLO Static IP Bay Configuration settings. This attribute must appear inside the RACK_INFO command block. The RACK_INFO command block may be set to read or write.

RIBCL RACK_INFO Command Examples

Getting Static IP Bay Configuration Settings

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
   <RACK_INFO MODE="write">
      <GET_ENCLOSURE_IP_SETTINGS/>
   </RACK_INFO>
</LOGIN>
</RIBCL>
```

Modifying Static IP Bay Configuration Settings

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RACK_INFO MODE="write">
   <MOD_ENCLOSURE_IP_SETTINGS>
      <BAY_ENABLE MASK="0x3FE"/>
      <IP_ADDRESS VALUE="16.100.222.111"/>
      <SUBNET_MASK VALUE="255.255.252.0"/>
      <GATEWAY_IP_ADDRESS VALUE="16.100.222.1"/>
      <DOMAIN_NAME VALUE="sum.won.here.now"/>
      <PRIM_DNS_SERVER VALUE="16.11.1.111"/>
      <SEC_DNS_SERVER VALUE=""/>
      <TER_DNS_SERVER VALUE=""/>
      <PRIM_WINS_SERVER VALUE="16.22.2.222"/>
      <SEC_WINS_SERVER VALUE=""/>
      <STATIC_ROUTE_1 DEST="16.33.3.33"
      GATEWAY="16.100.11.11"/>
      <STATIC_ROUTE_2 DEST="" GATEWAY=""/>
      <STATIC_ROUTE_3 DEST="" GATEWAY=""/>
   </MOD_ENCLOSURE_IP_SETTINGS>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

Modify Network Settings to Enable Static IP Bay Configuration

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_NETWORK_SETTINGS>
      <ENCLOSURE_IP_ENABLE VALUE="Yes"/>
   </MOD_NETWORK_SETTINGS>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

Integration with RILOE II Accessory Boards

RILOE II is supported as an option in servers with iLO. Previous generations of the Remote Insight boards, such as the Remote Insight board/PCI and the original RILOE, are not supported in servers with iLO.

iLO firmware detects the presence of RILOE II and automatically disables iLO functionality. Additionally, if iLO firmware detects the presence of the original RILOE, and iLO displays an invalid configuration message.

To re-enable iLO functionality after a RILOE II is removed, use the Security Override Switch and iLO RBSU (on page 22). Select **Settings>Enabled** for the Enable Lights-Out Functionality (on page 340) setting.

Using iLO

In This Section

Logging in to iLO for the First Time

iLO is configured with a default user name, password, and DNS name. Default user information is located on the iLO Network Settings tag attached to the server containing the iLO management processor. Use these values to access iLO remotely from a network client using a standard Web browser.

For security reasons, HP recommends changing the default settings after logging in to iLO for the first time. Use the "iLO Parameters Table (on page 331)" to record your settings.

The default values are:

- User name—Administrator
- Password—A random, eight-character, alphanumeric string

- DNS Name—*ILOXXXXXXXXXXXX,* where the 12 *X*s represent the serial number of the server

  NOTE: User names and passwords are case sensitive.

Logging in to iLO for the First Time Using a Browser

To start the login process, you must know the iLO network address, which is either the DNS name, or the iLO IP address. You can determine the iLO IP address using iLO RBSU (on page 22).

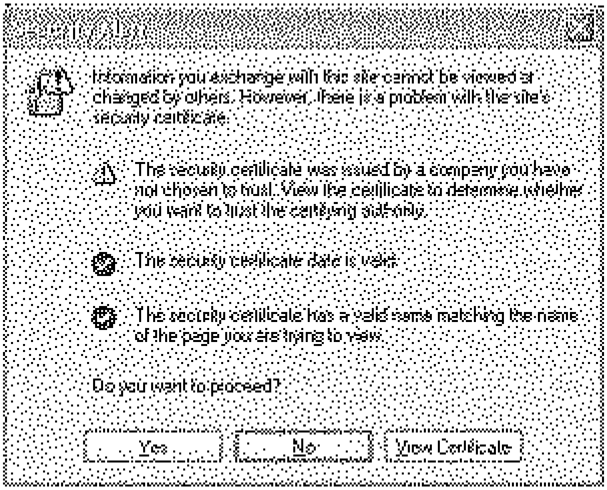
The Show iLO IP during POST configuration option, sets iLO to display the assigned IP address while the host is booting.

1. Enter the iLO IP address or DNS name using the address bar of the Web browser.

   NOTE: This procedure assumes that your network supports DNS/DHCP. If not, you must configure the IP address using the RBSU or, for ProLiant BL p-Class servers, through the iLO Diagnostic Port.

   When connecting to iLO in a browser for the first time, you will receive a security alert. This alert appears because the default SSL certificate that is dynamically generated by iLO is not known to the browser.

   Refer to "Certificates (on page 140)" to import a certificate generated by a CA.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

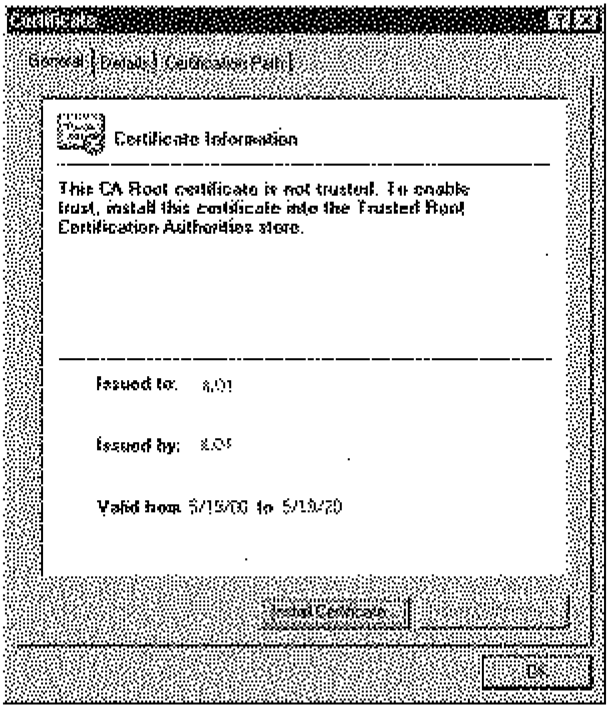
2. In the Security Alert window:

   – Click **Yes** to continue to the login screen of iLO. The alert message appears each time that you access the iLO management processor in a browser.

   – Click **No** to return to the Welcome screen of iLO.

   – Click **View Certificate** to display the certificate information. Installing the default certificate onto the browser prevents the security alert message from being displayed in the future.

   To install the certificate, proceed to step 3. If you choose not to install the certificate, proceed to step 4.



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate into the Trusted Root Certification Authorities store.

Issued to: iLO1

Issued by: iLO

Valid from 5/15/00 to 5/10/20

NOTE: If the certificate is removed from your browser, if you have upgraded the firmware, or if iLO is rebooted, the security alert message will be displayed again. Unless a certificate generated by a CA has been imported into iLO, iLO will generate a self-signed certificate each time it reboots. This self-signed certificate is not as secure as a certificate generated by a CA. (Refer to "Certificates (on page 140)" to import a certificate generated by a CA.) HP does not recommend using a self-signed certificate, because this certificate will change everytime iLO reboots. Also, some browsers do not allow easy editing of previously stored certificates and may cause problems when attempting to store a different certificate with the same name.

3. Install the default certificate to your browser:

   NOTE: Unless you have installed a certificate generated by a CA, iLO issues a self-signed certificate that lasts until iLO is reset for any reason.

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

   b. Click **Next.**

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

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

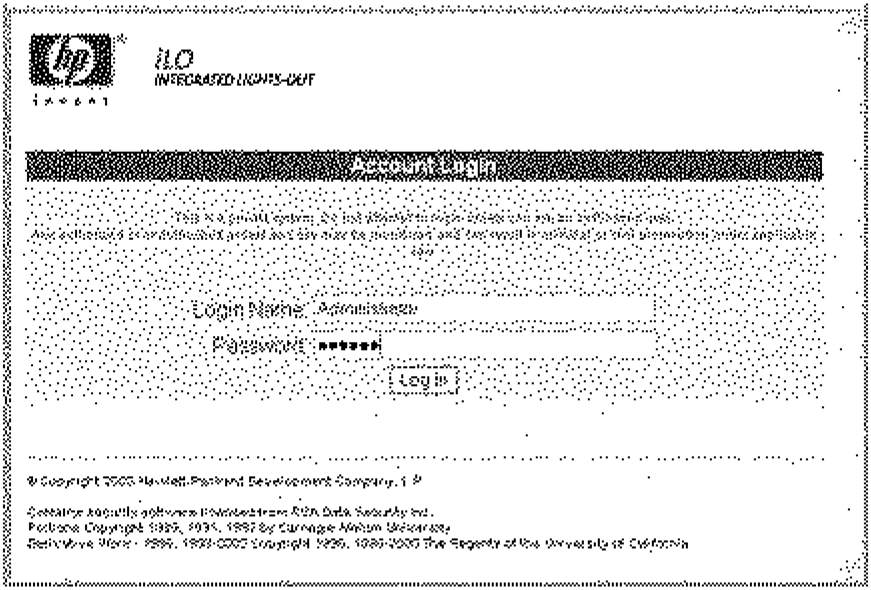
   e. Click **Yes** to confirm the installation of the default certificate when the confirmation window appears.

   f. Click **OK** to acknowledge that the certificate import was successful.

   g. Click **OK** in the Certificate window to return to the Security Alert window.

   h. Click **Yes** in the Security Alert window to log in.

4. When the browser completes the SSL connection to iLO, the Account Login screen prompts you for a user name and password. Use the default user name and password from the Network Settings tag, and click **Log In.**



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.

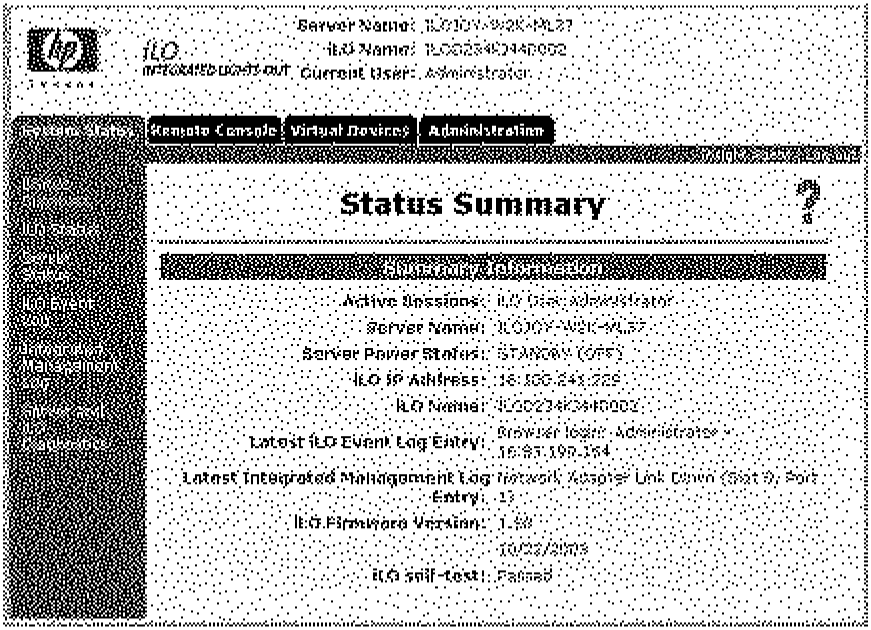
Login Name: Administrator

Password: ******

© Copyright 2003 Hewlett-Packard Development Company, L.P.

Contains security software licensed from RSA Data Security Inc.
Portions Copyright 1989, 1991, 1992 by Carnegie Mellon University
Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California

After the default user name and password have been verified, the Status Summary screen is displayed.



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

Status Summary

Summary Information

Active Sessions: iLO User: Administrator
Server Name: [illegible]
Server Power Status: STANDBY (OFF)
iLO IP Address: [illegible]
iLO Name: [illegible]
Latest iLO Event Log Entry: Browser login: Administrator - [illegible]
Latest Integrated Management Log Entry: Network Adapter Link Down (Slot [illegible], Port [illegible])
iLO Firmware Version: [illegible]
[illegible]
iLO Self-test: [illegible]

The BL p-Class tab is not illustrated in this and subsequent screen shots.

Progressive Delays for Failed Browser Login Attempts

After an initial failed log in attempt, iLO imposes a security delay. For more information on login security, refer to "Login Security (on page 138)."

Help

Assistance for all iLO options is available by means of the iLO Help option. These links provide summary information about the features of iLO and helpful information for optimizing its operation. To access page-specific help, click the **?** on the right side of the browser window.

System Status

The following options are available within the System Status tab.

Status Summary

The Status Summary screen provides general information about iLO, such as all logged in users, server name and status, iLO IP address and name, and latest log entry data. The Status Summary screen also shows whether iLO has been configured to use HP Web-Based Management and Insight Management Web agents.

iLO Status

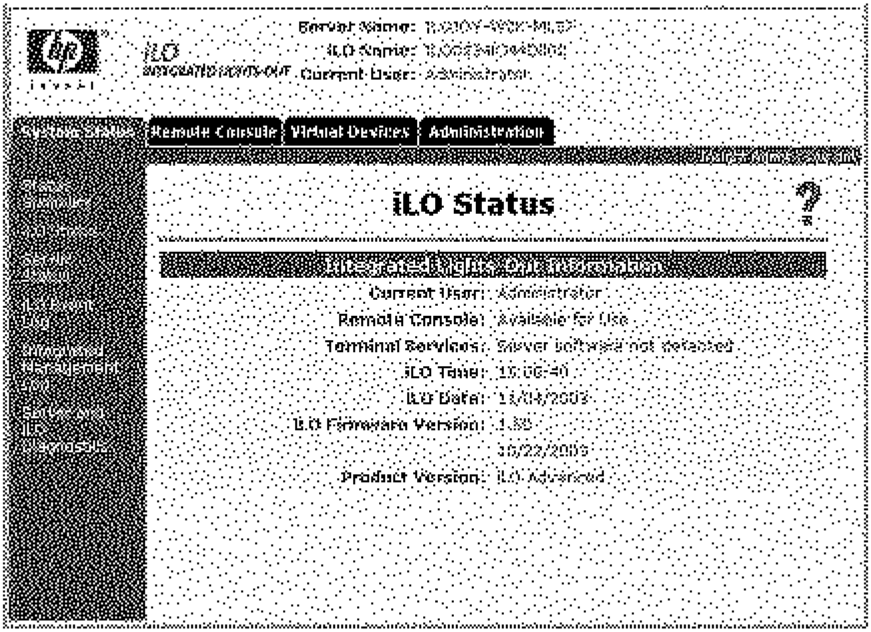
The iLO Status option provides comprehensive iLO status information, including:

- Current user
- Status and availability of the Remote Console
- Status and availability of Terminal Services pass-through
- Date and time currently in use by iLO

  NOTE: Date and time are set during POST and maintained by the MP Management Agents.

- Revision information of the iLO firmware

- Product version (iLO Standard or iLO Advanced) of iLO



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

iLO Status

Integrated Lights-Out Information

Current User: Administrator
Remote Console: Available for Use
Terminal Services: Server software not detected
iLO Time: 15:06:40
iLO Date: 11/04/2003
iLO Firmware Version: 1.50
10/22/2003
Product Version: iLO Advanced

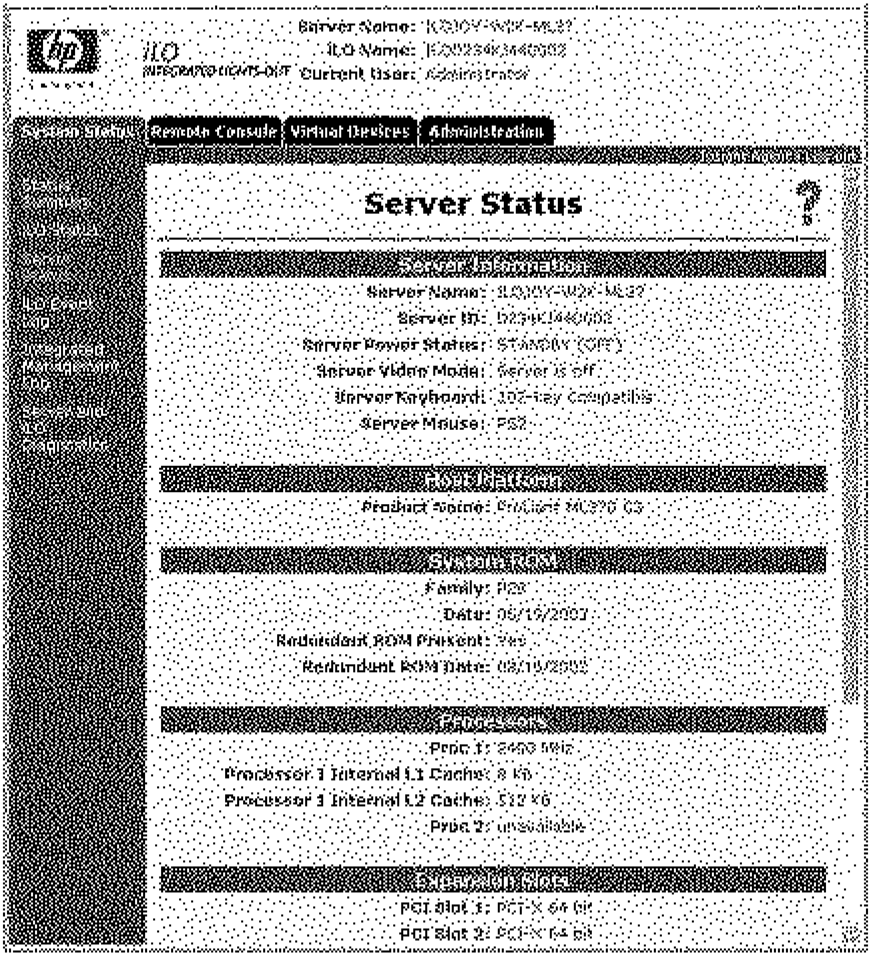
Server Status

The Server Status option provides comprehensive status information about the server, including:

- Server name associated with the iLO management processor

  The Server Name field reports host is `unnamed` if the HP Management Agents are not loaded on the host server.
- Server power status
- Server video mode
- Server keyboard and mouse type

- SMBIOS data such as host platform, system ROM, processors, embedded MAC addresses, expansion slots, and memory modules present at POST



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

Server Status

Server Information

Server Name: [illegible]
Server ID: [illegible]
Server Power Status: STANDBY (OFF)
Server Video Mode: Server is off
Server Keyboard: 102-key Compatible
Server Mouse: PS2

Host Platform

Product Name: ProLiant ML370 G3

System ROM

Family: P28
Date: 05/19/2003
Redundant ROM Present: Yes
Redundant ROM Date: [illegible]

Processors

Proc 1: 2400 MHz
Processor 1 Internal L1 Cache: 8 KB
Processor 1 Internal L2 Cache: 512 KB
Proc 2: unavailable

Expansion Slots

PCI Slot 1: PCI-X 64 bit
PCI Slot 2: PCI-X 64 bit

iLO Event Log

The iLO Event Log is a record of significant events detected by iLO. Logged events include major server events, such as a server power outage or a server reset; and iLO events, such as an unauthorized login attempt.

Other logged events include any successful or unsuccessful browser and Remote Console logins, virtual power and power cycle events, and clear event log actions. Some configuration changes, such as creating or deleting a user, are also logged.

iLO provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. When login attempts fail, iLO also generates alerts and sends them to a remote management console.

1. Click **Clear Event Log** to clear the event log of all previously logged information.
2. Click **OK** to confirm that you want to clear the event log. A line indicating that the log has been cleared is logged.

   Events logged by higher versions of iLO firmware may not be supported by lower version firmware. If an event is logged by an unsupported firmware, the event will be listed as `UNKNOWN EVENT TYPE.` You may clear the event log to eliminate these entries, or update firmware to the latest supported version to resolve this cosmetic issue.

Integrated Management Log

The IML is a record of significant events that have occurred to the host platform. The events are generated by the system ROM and by services like the System Management (Health) driver. iLO manages the IML, which can be accessed by using a supported browser, even when the server is off. This capability can be helpful when troubleshooting remote host server problems.

The IML enables you to view logged remote server events. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes. For more information, refer to the server guide.

1. Click **Clear Event Log** to clear the event log of all previously logged information.
2. Click **OK** to confirm that you want to clear the event log. A line indicating that the log has been cleared is logged.

Server and iLO Diagnostics

The Server and iLO Diagnostics option provides the following comprehensive diagnostic information:

- POST diagnostic results for the host server (on page 49)
- NVRAM environment variables listing (on page 50)
- Virtual NMI button (on page 50)
- iLO self-test results (on page 51)

NOTE: When connected through the Diagnostics Port, the directory server is not available. You can log in using a local account only.

POST Diagnostic Results for the Host Server

As an integrated management processor, iLO monitors the progress of the boot process of the server. The host server ROM writes POST codes as it is booting. iLO records and displays these codes.

The POST codes document the booting process of the ROM BIOS. A code indicates the start of a particular phase of the boot process. The POST code results can be used to determine the general phase in which the boot process stopped prematurely. Use of the POST codes alone is usually not sufficient to diagnose the actual root cause of a stopped boot process. The POST codes should be used in conjunction with other tools, such as the IML, the local or iLO Remote Console, and the Diagnostic utilities to determine the root cause of a stopped boot process.

The following list includes all of the POST codes and Diagnostic Results for the host server tracked by iLO for a routine boot sequence on ProLiant servers.

Code	Start of Phase
FE04	EISA Initialization
FE08	PCI Initialization
FE0C	Processor Initialization
FE10	Video Initialization
FE14	Cache Initialization

Code	Start of Phase
FE18	USB Initialization
FE1C	Memory Test
FE20	Memory Initialization
FE24	USB Startup
FE28	Floppy Controller Test
FE2C	Option ROM Initialization
FE30	ATAPI Option ROM Initialization
FE34	BBS Initialization
FE38	Begin BOOT Process
FE3C	Attempting SCSI CD Boot
FE40	Attempting Floppy Boot
FE44	Attempting HD Boot
FE48	Attempting CD Boot
FE4C	Attempting PXE Boot
FE50	Passing control to boot sector code
FE54	No bootable devices

NVRAM Environment Variables Listing

HP uses NVRAM to store server environment variable information, for example, host controller boot order. This information can be useful to HP engineers and advanced customers who have detailed knowledge of HP System Management architecture.

Virtual NMI Button

The Virtual NMI button halts the operating system for debugging purposes. This functionality is an advanced feature that should only be used for kernel-level debugging. The possible uses of this feature include:

- Demonstrate ASR

If the system management (Health) driver is loaded, and ASR is enabled, then the host automatically reboots after an NMI has occurred.

- Debug

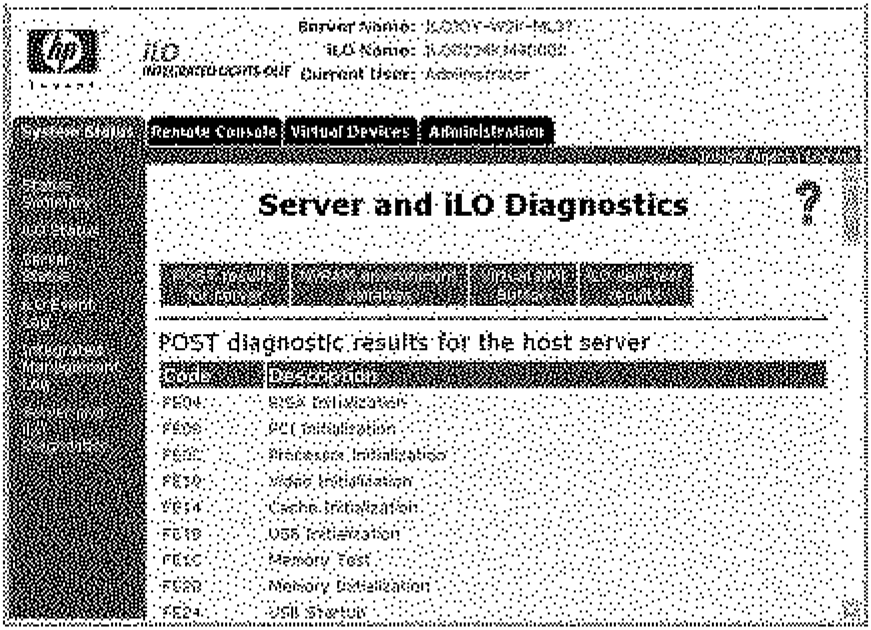
  If a software application hangs the system, the NMI capability can be used to engage the operating system debugger.

- Initiate dump of an unresponsive host

  A vendor might be interested in capturing the server context.

iLO Self-Test Results

The results of the iLO Self-Test are displayed on the Server and iLO Diagnostics screen. All tested subsystems should display Passed under normal situations.



Server and iLO Diagnostics

POST diagnostic results for the host server

Code	Description
FE04	EISA Initialization
FE08	PCI Initialization
FE0C	Processors Initialization
FE10	Video Initialization
FE14	Cache Initialization
FE18	USB Initialization
FE1C	Memory Test
FE20	Memory Initialization
FE24	USB Startup

Remote Console

The Remote Console tab provides access to different views of the Remote Console and enables you to define keystroke sequences that will be transmitted to the remote host server at the press of a hot key. Standard iLO provides embedded hardware Remote Console capabilities on a text mode screen. The operating system-independent console supports text modes that display remote host server activities, such as shutdown and startup operations.

The Graphical Remote Console is enabled by licensing the optional iLO Advanced Pack. Graphical Remote Console turns a supported browser into a virtual desktop, giving the user full control over the display, keyboard, and mouse of the host server. The operating system-independent console supports graphic modes that display remote host server activities, such as shutdown and startup operations.

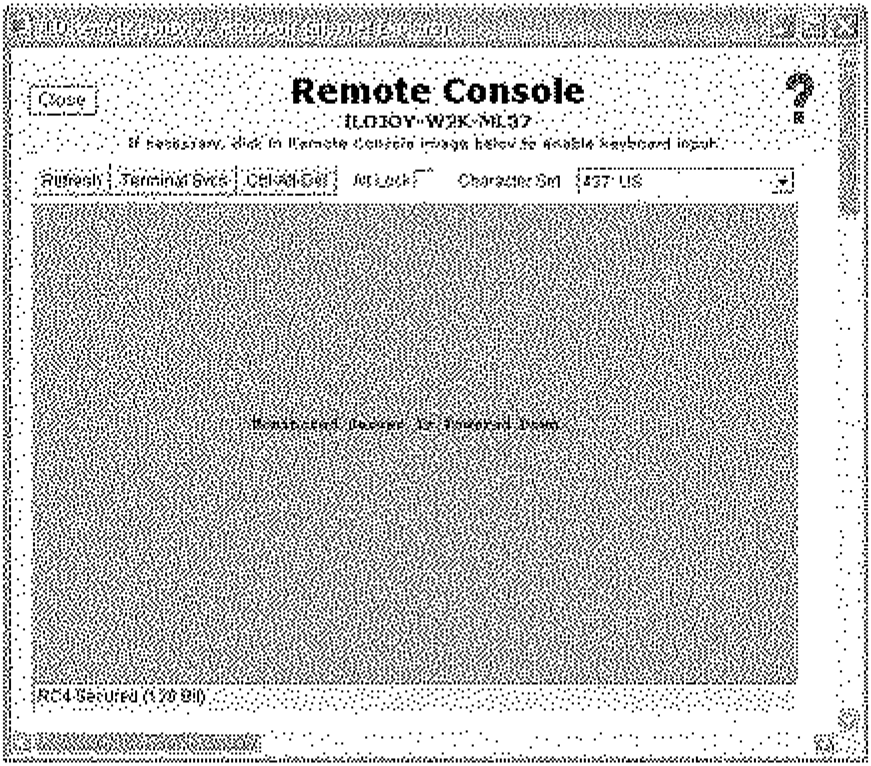
Remote Console Option

The Remote Console option redirects the host server console to the network client browser, providing full text (standard) and graphical mode video, keyboard, and mouse access to the remote host server (if licensed with the iLO Advanced Pack).

With the Remote Console, you have complete control over a remote host server as if you were in front of it. You can access the remote file system and the network drives. The Remote Console enables you to change hardware and software settings of the remote host server, install applications and drivers, change remote server screen resolution, and gracefully shut down the remote system.

With the Remote Console, you can observe POST boot messages as the remote host server restarts and initiate ROM-based setup routines to configure the hardware of the remote host server. When installing operating systems remotely, the graphical Remote Console (if licensed) enables you to view and control the host server screen throughout the installation process.

For best performance, be sure to configure the host operating system display as described in "Optimizing Performance for Graphical Remote Console (on page 54)."



If necessary, click in Remote Console image below to enable keyboard input.

Remote Console Information Option

The Remote Console Information option displays information concerning the Remote Console options available, as well as a link to download an updated Java™ Runtime Environment, which is necessary for using Remote Console with the single cursor option ("Remote Console (Single-Cursor)" on page 59).

Although up to 10 users are allowed to simultaneously log in to iLO, only one user at a time can access the Remote Console. If you attempt to open the Remote Console while it is already in use, a warning message is displayed indicating that it is in use by another user.

Remote Console will not be available if the remote console port configuration on the Global Settings tab is set to disabled.

Enhanced Features of the Remote Console

The Remote Console applet contains five buttons that provide iLO with enhanced features. These options have the following functions:

- **Refresh**—Forces iLO to repaint the screen.
- **Terminal Svcs**—Launches the Microsoft® Terminal Services client installed on this system. This button is grayed out if Terminal Services is disabled or is not installed on the server.
- **Ctrl-Alt-Del**—Enters the key sequence **Ctrl+Alt+Del** into the Remote Console.
- **Alt Lock**—When selected, any key pressed is sent to the server as if you pressed the Alt key and another key simultaneously.
- **Character Set**—Changes the default character set used by the Remote Console. Modifying the Remote Console character set ensures the correct display of characters.
- **Close**—Closes the Remote Console window and ends the Remote Console session.

Optimizing Performance for Graphical Remote Console

HP recommends the following client and server settings based on the operating system used.

Recommended Client Settings

Ideally, the remote server operating system display resolution should be the same resolution, or smaller, than that of the browser computer. Higher server resolutions transmit more information, slowing the overall performance.

Use the following client and browser settings to optimize performance:

- **Display Properties**

  - Select an option greater than 256 colors.
  - Select a greater screen resolution than the screen resolution of the remote server.
  - Linux X Display Properties—On the X Preferences screen, set the font size to **12.**

- **Remote Console**
  - For Remote Console speed, HP recommends using a 700-MHz or faster client with 128 MB or more of memory.
  - For the Remote Console Java™ applet execution, HP recommends using a single processor client.
- **Mouse Properties**
  - Set the Mouse Pointer speed to the middle setting.
  - Set the Mouse Pointer Acceleration to low or disable the pointer acceleration.

Remote Console Linux Settings

When using the iLO Remote Console to display text screens in Linux, border characters or other line drawing characters might not display correctly.

To properly configure the Remote Console text mode character set:

1. Click the **Character Set** dropdown menu from the Remote Console applet.
2. Select the **Lat1–16** character set.

Recommended Server Settings

The following is a list of recommended server settings based on the operating system used.

> **NOTE:** To display the entire host server screen on the client Remote Console applet, set the server display resolution less than or equal to that of the client.

Microsoft® Windows NT® 4.0 and Windows® 2000 Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - Plain Background (no wallpaper pattern)
  - Display resolution of 800 x 600 or 1024 x 768 pixels
  - 256-color or 24-bit color mode
- Server **Mouse Properties**
  - Select **None** for mouse pointer Scheme.
  - Deselect **Enable Pointer Shadow.**
  - Select **Motion** or **Pointer Options** and set the pointer Speed slider to the middle position.
  - Set pointer Acceleration to **None.**

Microsoft® Windows® Server 2003 Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - Plain Background (no wallpaper pattern)
  - Display resolution of 800 x 600 or 1024 x 768 pixels
  - 256-color or 24-bit color mode
- Server **Mouse Properties**
  - Select **None** for mouse pointer Scheme.
  - Select **Disable Pointer Trails.**
  - Deselect **Enable Pointer Shadow.**
  - Select **Motion** or **Pointer Options,** and set the pointer Speed slider to the middle position.
  - Deselect **Enhanced pointer precision.**

To automate the setting of the optimal mouse configuration, download the Lights-Out Optimization utility from the HP website (http://www.hp.com/servers/lights-out). Click the **Best Practices** graphic, then click the **Maximize Performance** links.

Red Hat Linux and SuSE Linux Server Settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - 1024 x 768 pixels or lower screen resolution
  - 256 colors
- Server **Mouse Properties**
  - Set Pointer Acceleration to **1x.** For KDE, access the **Control Center,** select **Peripherals/Mouse,** then select the **Advanced** tab.
- X Display Properties
  - On the X Preferences screen, set the font size to **12.**

Novell NetWare Settings

Use the following settings to optimize performance:

Server **Display Properties**

- 800 x 600 pixels or lower screen resolution
- 256 colors

Remote Console Hot Keys

The Remote Console hot keys feature enables you to define up to six multiple key combinations to be assigned to each hot key. When a hot key is pressed in the Remote Console, on client systems, the defined key combination (all keys pressed at the same time) will be transmitted in place of the hot key to the remote host server.

The Remote Console hot keys are active during a remote console session through the Remote Console applet and during a text remote console session through a telnet client.

To define a Remote Console hot key:

1. Click **Remote Console Hot Keys** in the Remote Console tab.
2. Select the hot key you want to define and use the dropdown boxes to select the key sequence to be transmitted to the host server at the press of the hot key.
3. Click **Save Hot Keys** when you have finished defining the key sequences.

The Remote Console Hot Keys screen also contains a Reset Hot Keys option. This option clears all entries in the hot key fields. Click **Save Hot Keys** to save the cleared fields.

Supported Hot Keys

The Program Remote Console Hot Keys page allows you to define up to 6 different sets of hot keys for use during a Remote Console session. Each hot key represents a combination of up to 5 different keys which are sent to the host machine whenever the hot key is pressed during a Remote Console session. The selected key combination (all keys pressed at the same time) are transmitted in its place. For more information, refer to "Remote Console Hot Keys (on page 57)." The following table lists keys available to combine in a Remote Console hot key sequence.

ESC	F12	:	o
L_ALT	" " (Space)	<	p
R_ALT	!	>	q
L_SHIFT	#	=	r
R_SHIFT	$	?	s
INS	%	@	t
DEL	&	[	u
HOME	~	]	v
END	(	\	w

PG UP	)	^	x
PG DN	*	_	y
ENTER	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	’
F4	2	g	L_CTRL
F5	3	h	R_CTRL
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	SCRL LCK
F9	7	l	BACKSPACE
F10	8	m	SYS RQ
F11	9	n	

Single- and Dual-Cursor Modes for Graphical Remote Console

The Graphical Remote Console can use either a single- or dual-cursor mode. A supported JVM might be required for support.

Remote Console (Single-Cursor)

Single-cursor means the local cursor is not displayed when the mouse cursor is over the Remote Console screen. Synchronization of two cursors is eliminated, making navigation easier in the Remote Console window.

On the client, download and install Java™ 1.3.1 JVM or later for Microsoft® Internet Explorer or Java™ 1.4.2 Runtime Environment, Standard Edition for Linux browsers. The remote server does not require any other software to obtain a single mouse pointer.

Links to download the required JVMs are available on the Remote Console Information screen.

You will be redirected from the main site to the http://java.sun.com (http://java.sun.com) site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Microsoft® Internet Explorer either from the java.sun site or on the SmartStart CD.

Remote Console (Dual-Cursor)

All the features discussed in the "Remote Console (on page 52)" section are available when using dual-cursor. When selecting this option, two cursors are on the screen: the main cursor and a secondary cursor within the dual cursor frame. When passing the main cursor across the Remote Console frame, the secondary cursor will track to the main cursor.

The mouse cursor of the client computer appears within the Remote Console as a cross-hair symbol. Some iLO users prefer to see exactly where the client computer mouse cursor is located. For best performance, be sure to configure the host operating system display as described in "Optimizing Performance for Graphical Remote Console (on page 54)."

The dual-cursor option is your only Remote Console option if you choose not to download an updated Java™ Runtime Environment. The dual-cursor option is supported with Java™ 1.1 VM and later. To synchronize the remote and local cursors if they drift apart:

1. Right-click, drag, and move the local crosshair cursor to align with the mouse cursor of the remote server.
2. Press and hold the **Ctrl** key and move the local crosshair cursor to align with the mouse cursor of the remote server.

You might prefer the dual-cursor option because you can see where the cursor exits the Remote Console applet window. HP recommends using the Remote Console dual-cursor mode with text-based operating systems.

When operating in dual-cursor mode, the local cursor assumes the shape of the remote cursor. The cursor appears as a single cursor if the local cursor and the remote cursor are perfectly aligned and the hardware acceleration is set to Full on the managed server.

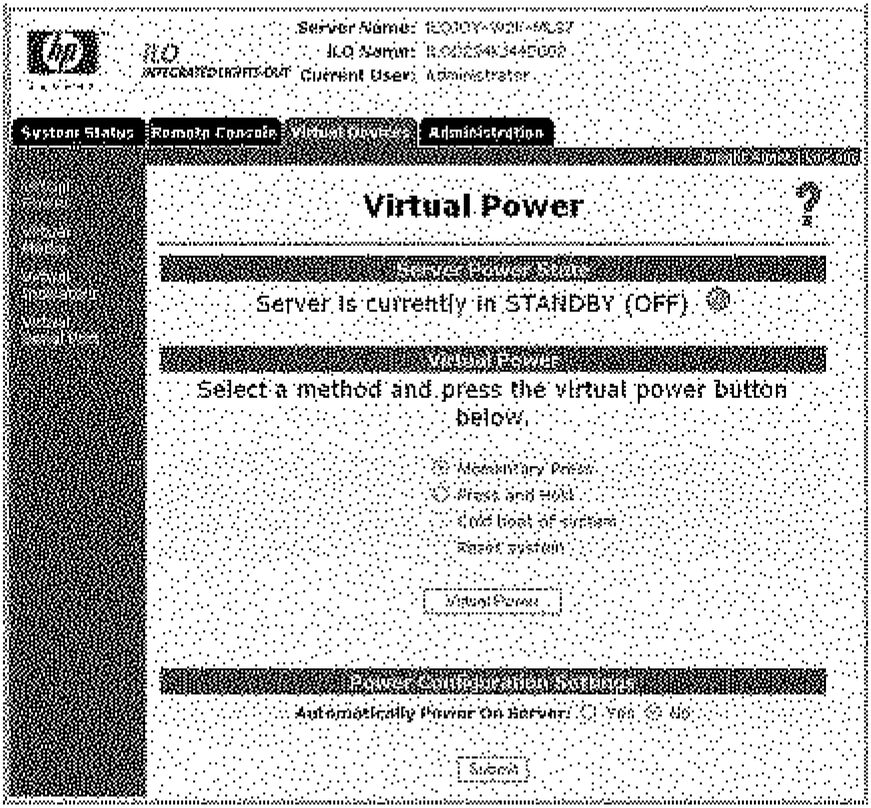
Virtual Devices

Within the Virtual Devices tab are:

- Virtual Power (on page 62)
- Virtual Media (on page 64)
- Virtual Indicators (on page 83)
- Virtual Serial Port (on page 84)

Virtual Power

The Virtual Power button enables control of the power state of the remote server and simulates pressing the physical power button on the server. If the remote host server is not responding, this feature enables an administrator to initiate a cold or warm reboot to bring the server back online.



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

Virtual Power

Server Power Status

Server is currently in STANDBY (OFF)

Virtual Power

Select a method and press the virtual power button below.

● Momentary Press
○ Press and Hold
Cold boot of system
Reset system

Power Configuration Settings

Automatically Power On Server: ○ Yes ● No

Some of these features will not gracefully shut down the operating system. An operating system shutdown should be initiated using the Remote Console before using the Virtual Power button.

Use the refresh feature of the browser to keep the status of the power indicator up to date.

To use the Virtual Power button, select the power option that you want and click **Virtual Power** to initiate the power option.

The available power options are:

- **Momentary Press**—This option simulates a momentary press of the power button. A momentary press is usually sufficient to turn off a server that is currently on or to turn on a server that is currently off. Depending on the host operating system, this option can gracefully shut down the operating system. To use this option, select **Momentary Press** and click **Virtual Power.**
- **Press and Hold**—This option presses and holds the power button for six seconds, which is useful in forcing the system to power off if the operating system is not responding to the momentary press.

  This feature will not gracefully shut down the operating system.
- **Cold Boot of system**—This option turns the server off, then back on. To reboot the system, select **Cold Boot of system** and then click **Virtual Power.** This will immediately remove power from the system. The system will restart after approximately six seconds. This option is not displayed when the server is off.
- **Warm Boot of system**—This option causes the server to reset, without turning it off. To use this option, select **Warm Boot of system** and click **Virtual Power.** This option is not displayed when the server is off.

  This feature will not gracefully shut down the operating system.
- **Automatically Power On Server**—This option automatically turns the server on when AC power is restored if Yes is selected. AC power is applied when a UPS is activated after a power outage. The server automatically powers on and begins the normal server booting process.
- **Manual Override for BL p-Class**—This option is displayed only when you are connected to a ProLiant BL p-Class server. This option enables you to forcibly power on a server, even if the rack reports insufficient power. An improperly configured rack or rack communication problem can cause a server to not power on when sufficient power is available. This option should only be used if you are certain your rack has sufficient power capacity.

CAUTION: It is possible using the **Manual Override for BL p-Class** option to power on servers that exceed the power available from the power supplies. Exceeding the available power can cause loss of all servers in the rack, server failures, and loss or corruption of data. HP recommends correcting configuration or communication problems to ensure reliable operation.

Virtual Media

Virtual Media is enabled by licensing the optional iLO Advanced Pack. If not licensed, the message `iLO feature not licensed` is displayed.

The iLO Virtual Media option provides the administrator with a Virtual Floppy disk drive and a Virtual CD drive which can direct a remote host server to boot and use standard media from anywhere on the network. Virtual Media devices are available when the host system is booting. The iLO Virtual Media devices connect to the host server using USB technology. Using USB also enables new capabilities for the iLO Virtual Media devices when connected to USB-supported operating systems. Different operating systems provide varying levels of USB support. The iLO Virtual Media is configurable to address these varying levels of support ("Operating System USB Support" on page 65).

- If the Virtual Floppy capability is enabled, the floppy drive normally cannot be accessed from the client operating system.
- If the Virtual CD-ROM capability is enabled, the CD-ROM drive cannot be accessed from the client operating system.

Under certain conditions, it is possible to access the Virtual Floppy drive from the client operating system while it is connected. However, it is important that access to the Virtual Floppy from the client operating system not be attempted while it is connected as a virtual media device. Doing so could cause data loss on the floppy drive. Always disconnect Virtual Media before trying to access it from the client operating system.

Operating System USB Support

Different operating systems provide varying levels of USB support. iLO uses the built-in USB drivers of the operating system. The level of USB support in the operating system affects the level of support for iLO Virtual Media. In general, any operating system issues that affect a physical USB floppy drive or a physical USB CD-ROM drive will also impact iLO Virtual Media.

The HP server ROM provides support at server boot time for Virtual Media. The Virtual Floppy will be available at boot time regardless of the server operating system.

The following server operating systems do not support USB media and, therefore, do not have access to Virtual Media during operating system run time:

- MS-DOS®
- Microsoft® Windows NT® 4.0
- Linux Red Hat (before 7.2)
- SuSE Linux (before 7.0)
- Novell NetWare 5.x and 6

Certain Linux operating systems do not correctly support USB Virtual Media drives at operating system install time. The iLO Virtual Media should not be used during the installation of the SuSE Linux Enterprise Server 7.

Windows® 95 OSR 1 does not support any USB devices. Therefore, SmartStart 5.x CDs cannot be used with the iLO Virtual Media.

The following table lists operating system USB capabilities and the corresponding iLO Virtual Media capabilities.

	Pre-operating system server boot using Virtual USB floppy	Pre-operating system server boot using Virtual USB CD	Operating system install using Virtual USB floppy[1]	Operating system install using Virtual USB CD	Operatin g system run time using Virtual USB floppy[2]	Operating system run time using Virtual USB CD[2]
NetWare 5.x or 6	Yes	Yes	No	No	No	No
NetWare 6.5	Yes	Yes	Yes	No	Yes	Yes
SUSE Linux Enterprise Server 7	Yes	Yes	No	Yes	Yes	Yes
UnitedLinux 1.0	Yes	Yes	Yes[3]	Yes	Yes	Yes
Red Hat Linux 7.2	Yes	Yes	Yes	Yes	Yes	Yes
Red Hat Linux 7.3	Yes	Yes	Yes	Yes	Yes	Yes
Red Hat Linux 8.0	Yes	Yes	Yes	Yes	Yes	Yes
Red Hat Enterprise Linux AS 2.1	Yes	Yes	Yes[3]	Yes	Yes	Yes
Red Hat Enterprise Linux 3	Yes	Yes	Yes	Yes[4]	Yes	Yes
Windows® NT 4.0	Yes	Yes	No	No	No	No
Windows® 2000 SP3 or later	Yes	Yes	Yes	No	Yes[5]	Yes
Windows® Server 2003	Yes	Yes	Yes	Yes	Yes	Yes

[1] **NOTE:** The typical use of the Virtual USB floppy is to assist for a network based installation of the Network Operating System.

[2] **NOTE:** Any additional software packages that must be installed can be accomplished using this method.

[3] **NOTE:** You must manually load the USB driver.

[4] **NOTE:** Not available on a BL20p G1.

[5] **NOTE:** Only with an integrated operating system CD.

Using iLO Virtual Media Devices

To use iLO Virtual Media devices, select **Virtual Media** on the Virtual Devices tab. An applet loads in support of the Virtual Floppy or Virtual CD-ROM device.

iLO Virtual Floppy

The iLO Virtual Floppy disk is available at server boot time for all operating systems. Booting from the iLO Virtual Floppy enables you to upgrade the host system ROM, deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

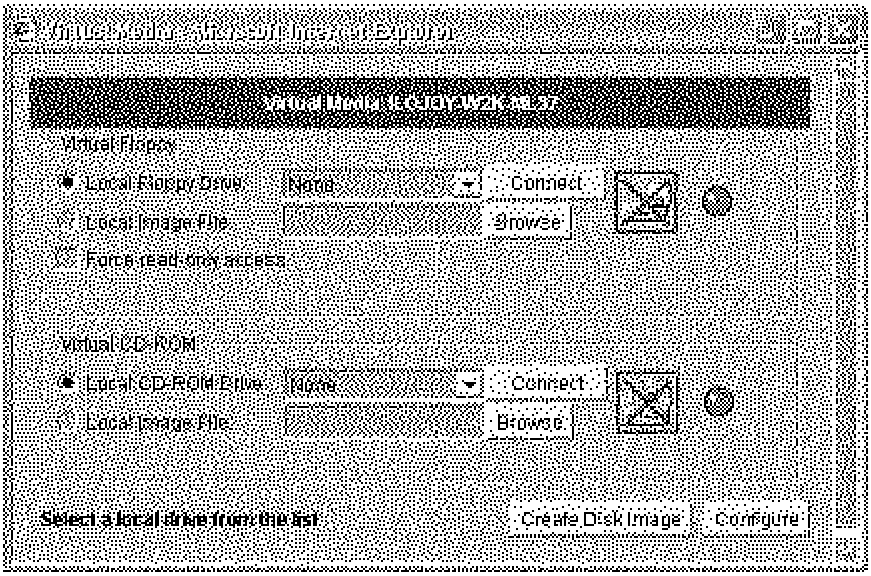
If the host server operating system supports USB mass storage devices, then the iLO Virtual Floppy is also available after the host server operating system loads. You can use the iLO Virtual Floppy when the host server operating system is running to upgrade device drivers, create an emergency repair diskette, and perform other tasks. Having the Virtual Floppy available when the server is running can be especially useful if the administrator must diagnose and repair a problem with the NIC driver.

The Virtual Floppy can be the physical floppy drive on which you are running the Web browser, or an image file stored on your local hard drive or network drive. For maximum performance, HP recommends the use of local image files stored either on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

To use a physical floppy drive in your client PC:

1. Select **Local Floppy Drive.**
2. Select the drive letter of the desired physical floppy drive on your client PC from the dropdown menu.

3. Click **Connect.**



Virtual Media - Microsoft Internet Explorer

Virtual Floppy

● Local Floppy Drive: None

○ Local Image File

□ Force read-only access

Virtual CD-ROM

● Local CD-ROM Drive: None

○ Local Image File

Select a local drive from the list

To use an image file:

1. Select **Local Image File** within the Virtual Floppy section of the Virtual Media applet.
2. Enter the name of the diskette image in the text box. You can also click **Browse** to locate image files.
3. Click **Connect.**

When connected, the virtual devices are available to the host server until you close the Virtual Media applet. When you are finished using the Virtual Floppy, you can either select to disconnect the device from the host server or close the applet.

> **NOTE:** The Virtual Media applet must remain open in your browser as long as you continue to use a Virtual Media Device.

The iLO Virtual Media floppy are available to the host server at run time if the operating system on the host server supports USB floppy drives. Refer to "Operating System USB Support (on page 65)" for information on which operating systems support USB mass storage at the time of the publication of this manual.

The iLO Virtual Floppy appears to your operating system just like any other floppy. When using iLO for the first time, the host operating system may prompt you to complete a New Hardware Found wizard.

When you are finished using iLO virtual media and disconnect it, you might receive a warning message from the host operating system regarding unsafe removal of a device. This warning can be avoided by using the operating system-provided feature to stop the device before disconnecting it from the Virtual Media.

Virtual Media Floppy Operating Systems Notes

- MS-DOS®

  During boot and during an MS-DOS® session, the Virtual Floppy device displays as a standard BIOS floppy drive. This device will display as `A:`. An existing physically attached floppy drive is obscured and unavailable during this time. You cannot use a physical local floppy drive and the Virtual Floppy simultaneously.

- Windows® 2000, Windows® XP, and Windows® Server 2003

  The Virtual Floppy displays automatically after Microsoft® Windows® has recognized the mounting of the USB device. Use it as you would a locally attached floppy device.

- NetWare 5.x or 6

  USB virtual media devices are not currently supported on the NetWare5.x or 6 operating systems.

- NetWare 6.5

  NetWare 6.5 supports the use of USB Virtual Floppy. Refer to "Mounting USB Virtual Floppy in NetWare 6.5 (on page 69)" for step-by-step instructions.

- Red Hat and SLES Linux

  Linux supports the use of USB Virtual Floppy. Refer to "Mounting USB Virtual Media Floppy in Linux (on page 70)" for step-by-step instructions.

Mounting USB Virtual Floppy in NetWare 6.5

1. Access iLO through a browser.

2. Select **Virtual Media** in the Virtual Devices tab.
3. Insert the media into the local floppy drive, select a diskette drive, and click **Connect.** Alternatively, select a diskette image to be used and click **Connect.**

In NetWare 6.5, use the `lfvmount` command on the server console to assign the device a drive letter.

The NetWare 6.5 operating system will pick the first available drive letter for the Virtual Floppy drive. The `volumes` command can now be used by the server console to show the mount status of this new drive.

When the drive letter shows as mounted, the drive will now be accessible through the server's GUI as well as the system console.

When the Virtual Floppy Drive is mounted, if the media is changed in the local floppy drive, the `lfvmount` command must be re-issued on the server console to see the new media in the NetWare 6.5 operating system.

Mounting USB Virtual Media Floppy in Linux

1. Access iLO through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Select a diskette drive or diskette image and click **Connect.**
4. Load the USB drivers, using the following commands:

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Load the SCSI disk driver, using the following command:

```
modprobe sd_mod
```

6. Mount the floppy drive, using the following command:

```
mount /dev/sda  /mnt/floppy -t vfat
```

NOTE: Use the `man mount` command for additional file system types.

The floppy device can be used as a Linux file system, if formatted as such, with the `mount` command. However, 1.44-Mb diskettes are usually accessed utilizing the mtools utilities distributed with both Red Hat and SLES. The default mtools configuration does not recognize a USB-connected floppy. To enable the various m commands to access the Virtual Floppy device, modify the existing /etc/mtools.conf file and add the following line:

```
drive v: file="/dev/sda" exclusive
```

This modification enables the mtools suite to access the Virtual Floppy as v. For example:

```
mcopy /tmp/XXX.dat v:

mdir v:

mcopy v:foo.dat /tmp/XXX
```

Creating an iLO Virtual Floppy Image

The iLO Virtual Media feature enables you to create floppy image files within the same applet. You can create image files from diskettes and create diskettes from existing image files. The performance of iLO Virtual Floppy is faster when image files are used.

To create a Virtual Media image file:

1. Click **Create Disk Image.**
2. Select the drive letter and the image file name. You can use the Browse feature to find and select an existing image file or to change the directory in which the image file will be created.
3. Click **Create.** The Virtual Media applet begins the process of creating the image file. The process is complete when the progress bar reaches 100 percent.

Disk >> Image changes to Image >> Disk when clicked. Use this button to switch from creating image files from physical diskettes to creating physical floppy diskettes from image files.

Changing Diskettes

When using the iLO virtual floppy drive, and the physical floppy drive on the client machine is a USB floppy drive, disk change operations will not be recognized. For example, in this configuration, if a directory listing is obtained from a floppy diskette and the diskette is changed, a subsequent directory listing will show the listing for the first diskette. If disk changes are necessary when using iLO virtual floppy, make sure the client machine contains a non-USB floppy drive.

iLO Virtual CD-ROM

The iLO Virtual CD-ROM is available at server boot time for operating systems specified in the "Operating System USB Support (on page 65)" section. Booting from the iLO Virtual CD-ROM enables you to deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

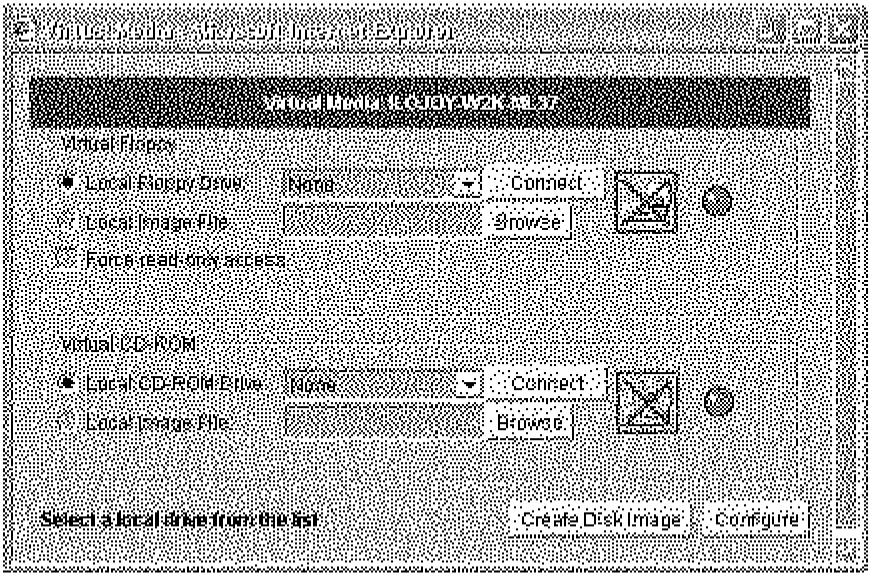
If the host server operating system supports USB mass storage devices, then the iLO Virtual CD-ROM is also available after the host server operating system loads. You can use the iLO Virtual CD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks. Having the Virtual CD-ROM available when the server is running can be especially useful if the administrator must diagnose and repair a problem with the NIC driver.

The Virtual CD-ROM can be the physical CD-ROM drive on which you are running the Web browser, or an image file stored on your local hard drive or network drive. For maximum performance, HP recommends the use of local image files stored either on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

To use a physical CD-ROM drive in your client PC:

1. Select **Local CD-ROM Drive.**
2. Select the drive letter of the desired physical CD-ROM drive on your client PC from the dropdown menu.

3. Click **Connect.**



Virtual Floppy

● Local Floppy Drive None

○ Local Image File

☐ Force read-only access

Virtual CD-ROM

● Local CD-ROM Drive None

○ Local Image File

Select a local drive from the list

Using an Image File

1. Select **Local Image File** within the Virtual CD-ROM section of the Virtual Media applet.
2. Enter the name of the CD-ROM image in the text box. You can also click **Browse** to locate image files.
3. Click **Connect.**

When connected, virtual devices are available to the host server until you close the Virtual Media applet. When you are finished using the Virtual CD-ROM, you can choose to disconnect the device from the host server or close the applet. The Virtual Media applet must remain open when using a Virtual Media Device.

iLO Virtual Media CD-ROM will be available to the host server at run time if the operating system on the host server supports USB floppy drives. Refer to "Operating System USB Support (on page 65)" for information on which operating systems support USB mass storage at the time of the publication of this manual.

iLO Virtual Media CD-ROM appears to your operating system just like any other CD-ROM. When using iLO for the first time, the host operating system may prompt you to complete a New Hardware Found wizard.

When you are finished using iLO virtual media and disconnect it, you might receive a warning message from the host operating system regarding unsafe removal of a device. This warning can be avoided by using the operating system-provided feature to stop the device before disconnecting it from the Virtual Media.

Virtual Media CD-ROM Operating System Notes

- MS-DOS®

  The virtual CD-ROM is not supported in MS-DOS®.

- Windows® 2000, Windows® XP, and Windows® Server 2003

  The virtual CD-ROM displays automatically after Windows® has recognized the mounting of the USB device. Use it as you would a locally attached CD-ROM device.

  On Windows® 2000 SP3 or later, My Computer on the host server displays an additional CD-ROM drive when the Virtual Media applet is connected. If the server operating system is up and running and you attempt to disconnect and reconnect within the Virtual Media applet, it can fail. The icon will turn green, but the additional CD-ROM drive will not display in My Computer.

  To resolve this problem, reboot the host server, and, after the operating system is available, the Virtual Media CD-ROM is ready for use. This problem only occurs on servers with no physical CD-ROM drive.

- NetWare 5.x or 6

  USB virtual media devices are not currently supported by this firmware release and the NetWare operating system.

- NetWare 6.5

  NetWare 6.5 supports the use of USB Virtual CD-ROM. Refer to "Mounting USB Virtual Media CD in NetWare 6.5 (on page 75)" for step-by-step instructions.

- Linux

  – Red Hat Linux

On servers with a locally attached IDE CD-ROM, the virtual CD-ROM device is accessible at /dev/cdrom1. However, on servers without a locally attached CD-ROM, such as the BL-class blade systems, the virtual CD-ROM is the first CD-ROM accessible at /dev/cdrom.

The virtual CD-ROM can be mounted as a normal CD-ROM device using:

```
mount /mnt/cdrom1
```

– SuSE Linux Enterprise Server 7

The SLES 7 operating system places USB-connected CD-ROMs in a different location, so the virtual CD-ROM can be found at /dev/scd0, unless there is already a USB-connected local CD-ROM, in which case it would be /dev/scd1.

The virtual CD-ROM can be mounted as a normal CD-ROM device using:

```
mount /dev/scd0 /mnt/cdrom
```

– UnitedLinux 1.0

The UnitedLinux 1.0 operating system might not properly support USB-connected CD-ROM devices. To ensure proper handling of the virtual CD-ROM, you must boot the operating system with the acpi=oldboot parameter.

The UnitedLinux 1.0 operating system places USB-connected CD-ROMs in a different location, so the virtual CD-ROM can be found at /dev/scd0, unless there is already a USB-connected local CD-ROM, in which case it would be /dev/scd1.

The virtual CD-ROM can be mounted as a normal CD-ROM device using:

```
mount /dev/scd0 /mnt/cdrom
```

Refer to "Mounting USB Virtual Media CD in Linux ("Mounting USB Virtual Media CD-ROM in Linux" on page 76)" for step-by-step instructions.

Mounting USB Virtual Media CD in NetWare 6.5

1. Access iLO through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.

3. Insert the media into the client's CD-ROM drive, select a drive, and click **Connect.**
4. The NetWare 6.5 operating system will automatically detect the new Virtual CD-ROM drive, mount it as an NSS volume, and display it as the media's volume label name. A volume label name will only appear in the NetWare 6.5 operating system if media is present in the Virtual Media CD-ROM drive. To show the mount status of the new drive, use the `volumes` command through the server console.

   The virtual CD-ROM can also be mounted as a normal CD-ROM device using the `LOAD CDDVD` command.

When the drive letter shows as mounted, the drive will be accessible through the server's GUI and the system console.

Mounting USB Virtual Media CD-ROM in Linux

1. Access iLO through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Select a CD-ROM to be used and click **Connect.**
4. Load the USB drivers using the following commands:

   ```
   modprobe usbcore
   modprobe usb-storage
   modprobe usb-ohci
   ```

5. Load the SCSI CD-ROM disk driver using the following command:

   ```
   modprobe sr_mod
   ```

6. Mount the drive using the following command:

   ```
   mount /dev/scd0  /mnt/cdrom –t iso9660
   ```

   NOTE: Use the `man mount` command for additional file system types.

Creating an iLO Virtual CD-ROM Image

The iLO Virtual Media feature enables you to create CD-ROM image files within the same applet. The image files created from the applet will be ISO-9660 file system images. The performance of iLO Virtual CD-ROM is faster when image files are used.

To create a Virtual Media image file:

1. Click **Create Disk Image.**
2. Select the drive letter and the image file name. You can use the Browse feature to find and select an existing image file or to change the directory in which the image file will be created.
3. Click **Create.** The Virtual Media applet begins the process of creating the image file. The process is complete when the progress bar reaches 100 percent.

The Disk>Image option is used to create image files from physical CD-ROMs. The Image>Disk option is not valid for a Virtual CD-ROM image.

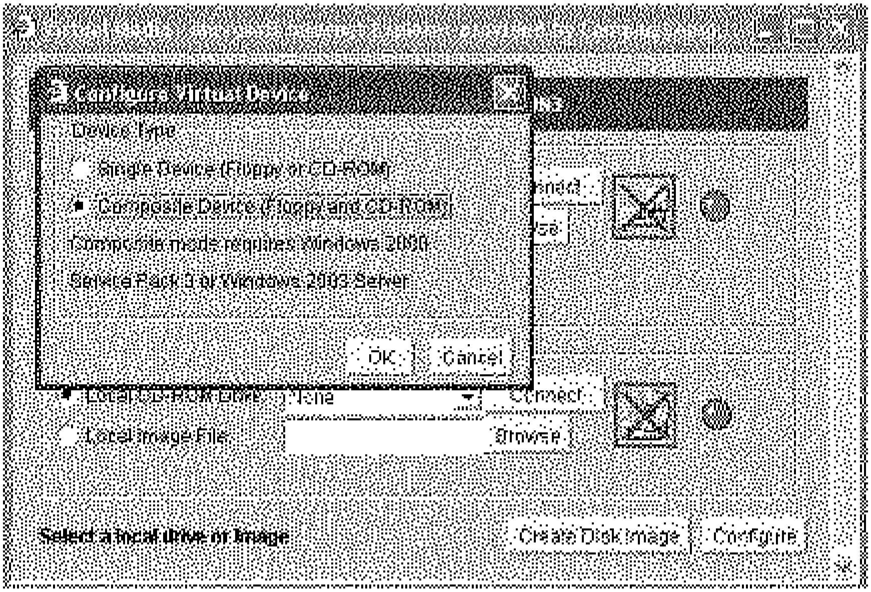
Virtual Media Composite Device Support

Composite device support allows both the Virtual Media Floppy Drive and the CD-ROM device to be connected to the host simultaneously. The drive selected can be either a physical drive or an image file or any combination of the two devices. Composite USB devices are only supported on Microsoft® Windows® 2000 with Service Pack 3 and Windows® 2003.

To configure composite mode:

1. Click **Configure.** The Configure Virtual Device window appears.
2. Select either:
   - **Single Device** for using either the Virtual Media Floppy or CD-ROM
   - **Composite Device** for using the Virtual Media Floppy and CD-ROM simultaneously

Composite Mode only functions properly on server operating systems that support composite USB devices. For a current list of supported server operating systems, refer to the server documentation and readme notes. Virtual Media Composite Device is not supported on the ProLiant ML370 G4, ProLiant DL360 G4, ProLiant DL380 G4, ProLiant DL360 G2, or ProLiant DL580 G2 servers.



Configure Virtual Device

Device Type

○ Single Device (Floppy or CD-ROM)

● Composite Device (Floppy and CD-ROM)

Composite mode requires Windows 2000 Service Pack 3 or Windows 2003 Server

● Local CD-ROM Drive None

○ Local Image File

Select a local drive or Image

To use composite devices:

1. Select **Local Floppy Drive.**
2. Select the drive letter of the desired physical floppy drive on your client PC from the dropdown menu, or select **Local Image File** within the Virtual Floppy section of the Virtual Media applet and enter the name of the diskette image in the text box or click **Browse** to locate image files.
3. Click **Connect.**

   If Virtual Media is configured for composite device support, whenever you connect just one of the devices, both devices become visible to the operating system. However, the operating system can only access the device you have connected. The other device shows a `Please insert a disk into drive` message if you try to access it. After you connect the other device from the applet, the operating system can to correctly access both devices.

4. Select **Local CD-ROM Drive.**
5. To locate image files do one of the following:
   - Select the drive letter of the desired physical CD-ROM drive on your client system from the dropdown menu.
   - Select **Local Image File** within the Virtual CD-ROM section of the Virtual Media applet and enter the name of the CD-ROM image in the text box.
   - Click **Browse** to locate image files.
6. Click **Connect.**

The operating system can now access both the Virtual Media Floppy Drive and the Virtual Media CD-ROM drive.

iLO Virtual Media Privilege

The ability to use the iLO Virtual Media is restricted by an iLO User Privilege. Authorized users must have the Virtual Media privilege to select a Virtual Media Device and connect it to the host server.

Do not attempt to upgrade the iLO firmware from a ROMPaq diskette using the iLO Virtual Floppy. If you attempt to remotely upgrade iLO using ROMPaq, iLO resets and you will lose the connection. iLO will not reconnect. Using the browser to upgrade iLO remotely makes the lost connection temporary and you are automatically reconnected. HP recommends remotely upgrading the iLO firmware using the Upgrade iLO Firmware option on the Administration tab.

Virtual Media Applet Timeout

The Virtual Media applet does not timeout when Virtual Media is connected to the host server. The Virtual Media applet closes if the user logs out.

Virtual Media Scripting

Virtual Media scripting is a method for controlling Virtual Media devices without going through the browser. Scriptable Virtual Media supports insert, eject and status commands for both floppy and CD-ROM images.

The XML commands enable you to configure Virtual Media in the same manner as the Virtual Media applet. The one exception is that the actual image will be located on a Web server with which the iLO can communicate with through the management network. After the image location is configured, the iLO will use the new firmware functionality to execute the USB or SCSI protocol with the Web server. Virtual Media scripting does not support composite devices. Only single Virtual Media devices (either Virtual Media Floppy OR Virtual Media CD-ROM) are supported.

HPLOVM.EXE is a new scripting utility that enables you to script insert, eject, and set boot options for Virtual Media devices. HPLOVM is intended to be used in place of the VFLOP.exe utility which is part of the SmartStart Scripting Toolkit.

Command line syntax:

```
HPLOVM [-device <floppy | cdrom>] [-insert <url>] [-
eject] [-wp <y | n>]
[-boot <once | always | never>] [-mgmt <ilo | riloe>] [-
ver] [-?]
```

Command Line Input	Result
`[-device <floppy	cdrom>]`	Defines which Virtual Media device is active.
`[-insert <url>]`	Defines the location of the Virtual Media image file that will be connected.
`[-eject]`	Ejects the media that is currently connected through the Virtual Media drive. The Virtual Media drive is still connected, but no media is present in the drive.
`[-wp <y	n>]`	Defines the write-protected status of the Virtual Floppy drive. This argument has no effect on the Virtual CD-ROM drive.
`[-boot <once	always	never>]`	Defines how the Virtual Media Drive is used to boot the target server.
`[-mgmt <ilo	riloe>]`	Defines which management processor is being used with LOVM utility. If RILOE is specified, the VLOP.EXE utility is used. The default setting of this argument is iLO.
`[-ver]`	Displays the HPLOVM utility version.

Command Line Input	Result
`[-?]`	Displays help information.

Scripting Web Server Requirements

Virtual Media scripting uses a media image that is stored and retrieved from a Web server accessible from the management network. The web server must be a HTTP 1.1 compliant server that supports the Range header. Furthermore, for write access to the file, the Web server should support DAV and must support the Content-Range header for DAV transactions. If the Web server does not meet the requirements for DAV, a helper CGI program may be used. The Web server may optionally be configured for basic HTTP authentication SSL support, or both.

Web Server	Read Support	Write Support	Authorization	SSL Support
Microsoft® IIS 5.0	Yes	Yes*	Not tested	Not Tested
Apache	Yes	Yes	Yes	Yes
Apache/Win32	Yes	Yes	Yes	Yes

*IIS does not support Content-Range for DAV transactions. A CGI helper program must be used for write support.

Virtual Media Image Files

Valid diskette images may be raw disk images, produced by the iLO Virtual Media applet, the UNIX® utility dd, the DOS utility rawrite, or images created by the CPQIMAGE utility. CD-ROM images must be ISO-9660 file system images. No other type of CD-ROM images are supported.

The images created by the Virtual Media applet are raw disk images in the case of diskettes and ISO-9660 images in the case of CD-ROMs. Many CD-ROM burning utilities can create ISO-9660 images. Refer to the documentation of your utility for additional information.

CGI Helper Application

The following perl script is an example of a CGI helper application that allows diskette writes on Web servers that cannot perform partial writes. When using the helper application, the iLO firmware posts a request to this application with three parameters:

- The file parameter contains the name of the file provided in the original URL.
- The range parameter contains an inclusive range (in hexadecimal) designating where to write the data.
- The data parameter contains a hexadecimal string representing the data to be written.

The helper script must transform the file parameter into a path relative to its working directory. This function might involve prefixing it with "../," or it might involve transforming an aliased URL path into the true path on the file system. The helper script requires write access to the target file. Diskette image files must have the appropriate permissions.

Example:

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working
# directory to the location of the image file#
my ($prefix) = "..";
my ($start, $end, $len, $decode);

# Get CGI data
my $q = new CGI();
# Get file to be written
my $file =  $q->param('file');

# Byte range
$range = $q->param('range');

# And the data
```

```
my $data =  $q->param('data');
#
# Change the filename appropriately
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {

   $start = hex($1);
   $end = hex($2);
   $len = $end - $start + 1;
}

#
# Decode the data (it's a big hex string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);
```

Virtual Indicators

The Unit ID LED is the blue LED on the HP server that is used for identifying systems in a rack full of servers. iLO enables you to view the status of the Unit ID LED and change the status using iLO Web pages.

The Unit ID LED flashes whenever a critical Remote Management task that should not be interrupted is currently active on the server.

The Unit ID LED flashes when the:

- Server is under active iLO Remote Console control.

- iLO settings are being modified through XML scripting.
- iLO firmware is being updated.

Never remove power from a server with a flashing Unit ID LED.

Virtual Serial Port

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. There are three types of data that can appear on a ProLiant server's serial port:

- Windows® EMS console
- Linux user session through serial tty (ttyS0)
- System POST dialog (if BIOS serial console redirection is enabled)

The Virtual Serial Port provides a Java™ applet that enables connection to the server serial port. The Java™ applet provides VT320 terminal emulation to access an application configured for the serial port.

Windows® EMS Console

The Windows® EMS Console, if enabled, provides the ability to perform Emergency Management Services in cases where video, device drivers, or other operating system features have prevented normal operation and normal corrective actions from being performed.

iLO, however, enables you to use EMS over the network through a Web browser. Microsoft® EMS enables you to display running processes, change the priority of processes, and halt processes. The EMS console and the iLO Remote Console can be used at the same time.

The Windows® EMS serial port must be enabled through the host system RBSU. The configuration allows for the enabling or disabling of the EMS port, and the selection of the COM port. The iLO system automatically detects whether the EMS port is enabled or disabled, and the selection of the COM port.

To obtain the SAC> prompt, entering Enter might be required after connecting through the Virtual Serial Port console.

For more information on using the EMS features, refer to the Windows® Server 2003 documentation.

Security Information

If Remote Console Data Encryption is enabled, the Virtual Serial Port data stream is encrypted as data is passed between the iLO system and the viewing applet.

Virtual Serial Port and Linux

The /dev/ttyS0 device, if configured, provides the ability to obtain serial tty sessions through the iLO Virtual Serial Port Console. The Linux system must be configured correctly. Refer to your specific Linux system implementation for the appropriate commands. Some general guidelines include:

- The Virtual Serial Port must be enabled through the host system RBSU. The configuration allows enabling or disabling of the Remote Virtual Serial Port. Refer to the host system RBSU documentation for the specific server for exact details. Generally, the RBSU contains a tab called BIOS Serial Console/EMS Support tab. Selecting this tab displays the EMS Console tab, which should be set to Remote. This enables both the Virtual Serial Port and the Windows® EMS Console.
- To begin a shell session on the configured UART, the appropriate Linux process must be started. This process can be started from the shell, but is usually configured in the /etc/inittab file to have the process available after the kernel has booted.

  ```
  s0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
  ```
- Linux expects the serial port to appear at the standard UART I/O address (0x3F8); however, LOM_short_name> presents the port at the non-standard address of 0x408. To inform Linux of the non-standard address, the following command must be used. This command can be placed in the rc.serial file which is commonly called from /etc/rc.local at system startup.

  ```
  setserial /dev/ttyS0 uart 16550A port 0x0408 irq 4
  ```

Linux requires that the terminal be listed in the /etc/securetty file in order to logon. Add the following line at the end of this file:

```
ttyS0
```

On some BL p-Class systems, the standard UART I/O address (0x3F8) is used when there is no conflict. On these systems, the setserial command is not required.

Linux End-to-End Support

The Virtual Serial Port, by default, uses the IO address 0x0408 and INTERRUPT 4 for communication. The Virtual Serial Port is configured and enabled when the RBSU is selected and the Virtual Serial Port feature is enabled. This is a known limitation of the Virtual Serial Port feature for Linux support, as this IO address is not a standard supported IO address. The `setserial` command can be used to configure agetty, but the kernel requires rebuilding to support LILO for booting redirection and kernel redirection. Full configurability, to standard UART IO addresses are provided in the 1.60 version of the iLO firmware, but a compatible host system ROM must be used. If the compatible host system ROM is available for the specific server, then the `setserial` command does not need to be used, and LILO booting redirection will appear on the Virtual Serial Port using the standard kernel.

Administration

The options available in the Administration tab enable you to manage user settings, SNMP alerting through integration with Systems Insight Manager, security settings, licensing, certificate administration, directory settings, and network environment settings. This section also provides a firmware upgrade option that enables you to keep iLO current.

User Administration

User Administration enables you to manage the user accounts stored locally in the secure iLO memory. Directory user accounts are managed using MMC or ConsoleOne snap-ins. Using the User Administration screen, you can add a new user, view or modify an existing user's settings, or delete a user.

iLO supports up to 12 users with customizable access rights, login names and advanced password encryption. Individual user's abilities are controlled by privileges. Each user can have privileges custom-tailored to their access requirements.

To support more than 12 users, iLO Advanced enables integration with virtually unlimited directory-based user accounts.

Adding a New User

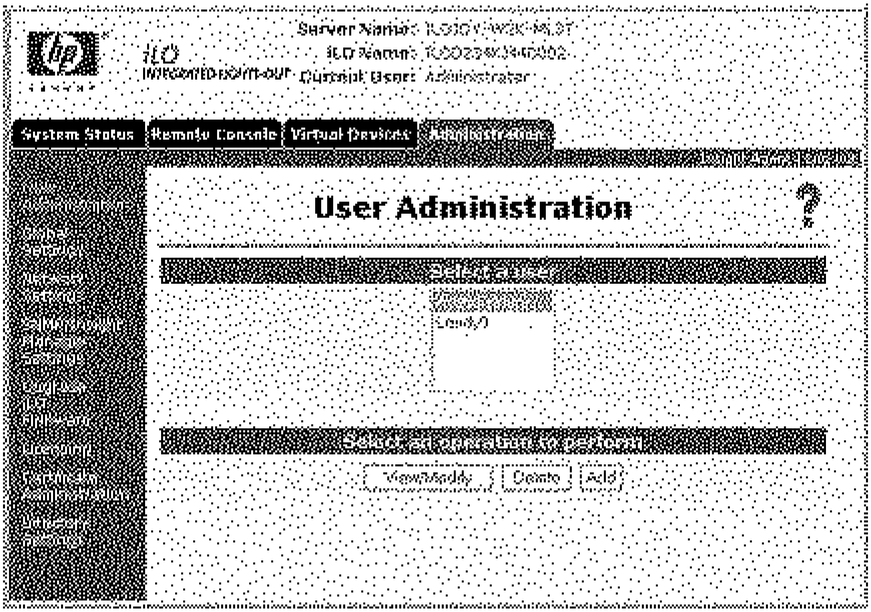
IMPORTANT: Only users with the Administer User Accounts privilege can manage other users on iLO.

You can assign a different access privilege to each user. Each user can have a unique set of privileges, designed for the tasks that the user must perform. Access to critical functions, such as Remote Console, Managing Users, Virtual Power button, and other features can be denied.

To add a new user to iLO:

1. Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration.**

2. Click User Administration. A screen similar to the one shown is displayed.



3. Click **Add.**
4. Complete the fields with the necessary information for the user being added.
5. When the user profile is complete, click **Save User Information** to return to the User Administration screen. To clear the user profile form while entering a new user, click **Restore User Information.**

Viewing or Modifying an Existing User's Settings

> **IMPORTANT:** Only users with the Administer User Accounts privilege can manage other users on iLO. All users can change their own password using the **View/Modify User** feature.

To view or modify an existing user's information:

1. Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration.**
2. Click **User Administration** and select from the list the name of the user whose information you want to change.
3. Click **View/Modify User.**

4. Change the user information in the fields that require modification. After changing the fields, click **Save User Information** to return to the User Administration screen. To recover the user's original information, click **Restore User Information.** All changes made to the profile will be discarded.

Deleting a User

> **IMPORTANT:** Only users with the Administer User Accounts privilege can manage other users on iLO.

To delete an existing user's information:

1. Log on to iLO using an account that has the Administer User Accounts privilege. Click **Administration.**
2. Click **User Administration** and select from the list the name of the user whose information you want to change.
3. Click **Delete User.** A pop-up window is displayed asking, `Are you sure you want to delete the selected user?` Click **OK.**

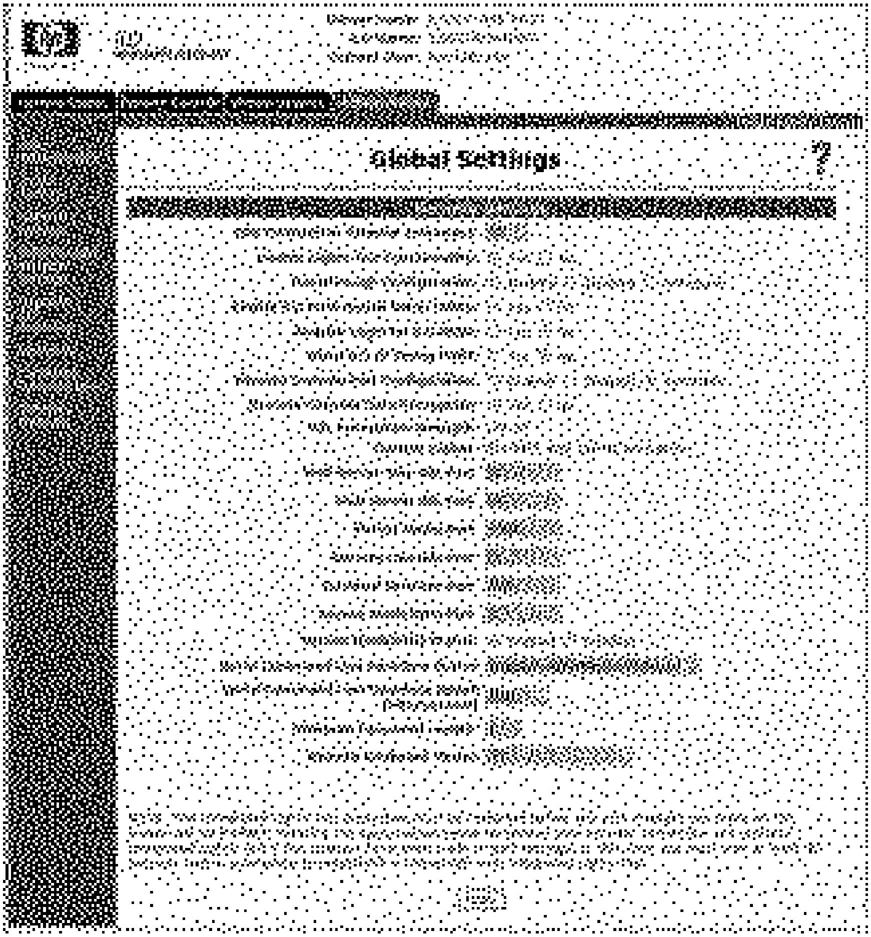
Global Settings

The Global Settings option enables you to view and modify security settings for iLO. The Global Settings screen enables you to configure the Remote Console timeout, and the iLO ports to be used for the iLO Web Server, Remote Console, and Virtual Media. These settings are applied globally, regardless of the individual user settings.

To change global settings for iLO:

1. Log on to iLO using an account that has the Configure iLO Settings privilege. Click **Administration.**
2. Click **Global Settings.**
3. Change the global settings as needed by entering your selections in the fields.
4. After completing any parameter changes, click **Apply** to save the changes.

IMPORTANT: Only users with the Configure iLO Settings privilege can change these settings. Users that do not have the Configure iLO Settings privilege can only view the assigned settings. This privilege is managed through the Configure Local Device Settings field in the directory administration snap-ins for directory users.



The Global Settings option enables you to define the following functions:

- Idle Connection Timeout (Minutes) (on page 340)
- Enable Lights-Out Functionality (on page 340)

- Pass-Through Configuration ("Terminal Services Pass-Through Option" on page 109)
- Enable iLO RBSU (on page 340)
- Require Login for iLO RBSU
- Show iLO during Post (on page 341)
- Remote Console Port Configuration (on page 341)
- Remote Console Data Encryption (on page 341)
- SSL Encryption Strength (on page 341)
- Current Cipher (on page 341)
- Web Server Non-SSL Port (on page 342)
- Web Server SSL Port (on page 342)
- Virtual Media Port (on page 342)
- Remote Console Port (on page 342)
- Terminal Services Port (on page 342)
- Secure Shell (SSH) Port (on page 342)
- Secure Shell (SSH) Status (on page 343)
- Serial Command Line Interface Status (on page 343)
- Serial Command Line Interface Speed (bits/second) (on page 343)
- Minimum Password Length (on page 343)
- Remote Keyboard Model (on page 343)

Network Settings

The Network Settings option enables you to view and modify the NIC IP address, subnet mask, and other TCP/IP-related settings. From the Network Settings screen you can enable or disable DHCP and, for servers not using DHCP, you can configure a static IP address.

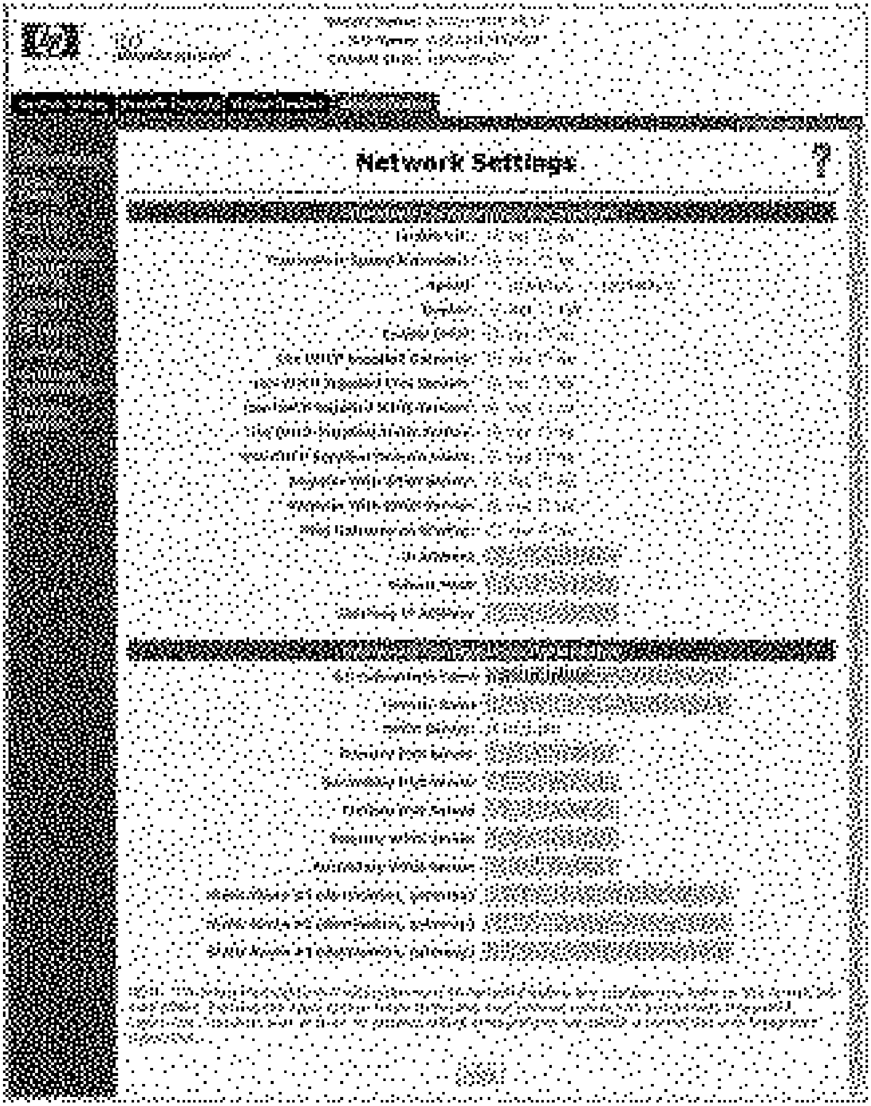
To change network settings for iLO:

1. Log on to iLO using an account that has the Configure iLO Settings privilege. Click **Administration.**

   IMPORTANT: Only users with the Configure iLO can change these settings. Users that do not have the Configure iLO Settings privilege can only view the assigned settings.

2. Click **Network Settings.**
3. Change the network settings as needed by entering your selections in the fields.

4. After completing any parameter ("Network Settings Parameters" on page 343) changes, click **Apply** to complete the changes.



When you click **Apply,** iLO restarts, and the connection of your browser to iLO terminates. To re-establish a connection, wait 60 seconds before launching another Web browser session and logging in.

iLO Diagnostic Port Configuration Parameters

The iLO Diagnostic Port on the front of ProLiant BL p-Class servers enables you to access and troubleshoot server issues by using a diagnostic cable. The iLO Diagnostic Port uses a static IP address. It does not use DHCP to obtain an IP address, register with WINS or dynamic DNS, or use a gateway. The diagnostic port cable should not be left plugged in without an active network connection, as it will cause degraded network performance on the standard iLO network port.

In Network Settings, you can configure specific diagnostic port information. For more information on using the diagnostic port and the diagnostic cable, refer to the Setup and Installation Guide for the blade server.

The following are the fields that can be configured for the diagnostic port:

- Enable NIC

  If Enable NIC is set to Yes, the diagnostic port is enabled.

- Transceiver Speed Autoselect
- Speed
- Duplex (on page 344)
- IP Address

  Use this parameter to assign a static IP address to iLO on your network. By default, the IP address is assigned by DHCP. By default, the IP address is 192.168.1.1 for all iLO Diagnostic Ports.

- Subnet Mask
  - Use the subnet mask parameter to assign the subnet mask for the iLO Diagnostic Port. By default, the subnet mask is 255.255.255.0 for all iLO Diagnostic Ports.
  - The use of the diagnostic port is automatically sensed when an active network cable is plugged in to it. When switching between the diagnostic and back ports, you must allow 90 seconds for the network switchover to complete before attempting connection through the Web browser.

    NOTE: The diagnostic port will not switch over if an active Remote Console session or a firmware update is in progress.

Recovering from a Failed iLO Firmware Update

In the event that an iLO firmware update has failed, there are various recovery options. For all of these options, you need a current firmware image. HP does not recommended downgrading iLO firmware, and the version you have could be corrupt.

1. Download the latest iLO firmware. iLO downloads are available on the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).
2. Determine if the update failed.
   a. Can you ping iLO?
   b. Can you log in?
   c. Does the iLO Option ROM prompt appear during host POST?
   d. Are the iLO status LEDs strobing in a regular pattern? Examine the iLO status LEDs inside the server to see if they are strobing in a regular pattern from LED 8, 7, 6, 5, 4, 3, 2, 1. If the iLO LED pattern is visible, proceed to step 4.
3. Attempt to re-flash over the network.

   You might be able to initiate a firmware update using RIBCL or a browser.

   If network flash failed, try the on-line flash component. Components are available for both Windowst® and Linux.
4. If the on-line flash component failed, try the ROMPAQ diskette.
   a. Build the ROMPAQ diskettes and boot the host using disk 1.
   b. You might need to set the iLO Security Override Switch for ROMPAQ to succeed. Restore the Security Override Switch after the flash process is complete.

SNMP/Insight Manager Settings

The SNMP/Insight Manager Settings option enables you to configure SNMP alerts, generate a test alert, and configure integration with Insight Manager 7 and Systems Insight Manager.

Enabling SNMP Alerts

iLO supports up to three IP addresses to receive SNMP alerts. Typically, this address is the same as the IP address of the Insight Manager 7 or Systems Insight Manager server console.

> **IMPORTANT:** Only users with the Configure iLO can change these settings. Users that do not have the Configure iLO Settings privilege can only view the assigned settings.

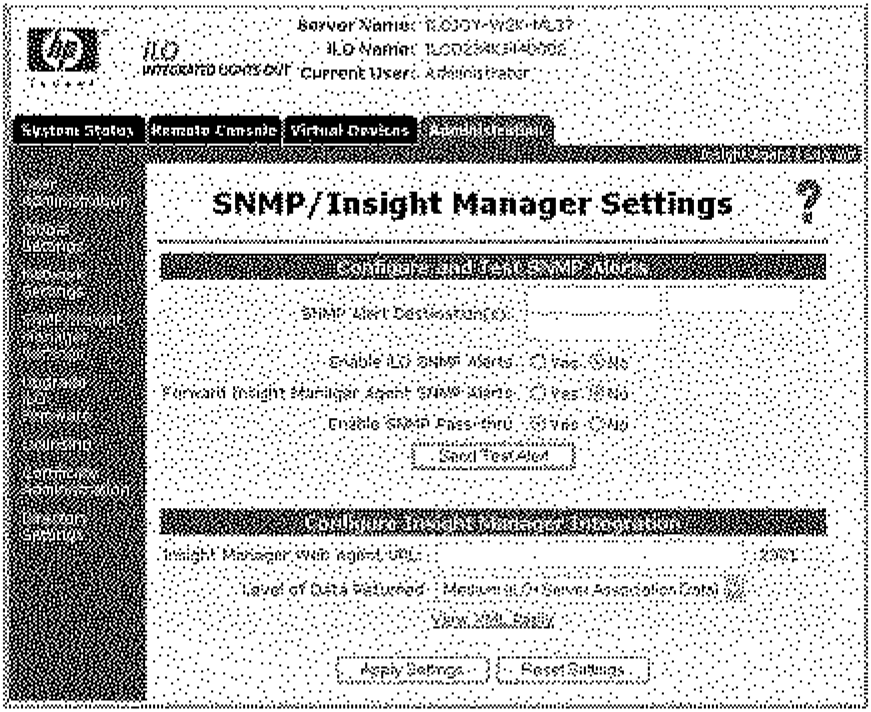
Three alert options are available in the SNMP/Insight Manager Settings screen:

- Enable iLO SNMP Alerts
- Forward Insight Manager Agent SNMP Alerts
- Enable SNMP Pass-Through (on page 347)

To configure alerts:

1. Log on to iLO using an account that has the Configure iLO Settings privilege.

2. Select **SNMP/Insight Manager Settings** in the Administration tab.



Current User: Administrator

SNMP/Insight Manager Settings

SNMP Alert Destination(s):

Enable iLO SNMP Alerts: ○ Yes ● No

Forward Insight Manager Agent SNMP Alerts: ○ Yes ● No

Enable SNMP Pass-thru: ● Yes ○ No

Insight Manager Web Agent URL: 2301

Level of Data Returned: Medium (iLO+Server Association Data)

3. Enter up to three IP addresses to receive the SNMP alerts.
4. Select the alert options you want iLO to support. For information on the Forward Insight Manager Agent SNMP Alerts field.
5. Click **Apply Settings.**

Generating Test Alerts

Test alerts are generated by means of the SNMP/Insight Manager Settings in the Administration section of the iLO navigation frame. These alerts include an Insight Manager SNMP trap and are used to verify the network connectivity of iLO in Insight Manager 7 and Systems Insight Manager. Only users with the Configure iLO Settings privilege can send test alerts.

Click **Apply Settings** to save any changes made to SNMP Alert Destination(s) before sending a test alert.

To send a test alert:

1. Select **SNMP/Insight Manager Settings** in the Administration tab.
2. Click **Send Test Alert** to generate a test alert and send it to the TCP/IP addresses saved in the SNMP Alert Destination(s) fields.
3. After generating the alert, a confirmation screen is displayed.
4. Check the Insight Manager 7 or Systems Insight Manager console for receipt of the trap.

Configure Insight Manager Integration

iLO enables you to configure the URL (DNS name or IP address) ("Insight Manager Web Agent URL" on page 348) of the Insight Manager Web Agents running on the host server. You can also configure the level of data returned with Insight Manager 7 or Systems Insight Manager identification information.

> **NOTE:** The expected entry in the Insight Manager Web Agent URL field is the IP address or the DNS name only. The protocol (for example, "http://") and a port ID (for example, ":2301") should not be entered.

The link to the Insight Web Agents is found on the blue header bar, next to the Log out link.

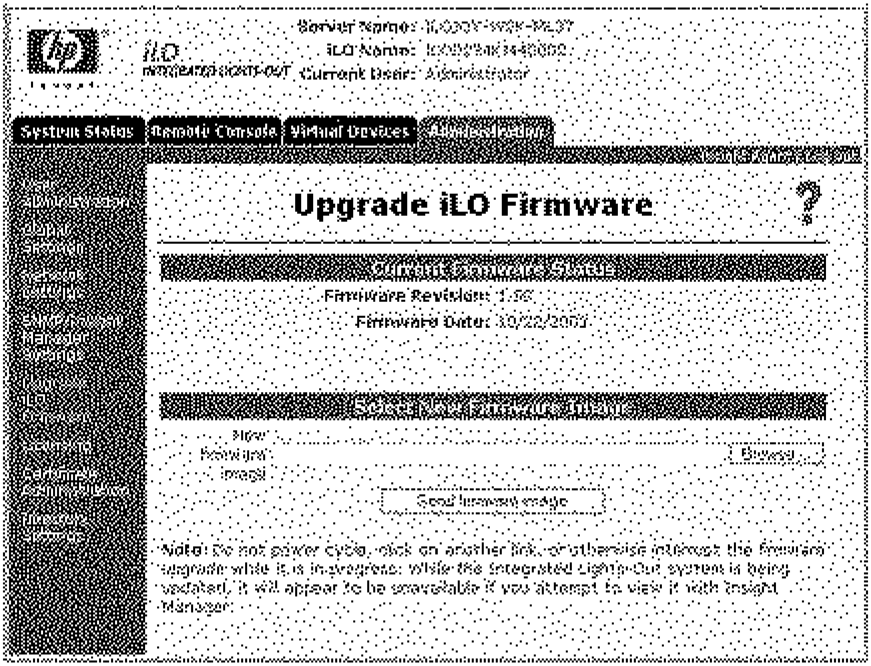
Upgrade iLO Firmware

Firmware upgrades enhance the functionality of iLO. The firmware upgrade can be done from any network client using a supported Web browser. Only users with the Update iLO Firmware privilege can upgrade the iLO firmware. The most recent firmware for iLO is available on the HP website.

To upgrade the iLO firmware using a supported Web browser:

1. Log on to iLO using an account that has the Configure iLO Settings privilege.

2. Click **Upgrade iLO Firmware** in the Administration tab.



Upgrade iLO Firmware

Current Firmware State

Firmware Revision: 1.50

Firmware Date: 10/22/2003

Select New Firmware Image

New firmware image:

Note: Do not power cycle, click on another link, or otherwise interrupt the firmware upgrade while it is in progress. While the Integrated Lights-Out system is being updated, it will appear to be unavailable if you attempt to view it with Insight Manager.

3. Enter the file name in the New firmware image field or browse for the file.
4. Click **Send firmware image.**
5. The firmware upgrade takes a couple of minutes. A progress bar displays the progress of the firmware upgrade.

Do not interrupt an Upgrade iLO Firmware session that is in progress. If the upgrade process is interrupted, refer to the "Inability to Upgrade iLO Firmware (on page 391)" section.

The iLO system automatically resets at the end of a successful firmware upgrade. The host operating system and server are not affected by the iLO system being reset.

If the firmware upgrade was interrupted or failed, immediately attempt the upgrade again. Do not reset the iLO system before reattempting a firmware upgrade. iLO provides an FTP-based firmware upgrade disaster recovery ("Inability to Upgrade iLO Firmware" on page 391) if a firmware upgrade is interrupted or failed.

> **NOTE:** For systems with diskette drives, you can also update the iLO firmware using ROMPaq diskettes. HP does **not** recommend updating iLO firmware using the Virtual Media floppy diskette.

Licensing

The iLO Advanced License Activation page is used to apply the license activation for the iLO Advanced Pack. The "Enabling iLO Advanced Functionality (on page 28)" section discusses the steps required to enter the activation key and enable the advanced features.

Certificate Administration

Certificate Information displays the information associated with the stored certificate. Information is encoded in the certificate by the CA, and is extracted by iLO for display.

- Issued To is the entity to whom the certificate was issued.
- Issued By is the CA that issued the certificate.
- Valid From is the date from which the certificate is valid.
- Valid Until is the date that the certificate will expire.
- Serial Number is the serial number assigned to the certificate by the CA.

Importing a Certificate displays information on how to import a certificate. For more information on importing certificates, refer to "Certificates (on page 140)" in the "iLO Security (on page 135)" section.

Directory Settings

The Directory Settings screen enables you to configure and test your directory services. For additional information on directories, refer to "Directory Services (on page 143)." For additional information on directory configuration parameters, refer to "Configuring Directory Settings (on page 184)."

ProLiant BL p-Class Advanced Management

iLO Advanced is a standard component of ProLiant BL p-Class server blades that provides server health and remote server blade manageability. Its features are accessed from a network client device using a supported Web browser. In addition to other features, iLO Advanced provides keyboard, mouse, and video (text and graphics) capability for a server blade, regardless of the state of the host operating system or host server blade.

iLO includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes iLO independent of the host server blade and its operating system. iLO provides remote access to any authorized network client, sends alerts, and provides other server blade management functions.

Using a supported Web browser, you can:

- Remotely access the console of the host server blade, including all text mode and graphics mode screens with full keyboard and mouse controls.
- Remotely power up, power down, or reboot the host server blade.
- Remotely boot a host server blade to a virtual diskette image to perform a ROM upgrade or install an operating system.
- Send alerts from iLO Advanced regardless of the state of the host server blade.
- Access advanced troubleshooting features provided by iLO Advanced.
- Launch a Web browser, use SNMP alerting, and diagnose the server blade using HP Systems Insight Manager.
- Configure static IP bay settings for the dedicated iLO management NICs on each server blade in an enclosure for faster deployment.

The server blade must be properly cabled for iLO connectivity. Connect to the server blade with one of the following methods:

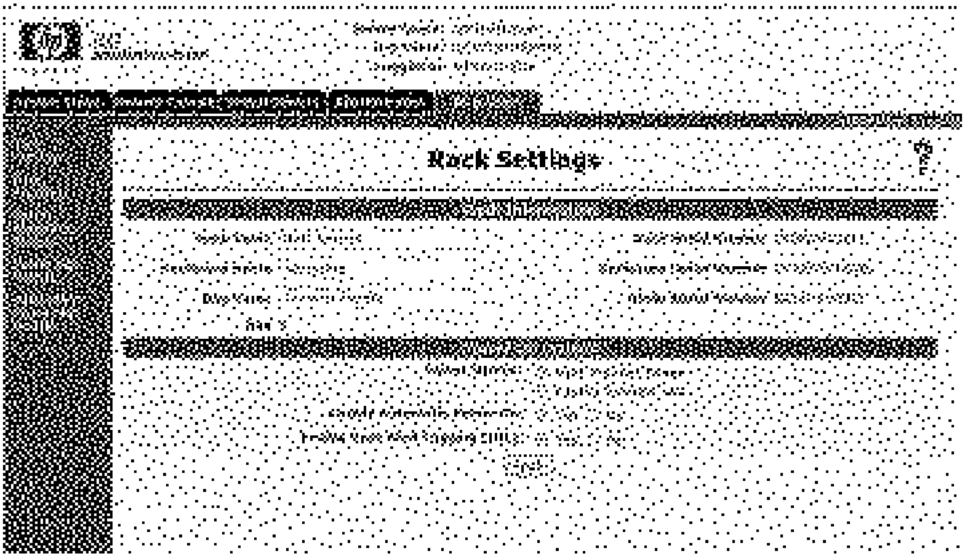
- Through an existing network (in the rack)—This method requires you to install the server blade in its enclosure and assign it an IP address manually or using DHCP.
- Through the server blade I/O port
  - In the rack—This method requires you to connect the local I/O cable to the I/O port and a client PC. Using the static IP address listed on the I/O cable label and the initial access information on the front of the server blade, you can access the server blade with the iLO Advanced Remote Console.
  - Out of the rack, with the diagnostic station—This method requires you to power the server blade with the optional diagnostic station and connect to an external computer using the static IP address and the local I/O cable. For cabling instructions, refer to the documentation that ships with the diagnostic station or to the Documentation CD.
  - Through the server blade rear panel connectors (out of the rack, with the diagnostic station)—This method enables you to configure a server blade out of the rack by powering the blade with the diagnostic station and connecting to an existing network through a hub. The IP address is assigned by a DHCP server on a network.

The BL p-Class tab enables you to control specific settings for the ProLiant BL p-Class blade server rack. iLO also provides Web-based status for the ProLiant BL p-Class server rack.

> **NOTE:** The fourth Web page is available when a redundant power management module is in the server configuration.

Rack Settings

Blade servers communicate with the rack environment to obtain power and manage shared resources of the rack (fans, temperature, power supplies). The Rack Settings option enables you to configure this communication.



The following fields are available:

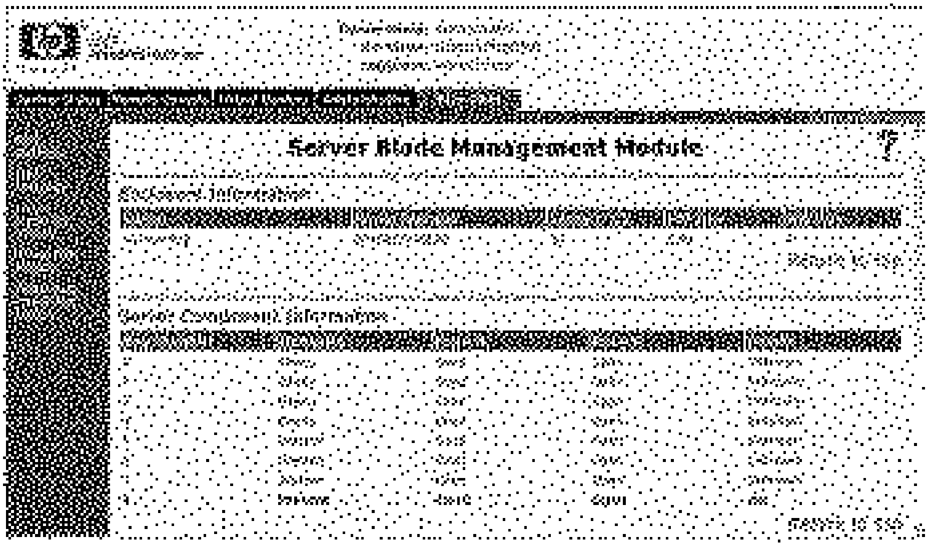
- Rack Name
- Enclosure Name
- Bay Name (on page 349)
- Bay (on page 349)
- Rack Serial Number (on page 349)
- Enclosure Serial Number (on page 349)
- Blade Serial Number (on page 350)
- Power Source
- Enable Automatic Power On (on page 350)

- Enable Rack Alert Logging (IML) (on page 350)

Server Blade Management Module

The Server Blade Management Module screen:

- Displays devices discovered in the BL p-Class server blade enclosure
- Reads and displays the current firmware version of the controller for the server blade enclosure
- Detects and displays the fuse state and power state of blade servers
- Enables you to activate the enclosure Unit Identification LEDs
- Displays network component information



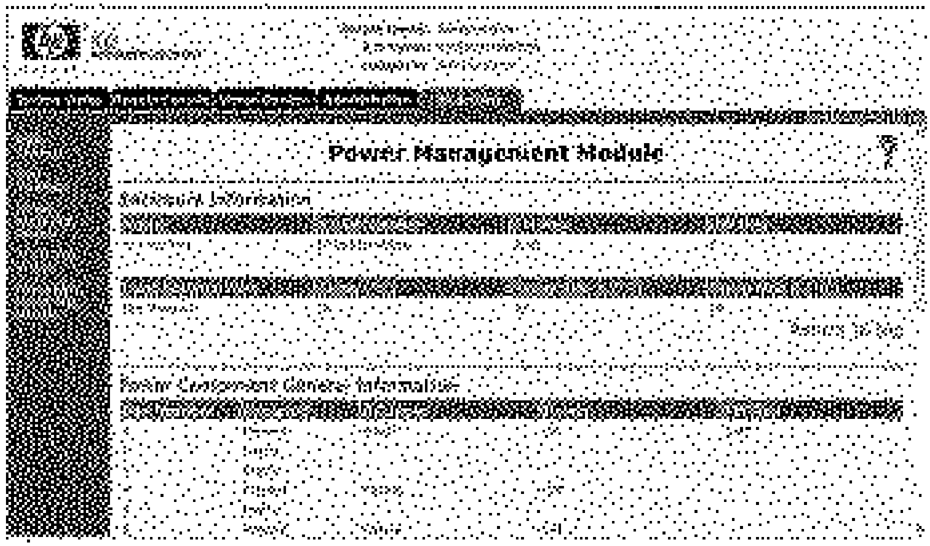
Server Blade Management Module

Power Management Module

The Power Management Module screen:

- Detects and displays the main power supplies

- Reads and displays the current firmware version of the controller for the power supply enclosure
- Displays the current power output, maximum power output, and temperature information for the power supply
- Enables you to activate the power management module Unit Identification LEDs



Redundant Power Management Module

If the rack topology consists of a redundant power supply, the Redundant Power Management Module screen will be available. The Redundant Power Management Module screen provides the same information concerning the redundant power management module as the Power Management Module screen provides for the power management module.

iLO Control of ProLiant BL p-Class Server LEDs

iLO can monitor BL p-Class servers through POST tracking and the Server Health LED.

Server POST Tracking

Feedback is limited while the server is booting because of the headless nature of the ProLiant BL p-Class servers. iLO provides boot-time feedback by flashing the Server Health LED green during server POST. The LED is set to solid amber if the boot is unsuccessful. The LED is set to solid green at the end of a successful boot.

After a successful boot, control of the Server Health LED is returned to the server, which can turn the LED off or set it to some other color to represent the health of the server hardware.

Insufficient Power Notification

iLO turns the Server Health LED solid red if iLO cannot power on the server because insufficient power is in the rack infrastructure.

Hot-Plug Keyboard

Hot-plug keyboard functionality was implemented for all servers with iLO. The hot-plug keyboard feature supports connecting a local keyboard to the server while the server is in a powered-on state. It is not necessary to power cycle the server to get local keyboard functionality after hot-plugging a keyboard. If a keyboard is connected to the server after the operating system has booted, the hot-plugged keyboard is fully functional. The keyboard can be hot-plugged multiple times after the operating system has booted.

Keyboard Definitions

- Local keyboard—A keyboard physically connected to the PS2 connector on the server.
- Remote Console keyboard—The keyboard used during a Remote Console session.
- Hot-plug keyboard functionality—A fully-functioning local keyboard after hot-plugging it to a server.
- Hot-plugging a keyboard—Connecting a local keyboard to the keyboard PS2 connector on the server while the server is in a powered-on state.

- Hot-unplugging a keyboard—Disconnecting a local keyboard from the server while the server is in a powered on state.

Hot-Plug Keyboard Recommended Usage

For best results, follow these guidelines:

- Only hot-plug a local keyboard after the operating system has booted.
- Do not hot-unplug the local keyboard before the operating system has booted. Hot-plugging or hot-unplugging of the local keyboard before the operating system boots can lead to unpredictable results.

⚠ **WARNING: Do not change iLO network settings or port assignments, reset iLO, upgrade iLO firmware, or otherwise make iLO unavailable while powering on the server or booting the operating system without a local keyboard connected. Perform these actions before powering on the server or after the operating system has booted. If performing these actions before powering on the server, wait 30 seconds until applying power.**

Failure to follow the preceding guidelines can result in loss of local and Remote Console keyboard functionality.

Hot-Plug Keyboard Troubleshooting

If the hot-plug keyboard is unavailable or locks up, review the following to correct the problem. For best results, follow the guidelines in "Hot-Plug Keyboard Recommended Usage (on page 107)."

- If a Remote Console session is active on the server, the local keyboard will not be functional after hot-plugging it. This configuration is by design, for security purposes.

- If iLO is unavailable from power-on through operating system boot and a local keyboard is not present, Remote Console keyboard functionality might not function when iLO becomes available again, depending on the operating system. iLO can become unavailable for various reasons, including firmware upgrade, network settings change, or reassignment of ports. It might be necessary to power cycle the system to regain Remote Console keyboard functionality.
- If iLO is unavailable from power-on through operating system boot and a local keyboard is hot-plugged after operating system boot, the Remote Console and local keyboard might not function when iLO becomes available again, depending on the operating system. iLO can become unavailable for various reasons, including a firmware upgrade, network settings change, or reassignment of ports. It might be necessary to power cycle the system to regain Remote Console and local keyboard functionality.
- If iLO should become so busy that it is unable to respond in a timely fashion to keyboard commands sent by operating system while the operating system is loading and a local keyboard is not present, the operating system will assume that no keyboard is connected. This situation is unlikely but can theoretically occur any time iLO becomes extremely busy. An example of this condition is when iLO experiences a Denial of Service attack over its NIC. In this case, if a keyboard is hot-plugged after the operating system is loaded, local and Remote Console keyboard functionality might not function, depending on the operating system. It might be necessary to power cycle the system to regain Remote Console keyboard functionality.
- If a local keyboard is hot-unplugged after the operating system boots with caps-lock, num-lock, or scroll lock on and then is hot-plugged, the LED indicators on the local keyboard will not reflect the current state of the keyboard. Press the lock key for the desired function until the correct LED indicator state is reached.
- If the local keyboard locks up when hot-plugged, unplug the keyboard and plug it in again.

Terminal Services Pass-Through Option

Terminal Services is provided by the Microsoft® Windows® operating systems. The iLO Terminal Services pass-through option provides a connection between the Terminal Services server on the host system and the Terminal Services client on the client system. When the Terminal Services pass-through option is enabled, iLO firmware sets up a socket, listening by default on port 3389. All data received from the Terminal Services on this port is forwarded to the server and all data it receives from the server is forwarded back to the socket. The firmware assumes anything received on this port is in an RDP packet. RDP packets are exchanged between the iLO firmware and the server's Terminal Services (RDP) server through the localhost address on the server. A service is provided to facilitate communications between the iLO firmware and the RDP server, such that the RDP server believes that an external RDP connection has been established. For more information on RDP service, refer to the "Windows® RDP Pass-Through Service (on page 110)" section.

A Terminal Services session provides a performance-enhanced view of the host system console. When the operating system is unavailable (or the Terminal Services server or client is unavailable), the traditional iLO remote console provides the view of the host system console. For more information on Remote Console and Terminal Services, refer to the "Remote Console and Terminal Services Clients (on page 114)" section.

To configure the Terminal Services pass-through option, refer to "Terminal Services Client Requirements (on page 109)" and "Terminal Services Pass-Through Installation (on page 111)."

Terminal Services Client Requirements

The Terminal Services client is available on Microsoft® Windows® client machines running:

- Windows® 2000

Microsoft® Windows® 2000 servers require the installation of Microsoft® .NET Framework to support the use of Terminal Services. After .NET Framework is installed, the Terminal Services client must be installed from diskettes created by the Terminal Services server. Consult your Windows® operating guides or help files for instructions. When installing the Terminal Services client on Windows® 2000, use the default installation location. The Terminal Services client in Windows® 2000 generates a dialog box asking for which target Terminal Services server to use.

- Windows® Server 2003

  On Windows® Server 2003 servers, the Terminal Services client and RDP connection is built in. The client is an integral part of the operating system and is activated using Remote Desktop sharing. To activate desktop sharing allow, select **My Computer>Properties>Remote>Remote Desktop.** The Terminal Services client in Windows® Server 2003 provides command line options and seamless launches from the Remote Console applet.

- Windows® XP

  On Windows® XP servers, the Terminal Services client and RDP connection is built in. The client is an integral part of the operating system and is executed by selecting **Start>Programs>Accessories>Communications>Remote Desktop.** The Terminal Services client in Windows® XP provides command line options and seamless launches from the Remote Console applet.

Windows® RDP Pass-Through Service

To use the iLO Terminal Services Pass-Through feature, a service must be installed on the host system. This service will show the name of iLO Proxy in the host's list of available services. The service utilizes the Microsoft® .NET framework's security and reliability. After the service has started, the service polls the iLO to find out if a an RDP connection with the client has been established. If an RDP connection with the client has been established, it then establishes a TCP connection with localhost and begins exchanging packets. The port used to communicate with localhost is read from the Windows® registry at

```
HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds
\rdpwd\Tds\tcp\PortNumber
```

This is typically port 3389.

Terminal Services Pass-Through Installation

- Microsoft® Windows® 2000 and Windows® 2003

  Microsoft® Windows® 2000 servers require Microsoft® .NET Framework to support the use of Terminal Services. The Terminal Services pass-through service and the iLO Management Interface Driver for Windows® 2000 and Windows® Server 2003 must be installed on the server that has the iLO. The service and iLO driver are available as Smart Components on the HP website and on the HP SmartStart CD. They are also part of the ProLiant Support Pack for Microsoft® Windows® Server 2003 and Microsoft® Windows®.

  a. Install the iLO Management Interface driver.

  b. Install the service. To install the service, launch the component installer and follow the directions in the installation wizard.

     If the service is already installed, then it must be manually restarted or the server rebooted when the driver is installed.

  c. Install or activate the Terminal Services client.

     Microsoft® Windows® 2000 servers require the installation of Microsoft® .NET Framework to support the use of Terminal Services. After .NET Framework is installed, the Terminal Services client must be installed from diskettes created by the Terminal Services server or by downloading the client from the Microsoft® website and installed through the Control Panel using Add or Remove Programs. Consult your Windows® operating guides or help files for instructions. When installing the Terminal Services client on Windows® 2000, use the default installation location.

     On Windows® Server 2003, you can activate Remote Desktop sharing by selecting the **Remote** tab under My Computer and Properties.

  If the iLO installation is complete and if Terminal Services pass-through is set to automatic, then Terminal Services launches when the installation is complete.

- Microsoft® Windows® XP

  On Windows® XP servers, Remote Desktop Connection is built in and has no other installation requirements.

Errors during installation and during execution of the pass-through service will be logged in the server's Application Event Log. The pass-through service may be removed using Add or Remove Programs in the Control Panel.

Windows® 2000 Terminal Services Port Change

If the Terminal Services port is changed, Windows® 2000 client must manually configure the Terminal Services Client Connection Manager.

1. Start the Terminal Services Client Connection Manager, and create a new connection to the terminal server.
2. Highlight the icon created, and select **File>Export.** Rename the file with a .cns extension. For example: myilo.cns.
3. Edit the `myilo.cns` file by looking for the line Server Port=3389. Replace 3389 with your new port number and save the file.
4. From the Client Connection Manager, highlight the **New Connection** icon, and click **File>Import.**
5. Double-click the newly created icon to launch terminal server and connect to the new port.

Enabling the Terminal Services Pass-Through Option

By default, the Terminal Services pass-through feature is disabled and must be enabled in Global Settings. Until the Terminal Services pass-through feature is enabled, the Remote Console has the Terminal Services button deactivated, and the console session error message `Remote Session already in use by another user` is misleading.

Use of the Terminal Services pass-through feature requires installation of the latest Lights-Out Management Interface Driver and Terminal Services pass-through Service for Microsoft® Windows® on the server. The interface driver must be installed before installing the service.

When the Terminal Services pass-through option is set to Enabled or Automatic on the Global Settings page and the Terminal Services Client is installed on the Windows® client (installs by default on Windows® XP), the Terminal Services button is enabled. When the Terminal Services button is clicked, the applet tries to launch the Terminal Services, even if the server is not running a Windows® operating system.

You must comply with Microsoft® license requirements which are the same as connecting through the server's NIC. For instance, when set for administrative access, Terminal Services does not allow more than two connections, regardless of whether the connections are through the server's NIC or iLO or both.

Terminal Services Pass-Through Status

The iLO Status page displays the status of the Terminal Services pass-through feature, as follows:

- Server software not detected
- Available for use
- In use

The UID light flashes whenever a Terminal Services connection is active through the iLO. It flashes at the same frequency and duty cycle as when the Remote Console is active.

Terminal Services Warning Message

Terminals Services users operating on Windows® 2003 Server might notice the following when using the Terminal Services pass-through feature of iLO. If a Terminal Services session is established through iLO and a second Terminal Services session is established by a Windows® administrator (Console mode), the first Terminal Services session is disconnected. However, the first Terminal Services session does not receive the warning message indicating the disconnection until approximately one minute later. During this one-minute period, the first Terminal Services session is available or active. This is normal behavior, but it is different than the behavior observed when both Terminal Services sessions are established by Windows® administrators. In that case, the warning message is received by the first Terminal Services session immediately.

Terminal Services Button Display

This version of the iLO firmware does not accurately display through the Terminal Services button whether the host operating system is enabled for Terminal Services operation. Even if the operating system is not enabled (for example, the host operating system is Linux, which does not support Terminal Services operation), the Terminal Services button might not appear inactive and might inaccurately imply that Terminal Services operation is available.

Remote Console and Terminal Services Clients

Using the management network connection to the iLO, an iLO Remote Console session can be used to display a Terminal Services session to the host. When the iLO Remote Console applet runs, it launches the Terminal Services client based on user preference. The Sun JVM must be installed to obtain full functionality of this feature. If the Sun JVM is not installed, then the dual-cursor Remote Console cannot automatically launch the Terminal Services client.

If Terminal Services pass-through is enabled, and the Terminal Services server is available, switching between iLO Remote Console and the Terminal Services client will be seamless as the server progresses from pre-OS environment to OS-running environment, to OS-not available environment. The seamless operation is available as long as the Terminal Services client is not started before Remote Console is available. If Remote Console is available, and the Terminal Services client is available, Remote Console will start the Terminal Services client when appropriate.

When using the Terminal Services pass-through option with Windows® 2000, there is approximately a one-minute delay after the CTRL-ALT-DEL dialog box appears before the Terminal Services client launches. On Windows® Server 2003, the delay is about 30 seconds. The 30 second delay represents how long it takes for the service to connect to the RDP client running on the server. If the server is rebooted from the Terminal Services client, the Remote Console screen turns grey or black for up to one minute while iLO determines that the Terminal Services server is no longer available.

If Terminal Services mode is set to `Enabled,` but you want to use the Remote Console, then the Terminal Services client should be launched directly from the Terminal Services client menu. Launching directly from the client menu allows simultaneous use of the Terminal Services client and the Remote Console.

Terminal Services can be disabled or enabled at any time. Changing the Terminal Services configuration causes the iLO firmware to reset. Resetting the iLO firmware interrupts any open connections to iLO.

When the Terminal Services client is launched by the Remote Console, Remote Console goes into a sleep mode to avoid consuming CPU bandwidth. Remote Console still listens to the Remote Console default port 23 for any commands from the iLO.

iLO passes-through only one Terminal Services connection at a time. Terminal Services has a limit of two concurrent sessions.

The Remote Console activates and becomes available if the Remote Console is in sleep mode and the Terminal Services client is interrupted by any of the following:

- The Terminal Services client is closed by the user.
- The Windows® operating system is shut down.
- The Windows® operating system locks-up.

Terminal Services Troubleshooting

If you are experiencing problems with iLO Terminal Services Pass-through, check the following:

1. Verify that Terminal Services is enabled on the host by selecting **My Computer>Properties>Remote>Remote Desktop.**
2. Verify that the iLO pass-through configuration is enabled or automatic by checking iLO Global Settings.
3. Verify whether iLO Advanced functionality is licensed.
4. Verify whether the iLO Management Interface Driver is installed on the host by selecting **My Computer>Properties>Hardware>Device Manager>Multifunction Adapters.**
5. Verify if Terminal Services pass-through service and iLO Proxy is installed and running on the host by selecting **Control Panel>Administrative Tools>Services** and attempting to restart the service.
6. Determine whether the Application Event Log is full.

The Terminal Services Pass-through service might experience start-up problems when the operating system Application Event Log is full. To view the event log, select **Computer Management>System Tools>Event Viewer>Application.**

7. Verify that the Terminal Services port assignment is correct. Verify that the Terminal Services client, mstsc.exe is located in \WINDOWS\SYSTEM32.

   If not, reconfigure the pass-through configuration to **Enabled** and manually activate the terminal services client.

HP ProLiant Essentials Rapid Deployment Pack Integration

HP ProLiant Essentials Rapid Deployment Pack integrates with iLO to allow the management of remote servers and the performance of remote console operations regardless of the state of the operating system or hardware.

The Deployment Server provides the ability to use the power management features of iLO to power on, power off, or cycle power on the target server. Each time a server connects to the Deployment Server, the Deployment Server polls the target server to see if a LOM management device is installed. If installed, the server gathers information including the DNS name, IP address, and first user name. Security is maintained by requiring the user to enter the correct password for that user name.

For more information about the ProLiant Essentials Rapid Deployment Pack, refer to the documentation that ships on the ProLiant Essentials Rapid Deployment Pack CD or the HP website (http://www.hp.com/servers/rdp).

Telnet Support

iLO supports the use of telnet to access the iLO command line interface. Telnet access to iLO supports the CLI, which can invoke a Remote Console connection as well as a Virtual Serial Port connection. Refer to the "Command Line Interface (on page 130)" section for more information.

Using Telnet

To use telnet, the iLO Remote Console Port Configuration and Remote Console Data Encryption on the Global Settings screen must be configured as follows:

1. Set the Remote Console Port Configuration to **Enabled.**
2. Set the Remote Console Data Encryption to **No.**

You can open either a telnet based Remote Console session or a browser-based Remote Console session. You cannot open both at the same time. An error message is generated if both sessions are opened simultaneously.

To access iLO using telnet:

1. Open a telnet window.
2. When prompted, enter the IP address or DNS name, login name, and password.

   NOTE: Access through telnet will be disabled, if the remote console port configuration on the Global Settings tab is set to Disabled or Automatic, or if remote console data encryption is enabled.

To terminate a telnet session:

1. Press the **Ctrl+]** keys and press the **Enter** key at the prompt.
2. If you see an extra carriage return each time the Enter key is pressed, press the **Ctrl+]** keys and enter `set crlf off` at the prompt.

   Refer to "iLO VT100+ Key Map (on page 119)" for a complete list of key sequences.

Telnet Simple Command Set

The following key sequences for simple command set are available for use during telnet sessions. These commands are available only when in a telnet-based Remote Console or Virtual Serial Port session.

Action	Key Sequence	Comments
POWER ON	CTRL P 1	CTRL P is the prefix for the Power commands. The 1 indicates an ON selection.

Action	Key Sequence	Comments
POWER OFF	CTRL P 0	CTRL P is the prefix for the Power commands. The 0 indicates an OFF selection.
ACPI PRESS	CTRL P 6	CTRL P is the prefix for the Power commands. The 6 indicates an ACPI power press. The ACPI power press is equivalent to holding the power button for approximately 6 seconds.
SYSTEM REBOOT	CTRL P !	CTRL P is the prefix for the Power commands. The ! indicates an immediate emergency reboot.
UID ON	CTRL U 1	CTRL U is the prefix for the UID commands. The 1 indicates an ON selection
UID OFF	CTRL U 0	CTRL U is the prefix for the UID commands. The 0 indicates an OFF selection.

Key sequences operate during a telnet Remote Console session or Virtual Serial Port session. The keys do not work before authentication. The power control requests are correctly ignored when you do not have the correct power control privileges.

Telnet Security

Telnet is an unsecured network protocol. To reduce any security risks:

- Use SSH instead of telnet. SSH is essentially secure or encrypted telnet. CLI is supported through telnet as well as SSH.
- Use a segregated management network. Preventing unauthorized access to the network segment prevents unauthorized activity.

Supported Key Sequences

iLO supports the VT100+ protocol. The following tables define the supported key sequences.

iLO VT100+ Key Map

The following are VT100+ key sequences.

- Many terminal programs send CR-LF when they mean ENTER.

  `Sequence "\r\n" = '\r'`

- Some terminals send `ASCII 127` (DEL) when they mean backspace. The DELETE key never sends DEL, it sends `"\e[3~"`.

- Some programs use the following mapping for HOME and END:

  ```
  sequence "\e[H" = HOME_KEY
  sequence "\e[F" = END_KEY
  ```

- `ALT_CAPITAL_O` and `ALT_LEFT_SQBRACKET` are ambiguous.

- Terminate longer sequences that start with `\eO and \e[`), with `\?.`

Key	Sequence	Key	Sequence
\010	\177	**ALT_AMPER**	\e&
UP_KEY	\e[A	**ALT_APOS**	\e'
DOWN_KEY	\e[B	**ALT_OPAREN**	\e(
RIGHT_KEY	\e[C	**ALT_CPAREN**	\e)
LEFT_KEY	\e[D	**ALT_STAR**	\e*
ALT_A	\eA	**ALT_PLUS**	\e+
ALT_B	\eB	**ALT_COMMA**	\e,
ALT_C	\eC	**ALT_MINUS**	\e-
ALT_D	\eD	**ALT_PERIOD**	\e.
ALT_E	\eE	**ALT_SLASH**	\e/
ALT_F	\eF	**ALT_COLON**	\e:
ALT_G	\eG	**ALT_SEMICO**	\e;
ALT_H	\eH	**ALT_LESS**	\e<
ALT_I	\eI	**ALT_EQUAL**	\e=
ALT_J	\eJ	**ALT_MORE**	\e>

Key	**Sequence**	**Key**	**Sequence**
ALT_K	\eK	**ALT_QUES**	\e?
ALT_L	\eL	**ALT_AT**	\e@
ALT_M	\eM	**ALT_OPENSQ**	\e[\?
ALT_N	\eN	**ALT_BSLASH**	\e\\
ALT_O	\eO\?	**ALT_CLOSESQ**	\e]
ALT_P	\eP	**ALT_CARAT**	\e^
ALT_Q	\eQ	**ALT_USCORE**	\e_
ALT_R	\eR	**ALT_ACCENT**	\e`
ALT_T	\eT	**ALT_PIPE**	\e|
ALT_U	\eU	**ALT_CBRACK**	\e}
ALT_V	\eV	**ALT_TILDE**	\e~
ALT_W	\eW	**ALT_TAB**	\e\t
ALT_X	\eX	**ALT_BS**	\e\010
ALT_Y	\eY	**ALT_CR**	\e\r
ALT_Z	\eZ	**ALT_ESC**	\e\e\?
ALT_LOWER_A	\ea	**ALT_F1**	\e\eOP
ALT_LOWER_B	\eb	**ALT_F2**	\e\eOQ
ALT_LOWER_C	\ec	**ALT_F3**	\e\eOR
ALT_LOWER_D	\ed	**ALT_F4**	\e\eOS
ALT_LOWER_E	\ee	**ALT_F5**	\e\eOT
ALT_LOWER_F	\ef	**ALT_F6**	\e\eOU
ALT_LOWER_G	\eg	**ALT_F7**	\e\eOV
ALT_LOWER_H	\eh	**ALT_F8**	\e\eOW
ALT_LOWER_I	\ei	**ALT_F9**	\e\eOX

Key	Sequence	Key	Sequence
ALT_LOWER_J	\ej	**ALT_F10**	\e\eOY
ALT_LOWER_K	\ek	**ALT_F11**	\e\eOZ
ALT_LOWER_L	\el	**ALT_F12**	\e\eO[
ALT_LOWER_M	\em	**ALT_F5**	\e\e[15~
ALT_LOWER_N	\en	**ALT_F6**	\e\e[17~
ALT_LOWER_O	\eo	**ALT_F7**	\e\e[18~
ALT_LOWER_P	\ep	**ALT_F8**	\e\e[19~
ALT_LOWER_Q	\eq	**ALT_F9**	\e\e[20~
ALT_LOWER_R	\er	**ALT_F10**	\e\e[21~
ALT_LOWER_S	\es	**ALT_F11**	\e\e[23~
ALT_LOWER_T	\et	**ALT_F12**	\e\e[24~
ALT_LOWER_U	\eu	**ALT_HOME**	\e\e[1~
ALT_LOWER_V	\ev	**ALT_INS**	\e\e[2~
ALT_LOWER_W	\ew	**ALT_DEL**	\e\e[3~
ALT_LOWER_X	\ex	**ALT_END**	\e\e[4~
ALT_LOWER_Y	\ey	**ALT_PGUP**	\e\e[5~
ALT_LOWER_Z	\ez	**ALT_PGDN**	\e\e[6~
ALT_SPACE	\e\040	**ALT_HOME**	\e\e[H
ALT_EXCL	\e!	**ALT_END**	\e\e[F
ALT_QUOTE	\e\"	**ALT_UP**	\e\e[A
ALT_POUND	\e#	**ALT_DOWN**	\e\e[B
ALT_DOLLAR	\e$	**ALT_RIGHT**	\e\e[C
ALT_PERCENT	\e%	**ALT_LEFT**	\e\e[D

VT100+ Codes for the F-Keys

Key	Sequence
F1_KEY	\eOP
F2_KEY	\eOQ
F3_KEY	\eOR
F4_KEY	\eOS
F5_KEY	\eOT
F6_KEY	\eOU
F7_KEY	\eOV
F8_KEY	\eOW
F9_KEY	\eOX
F10_KEY	\eOY
F11_KEY	eOZ
F12_KEY	\eO[

Linux Codes for the F-Keys

Key	Sequence
F5_KEY	\e[15~
F6_KEY	\e[17~
F7_KEY	\e[18~
F8_KEY	\e[19~
F9_KEY	\e[20~
F10_KEY	\e[21~
F11_KEY	\e[23~
F12_KEY	\e[24~
HOME_KEY	\e[1~
INSERT_KEY	\e[2~
DELETE_KEY	\e[3~

Key	Sequence
END_KEY	\e[4~
PG_UP	\e[5~
PG_DOWN	\e[6~

Secure Shell

SSH is a telnet-like program for logging into and for executing commands on a remote machine, which includes security with authentication, encryption, and data integrity features. iLO can support simultaneous access from two SSH clients. After SSH is connected and authenticated, the command line interface is available.

iLO supports:

- SSH protocol version 2
- PuTTY 0.54, which is a free version of telnet and SSH protocol available for download on the Internet. When using PuTTY, versions before 0.54 may display 2 line feeds instead on a single line feed, when the ENTER key is pressed. To avoid this issue and for best results, HP recommends using version 0.54 or later.
- OpenSSH, which is a free version of the SSH protocol available for download on the Internet.

When upgrading the firmware to version 1.60, there will be a one-time 25 minute delay before SSH functionality is available. During this time, iLO generates the 1024 bit RSA and DSA keys. These keys are saved by iLO for future use. If iLO is reset to factory defaults, the RSA and DSA keys are erased and are regenerated on the next boot.

Using Secure Shell

Using SSH

To access iLO using SSH:

1. Open an SSH window.
2. When prompted, enter the IP address or DNS name, login name, and password.

Using OpenSSH

To start an OpenSSH client in Linux, use:

```
ssh -l loginname ipaddress/dns name
```

Using PuTTY

- To start a PuTTY session, double-click the PuTTY icon in directory where PuTTY is installed.
- To Start a PuTTY session from the command line:
  - To start a connection to a server called *host:*

    ```
    putty.exe [-ssh | -telnet | -rlogin | -raw]
    [user@]host
    ```
  - For telnet sessions, the following alternative syntax is supported:

    ```
    putty.exe telnet://host[:port]/
    ```
  - To start an existing saved session called *sessionname:*

    ```
    putty.exe -load "session name"
    ```

iLO Supported SSH Features

The iLO library only supports version 2, SSH-2, of the protocol. The different algorithms supported are:

Feature	
Server host key algorithms	ssh-dsa , ssh-rsa
Encryption (same set supported both ways)	3des-cbc, aes128-cbc
Hashing algorithms	hmac-sha1, hmac-md5
Public key algorithms	ssh-dss, ssh-rsa
Key exchange	Diffie-hellman-group1-sha1
Compression	None

Feature	
Language	English
Client/User authentication method	Password
Authentication timeout	2 minutes
Authentication attempts	3
Default SSH port	22

iLO Shared Network Port

The iLO Shared Network Port enables you to choose either the system NIC or the dedicated iLO NIC for server management. Both regular network traffic and network traffic intended for iLO pass through the system NIC when this feature is selected. The iLO Shared Network Port is only available on a limited number of ProLiant servers, as shown in the "iLO Shared Network Port Requirements (on page 125)" section.

Not all iLO management features are available when using the iLO Shared Network Port. Refer to the "iLO Shared Management Port Features and Restrictions (on page 126)" section for a list of supported and unsupported iLO management features.

iLO Shared Network Port Requirements

The iLO Shared Network Port feature is only available on servers with hardware that supports this feature. In addition to the hardware, both the NIC and iLO firmware must support the feature.

ProLiant Server	**Minimum iLO firmware version**
DL360 G4	1.60
DL380 G4	1.60
ML370 G4	1.60

When using the iLO Shared Network Port, flashing the iLO firmware through the XML interface will take approximately 7 minutes to complete.

iLO Shared Management Port Features and Restrictions

Only the iLO Shared Network Port or the iLO Dedicated Management NIC port can be used for iLO server management at one time. The iLO Shared Network Port and the iLO Dedicated Management NIC port cannot operate simultaneously. Enabling the dedicated iLO NIC disables the iLO Shared Network Port, and enabling the iLO Shared Network Port disables the dedicated iLO NIC.

Disabling the Shared Network Port does not completely disable the system NIC. Regular network traffic still passes through the system NIC. When the Shared Network Port network traffic is disabled any traffic going to or originating from iLO is not passed on to iLO through the shared Network Port because the port is no longer shared with iLO.

The speed of the Shared Network Port is relatively low compared to the dedicated iLO Management Port. Only a limited number of iLO features are supported through the Shared Network Port. These include:

- Command line interface
- XML scripting
- Virtual Serial Port
- Text based Remote Console
- SNMP protocol

Due to the relatively low performance of the Shared Network Port, certain operations performed over the Virtual Serial Port connection may perform at less than optimum levels. In particular, display or text editing operations involving the display of large amounts of data may result in some dropped characters. The loss of characters affects the display only, and does not affect the data stored on the server.

The iLO Web interface is not supported through the Shared Network Port, including:

- Graphical Remote Console
- Virtual Media

When the Shared Network Port is selected, iLO must be configured through either the iLO RBSU or XML. Configuration through RBSU requires that the system be rebooted.

Enabling the iLO Shared Network Port Feature

The iLO Shared Network Port feature is disabled by default. This feature can be enabled through:

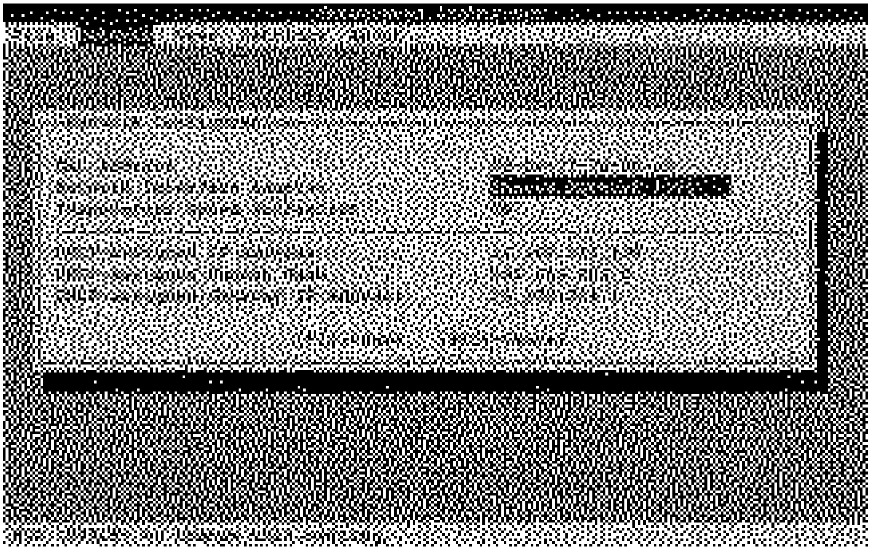
- iLO RBSU
- The iLO Web interface
- XML scripting

When configured for iLO Shared Network Port, iLO's MTU is 320 bytes, and its DHCP request packets are split into multiple packets (using IP fragmentation). This may be a problem if your DHCP server is on a different subnet, and your DHCP relay agent (commonly your Layer 3 Ethernet Switch) does not support forwarding of fragmented DHCP frames. The DHCP server will never receive the DHCP request from iLO, and iLO will not be able to obtain an IP address. In this situation, you must configure iLO with a static IP address.

Enabling the iLO Shared Network Port Feature through iLO RBSU

1. Connect the server's NIC port 1 to a LAN.
2. When prompted during POST, press the **F8** key to enter iLO RBSU.
3. Select **Network>NIC>TCP/IP** and press the **Enter** key.

4. In the Network Configuration menu, toggle the Network Interface Adapter Field to Shared Network Port by pressing the space bar. The Shared Network Port option is only available on supported servers.



5. Press the **F10** key to save the configuration.
6. Select **File>Exit,** and press the **Enter** key.

After iLO resets, the Shared Network Port feature will be active. Any network traffic going to or originating from iLO is directed through the system's NIC port 1.

Enabling the iLO Shared Network Port Feature through the Web Interface

1. Connect iLO NIC port 1 to a LAN.
2. Open a browser, and browse to the iLO IP address or DNS name.
3. Select **Administration>Network Settings.**
4. On the Network Settings page, select **Shared Network Port.** The Shared Network feature is only available on supported servers.
5. Click **Apply** at the bottom of the page.
6. Click **Yes** in the warning dialog box, and click **OK.**

After iLO resets, the Shared Network Port feature will be active. Any network traffic going to or originating from iLO is directed through the system's NIC port 1.

The iLO web interface is no longer available after iLO resets. To restore the use of the web interface, iLO's Dedicated Management NIC port must be re-enabled. Refer to the "Re-enabling the Dedicated iLO management Port (on page 129)" section for more information.

Only the Shared Management NIC Port or the dedicated iLO NIC port is active for server management at one time. They both cannot be enabled at the same time.

Enabling the iLO Shared Network Port Feature through XML Scripting

For information on how to use the SHARED_NETWORK_PORT command to enable the iLO Shared Network Port through XML scripting, refer to the “Remote Insight Command Language (on page 269)” section.

The following sample script configures iLO to select the Shared Network Port. You can tailor this script to your needs. Using this script on platforms that do not support the Shared Network Port will cause an error.

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="WRITE">
   <MOD_NETWORK_SETTINGS>
      <SHARED_NETWORK_PORT VALUE="Y" />
   </MOD_NETWORK_SETTINGS>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

Re-enabling the Dedicated iLO Management Port

The iLO RBSU or XML scripting must be used to re-enable the iLO dedicated NIC management port. For information on how to use the SHARED_NETWORK_PORT command to re-enable the iLO dedicated management port refer to the "Remote Insight Command Language (on page 269)" section. Re-enabling iLO through RBSU requires that the system be rebooted.

To re-enable the dedicated management port:

1. Connect the iLO dedicated management NIC port to a LAN from which the server is managed.
2. Reboot the server.
3. When prompted during POST, press the **F8** key to enter iLO RBSU.
4. Select **Network>NIC>TCP/IP,** and press the **Enter** key.
5. In the Network Configuration menu, toggle the Network Interface Adapter Field to ON by pressing the space bar.
6. Press the **F10** key to save the configuration.
7. Select **File>Exit** and press the **Enter** key.

After iLO resets, the iLO dedicated management NIC Port is active.

The following sample RIBCL script configures iLO to select the iLO Network Port. You can modify this script for your specific needs. Using this script on platforms that do not support the Shared Network Port will cause an error.

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="WRITE">
   <MOD_NETWORK_SETTINGS>
      <SHARED_NETWORK_PORT VALUE="N" />
   </MOD_NETWORK_SETTINGS>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

Command Line Interface

The CLI option on iLO enables you to execute the supported commands from a command line. There are two interfaces through which the CLI option can be accessed:

- Serial port using one connection
- Network using the:

- SSH allowing two simultaneous connections. IP address or DNS name, login name and password are required to start a CLI session using SSH.
- Telnet protocol using three simultaneous connections

All six connections can be active simultaneously. After serial CLI is enabled on the Global Settings screen, the iLO CLI is invoked by entering `ESC (`. The SSH and telnet sessions start the CLI after authentication.

CLI Commands

The following commands are supported in this release of CLI. The same command set is supported through the serial port, the SSH connection, and telnet connection

The privilege level of the logged in user is checked against the privilege required for the command. The command is only executed if the privilege levels match. If the serial and Virtual Serial Port CLI session status is set to Enabled-No Authentication, then all the commands except Remcons are executed without checking the privilege level. The Remote Console Virtual Serial Port session displays the login prompt.

The supported commands are:

- **Escape**
  - `ESC (` invokes the serial CLI connection. This is not necessary for SSH or telnet sessions because they automatically start a CLI session after a successful login.
  - `ESC Q` stops the CLI session and terminates the SSH and telent connection.
  - `ESC R ESC r ESC R` resets the system.
  - `ESC ^` powers on the system.
  - `ESC ESC` erases the current line.

  There is a 1–second timeout for entering any of the escape sequence characters.
- **Help**

The following commands display help messages :

– help

– ?

Entering `help` or `?` displays all the supported commands. Entering `<command help/?>` or `<help/? command>` displays the help message specific to that command.

- **Power**

  The power command is used to change the power state of the server and is limited to users with the Power and Reset privilege.

  – `power` displays the current server power state

  – `power on` turns the server on

  – `power off` turns the server off

  – `power reset` resets the server (server power off followed by server power on)

  – `power warm` warm boots the server

- **UID**

  The UID command is used to change the state of the Unit-ID light on the server.

  – `uid` displays the current Unit-ID state on the server.

  – `uid on` turns the Unit-ID light on.

  – `uid off` turns the Unit-ID light off.

- **NMI**

  The NMI command is used to generate and send an NMI to the server and is limited to users with the Power and Reset privilege.

- **Remcons**

  The remcons command starts a Remote Console session and is limited to users with the Remote Console privilege. Only a text based remote console is supported, similar to a telnet session. When in Remote Console session, enter `<ESC>(` to return to the CLI.

- **Vsp**

  The vsp command invokes a virtual serial port session. When in virtual serial port session, press `<ESC>(` to return to the CLI.

- **Vm**

  The vm command allows Virtual Media scripting commands to be entered at the CLI.

  `vm` *device* `insert` *path* inserts an image.

  `vm` *device* `eject` ejects an image.

  `vm` *device* `get` gets the status of the Virtual Media.

  `vm` *device* `set boot` *access*—sets the status of the virtual media

  Command options:

  – Valid device names are `floppy` or `cdrom`.

  – The path is the URL to the media image.

  – Boot options are `boot_once`, `boot_always`, no_boot, `connect` or `disconnect`.

  – Access options are `write_protect` or `write_allow`.

  Please refer to the commands INSERT_VIRTUAL_MEDIA, EJECT_VIRTUAL_MEDIA, GET_VM_STATUS, and SET_VM_STATUS in the "Remote Insight Command Language (on page 269)" section for more details on how to use these commands.

  Composite Virtual Media is not supported using the CLI. You must specify Virtual Media images. Refer to the "Virtual Media Scripting (on page 79)" section for more information.

- **Exit**

  The exit command stops the CLI session and terminates the SSH connection.

iLO Security

In This Section

Security Features

iLO provides the following security features:

- User-defined TCP/IP ports ("Network Settings" on page 91)
- User actions logged in the iLO Event Log
- Progressive delays for failed login attempts ("Login Security" on page 138)
- Support for X.509 CA signed certificates (on page 140)
- Support for RBSU settings ("Global Security Settings" on page 139)
- Support for optional LDAP-based directory services authentication and authorization (requires iLO Advanced)
- Encrypted communication using SSL and SSH.

General Security Guidelines

The following are general guidelines concerning security for iLO:

- For maximum security, iLO should be set up on a separate management network.

- iLO should not be connected directly to the Internet.
- A 128-bit cipher strength browser must be used.

Encryption

iLO provides strong security for remote management in distributed IT environments by using 128-bit SSL encryption of HTTP data transmitted across the network. SSL encryption ensures that the HTTP information is secure as it travels across the network.

Remote Console data is protected using 128-bit RC4 bidirectional encryption.

iLO Security Override Switch Administration

The iLO Security Override Switch allows the administrator full access to the iLO processor. This access may be necessary for any of the following conditions:

- iLO must be re-enabled after it has been disabled.
- All user accounts with the Administer User Accounts privilege have been locked out.
- A bad configuration keeps the iLO from displaying on the network and RBSU has been disabled.
- The boot block must be flashed.

Ramifications of setting the Security Override Switch include:

- All security authorization checks are disabled while the switch is set.
- iLO RBSU runs if the host server is reset.
- iLO is not disabled and might display on the network as configured.
- iLO, if disabled while the Security Override Switch is set, does not log the user out and complete the disable process until the power is cycled on the server.
- iLO Option ROMPaq is allowed to reprogram the iLO ROM even if the iLO firmware is not running.

- The boot block is exposed for programming.

A warning message is displayed on iLO browser pages indicating that the iLO Security Override Switch is currently in use. An iLO log entry records the use of the iLO Security Override Switch. An SNMP alert can also be sent upon setting or clearing the iLO Security Override Switch.

Setting the iLO Security Override Switch also enables you to flash the iLO boot block. HP does not anticipate that you will need to update the iLO boot block. If an iLO boot block update is ever required, physical presence at the server will be required to reprogram the boot block and reset iLO. The boot block will be exposed until iLO is reset. For maximum security, HP recommends that you disconnect the iLO from the network until the reset is complete. The iLO Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure.

To set the iLO Security Override Switch:

1. Power off the server.
2. Set the switch.
3. Power on the server.

Reverse the procedure to clear the iLO Security Override Switch.

Depending on the server, the iLO Security Override Switch might be a single jumper or a specific switch position on a dip switch panel. To access and locate the iLO Security Override Switch, refer to the server documentation. The iLO Security Override Switch can also be located using the diagrams on the server access panel.

User Accounts

iLO supports the configuration of up to 12 local user accounts. Each of these accounts can be managed through the use of the following features:

- Privileges
- Global Security Settings
- Login Security

An alternative to local iLO user accounts is to integrate iLO user authentication into directory services. This configuration allows a virtually unlimited number of users, and easily scales to the number of Lights-Out devices in an enterprise. Additionally, the directory provides a central point of administration for Lights-Out devices and users, and the directory can enforce a stronger password policy. iLO enables you to use local users, directory users, or both.

Privileges

iLO allows the administrator to control user account access to iLO functions through the use of privileges. When a user attempts to use a function, the iLO system verifies that the user has the privilege before the user is allowed to perform the function.

Each feature available through iLO can be controlled through privileges, including Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO Settings. Privileges for each user can be configured on the User Administration page of the Administration tab.

Login Security

iLO provides several login security features. After an initial failed login attempt, iLO imposes a delay of five seconds. After a second failed attempt, iLO imposes a delay of 10 seconds. After the third failed attempt, and any subsequent attempts, iLO imposes a delay of 60 seconds. All subsequent failed login attempts cycles through these values. An information page is displayed during each delay. This will continue until a valid login is completed. This feature assists in defending against possible dictionary attacks against the browser login port.

iLO saves a detailed log entry for failed login attempts, which imposes a delay of 60 seconds.

Global Security Settings

Global security settings allow the administrator to control access to functions or to control specific actions of functions that have been enabled globally. For example, you can control access to iLO RBSU, enable or disable Lights-Out Functionality, set the Remote Console timeout, Web server SSL and non-SSL ports, virtual media port, and set the minimum password length.

Password Guidelines

The following is a list of recommended password guidelines. Passwords should:

- Never be written down or recorded
- Never be shared with others
- Not be words generally found in a dictionary, or easy to guess words, such as the company name, product names, the user's name, or the user's User ID
- Include at least three of the four following characteristics:
  - At least one numeric character
  - At least one special character
  - At least one lowercase character
  - At least one uppercase character

Passwords issued for a temporary user ID, password reset, or a locked-out user ID should also conform to these standards. Each password must be a minimum length of zero characters and a maximum length of 39 characters. The default minimum length is set to eight characters. Setting the minimum password length to fewer than eight characters is not recommended unless you have a physically secure management network that does not extend outside the secure data center.

Certificates

By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables the iLO to work without any additional configuration steps. The security features of the iLO can be enhanced by importing a trusted certificate.

- **Create Certificate Request**—iLO can create a CR (in PKCS #10 format), which can be sent to a CA. This certificate request is base64 encoded. A CA processes this request and returns a response (X.509 certificate) that can be imported into iLO.

  The CR contains a public/private key pair that is used for validation of communications between the client browser and iLO. The generated CR is held in memory until either a new CR is generated, a certificate is imported by this process, or the iLO is reset, which means you can generate the CR and copy it to the client clipboard, leave the iLO website to retrieve the certificate, then return to import the certificate.

  When submitting the request to the CA, be sure to:

  – Use the iLO name as listed on the System Status screen as the URL for the server.

  – Request the certificate be generated in the RAW format.

  – Include the `Begin` and `End` certificate lines.

  Every time you click **Create Certificate Request**, a new certificate request is generated even though the iLO name is same.

- **Import Certificate**—If you are returning to the Create Certificate Request page with a certificate to import, click **Import Certificate** to go directly to the Certificate Import screen without generating a new CR. This is important in that a given certificate only works with the keys contained in the CR from which the certificate was generated. If the iLO has been reset or another CR has been generated since the CR that was used to request the certificate was generated, then another CR must be generated and a new certificate procured from the CA.

Securing RBSU

The iLO RBSU allows user access for viewing and modifying the iLO configuration. RBSU access settings can be configured using RBSU, browser, RIBCL scripts, and the iLO Security Override Switch. RBSU has three levels of security:

- RBSU Disabled (most secure)

  If iLO RBSU is disabled, user access is prohibited. This prevents modification using the RBSU interface.

- RBSU Login Required (more secure)

  If RBSU login is required, then the active configuration menus are controlled by the authenticated user's access rights.

- RBSU Login Not Required (default)

  Anyone with access to the host during POST may enter the iLO RBSU to view and modify configuration settings. This is an acceptable setting if host access is controlled.

Directory Services

In This Section

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.
- Anonymity (lack thereof)—In some environments, users share Lights-Out accounts, which results in the lack of knowing who performed an operation, instead of knowing what account (or role) was used.
- 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 applies to all users and Lights-Out devices associated with that role.

- Single point of administration—You can use native administrative tools like MMC and ConsoleOne to administrate Lights-Out users.
- Immediacy—A single change in the directory rolls-out immediately to associated Lights-Out processors. This eliminates the need to script this process.
- Elimination of another 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 Lights-Out.
- Flexibility—You can create a single role for a single user on a single iLO, or you can create a single role for multiple users on multiple iLOs, or you can use a combinations of roles as is suitable for your enterprise.
- Compatibility—Lights-Out directory integration applies to iLO, RILOE and RILOE II products. The integration supports the popular Active Directory and eDirectory.
- Standards—Lights-Out directory support builds on top of the LDAP 2.0 standard for secure directory access.

Features Supported by Directory Integration

iLO 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 iLO management processors and iLO users.

Installing Directory Services for iLO requires extending the directory schema. Extending the schema must be completed by a Schema Administrator.

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

> **NOTE:** When connected through the Diagnostics Port, the directory server is not available. You can log in using a local account only.

Installing Directory Services

To successfully enable directory-enabled management on any Lights-Out management processor:

1. Plan

   Review the following sections:

   – "Directory Services (on page 143)"

   – "Directory Services Schema (on page 353)"

   – "Directory-Enabled Remote Management (on page 193)"

2. Install

   a. Download the HP Lights-Out Directory Package containing the schema installer, the management snap-in installer, and the migrations utilities from the HP website (http://www.hp.com/servers/lights-out).

   b. Run the schema installer (on page 148) once to extend the schema.

   c. Run the management snap-in installer (on page 152) and install the appropriate snap-in for your directory service on one or more management workstations.

3. Update

   a. Flash the ROM ("Upgrade iLO Firmware" on page 98) on the Lights-Out management processor with the directory-enabled firmware.

   b. Set directory server settings and the distinguished name of the management processor objects on the Directory Settings page in the iLO GUI.

4. Manage

   a. Create a management device object and a role object ("Directory Services Objects" on page 162) 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, refer to "Directory-Enabled Remote Management (on page 193)." Examples are available in the "Directory Services for Active Directory (on page 153)" and "Directory Services for eDirectory (on page 171)" sections.

5. Handle exceptions
   - Lights-Out migration utilities are easier to use with a single Lights-Out role. If you plan on creating multiple roles in the directory, you might need to use directory scripting utilities, like LDIFDE or VB script to create complex role associations. Refer to the "Using Bulk Import Tools (on page 194)" for more information.
   - If you have iLO or RILOE processors with old firmware, you might need to manually update the firmware using a browser. Minimum firmware requirements for remote firmware update using RIBCL and directory migration utility are:

LOM Product	Minimum Supported Firmware
RILOE	2.41
RILOE II	All versions
iLO	1.10

After the schema has been extended, you can complete the directory services setup by using HP Lights-Out Directories Migration Utilities (on page 205). The migration utilities are included in the HP Lights-Out Directory Package. Version 1.13 of the Directories Migration Utility allows Lights-Out import and export and supports different user credentials for each Lights-Out processor.

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, refer to "Directory Services Schema (on page 353)."

Directory Services Support

iLO supports the following directory services:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.6.2
- Novell eDirectory 8.7

iLO software is designed to run within the Microsoft® Active Directory Users and Computers and Novell ConsoleOne management tools, enabling 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™ 1.4.0 or later for SSL authentication.

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

- Windows® 2000 family
- Windows® Server 2003 family

iLO supports eDirectory 8.6.2 and 8.7 running on one of the following operating systems:

- Windows® 2000 family
- Windows® Server 2003 family
- NetWare 5.X
- NetWare 6.X
- Red Hat Enterprise Linux AS 2.1
- Red Hat Linux 7.3
- Red Hat Linux 8.0

eDirectory Installation Prerequisites

Directory Services for iLO uses LDAP over SSL to communicate with the directory servers. iLO software is designed to install in an eDirectory version 8.6.1 (and above) tree. HP does not recommend installing this product if you have eDirectory servers with a version less than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, you should read and have available the following technical information documents, available at Novell Support (http://support.novell.com).

Installing Directory Services for iLO requires extending the eDirectory schema. Extending the schema must be completed by an Administrator.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility*
- TID10057565 *Unknown objects in a mixed environment*
- TID10059954 *How to test whether LDAP is working correctly*
- TID10023209 *How to configure LDAP for SSL (secure) connections*
- TID10075010 *How to test LDAP authentication*

Schema Required Software

iLO requires specific software, which will extend the schema and provide snap-ins to manage the iLO network. An HP Smart Component is available for download that contains the schema installer and the management snap-in installer. The HP Smart Component can be downloaded from the HP website (http://www.hp.com/servers/lights-out).

Schema Installer

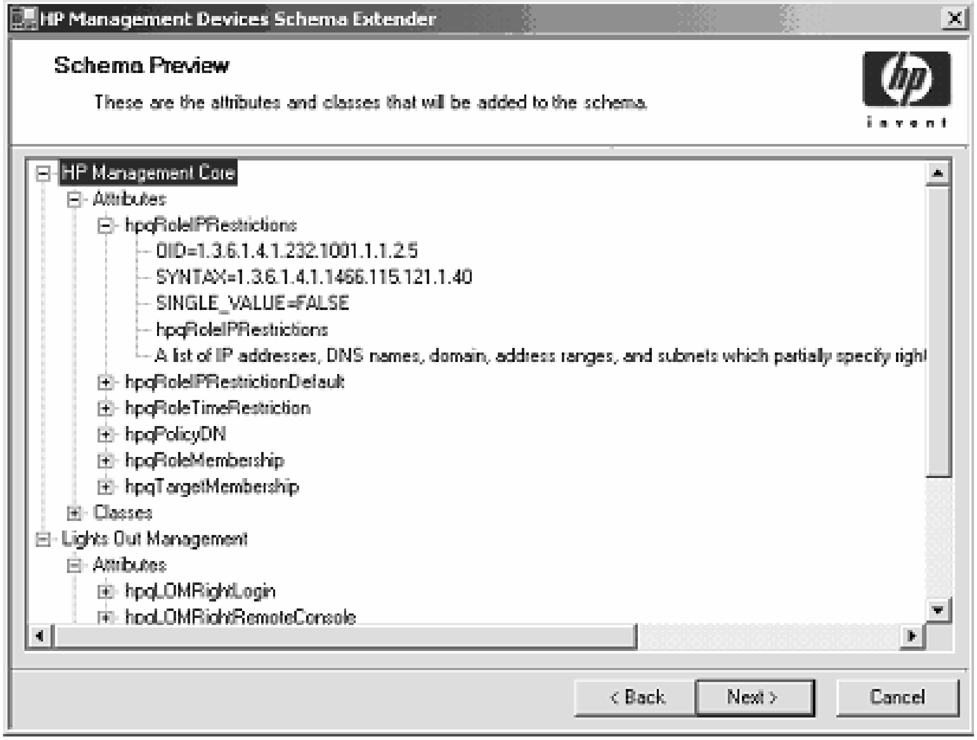
Bundled with the schema installer are one or more .xml files. These files contain the schema that will be added to the directory. Typically, one of these files will contain core schema that is common to all the supported directory services. Additional files contain only product-specific schemas. The 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 enables the user 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 will be installed.



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 right
        ⊞ hpqRoleIPRestrictionDefault
        ⊞ hpqRoleTimeRestriction
        ⊞ hpqPolicyDN
        ⊞ hpqRoleMembership
        ⊞ hpqTargetMembership
    ⊞ Classes
⊟ Lights Out Management
    ⊟ Attributes
        ⊞ hpqLOMRightLogin
        ⊞ hpqLOMRightRemoteConsole
```

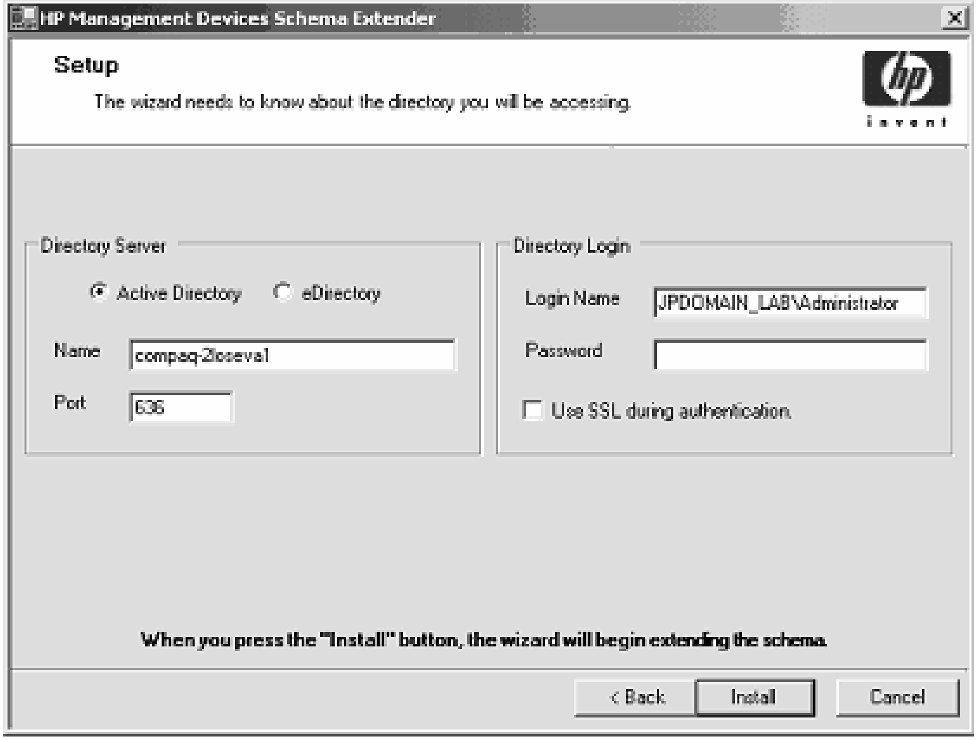
Setup

The Setup screen is used to enter the appropriate information before extending the schema.

The Directory Server section of the Setup screen enables you to select whether you will be using 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 the user be an authenticated Schema Administrator, that the schema is not write protected, and the directory is the FSMO role owner in the tree. The installer will attempt to make the target directory server the FSMO Schema Master of the forest.
>
> To get write access to the schema on Windows® 2000 requires a change to the registry safety interlock. If the user selects the **Active Directory** option, the schema extender will attempt to make the registry change. It will only succeed if the user has 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 might 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 will proceed using an unencrypted (clear text) connection.



HP Management Devices Schema Extender

Setup

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

Directory Server

● Active Directory ○ eDirectory

Name: compaq-2loseval

Port: 636

Directory Login

Login Name: JPDOMAIN_LAB\Administrator

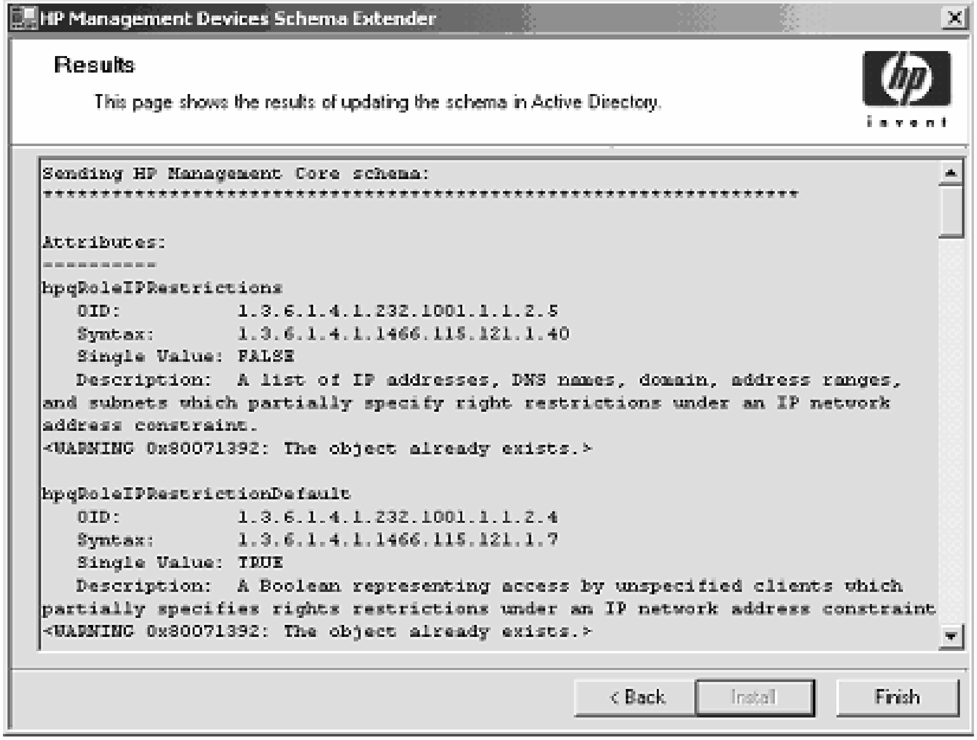
Password:

□ Use SSL during authentication.

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

Results

The Results screen displays the results of the installation, including whether the schema could be extended and what attributes were changed.



HP Management Devices Schema Extender
Results
This page shows the results of updating the schema in Active Directory.
invent
< Back
Install
Finish

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

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

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

Management Snap-In Installer

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

iLO snap-ins are used to perform the following tasks in creating an iLO directory:

- Creating and managing the iLO and role objects (policy objects will be supported at a later date)

- Making the associations between iLO objects and the role (or policy) objects

Directory Services for Active Directory

The following sections provide installation prerequisites, preparation, and a working example of 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 website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Active Directory Installation Prerequisites

- The Active Directory must have a digital certificate installed to allow iLO to connect securely over the network.
- The Active Directory must have the schema extended to describe Lights-Out object classes and properties.
- The Integrated Lights-Out firmware must be version 1.40 or later.
- iLO Advanced features must be licensed.

  You can evaluate iLO Advanced with a free evaluation license key that you can download from the HP website (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html).

Directory Services for iLO 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 iLO requires extending the Active Directory schema. Extending the schema must be completed by an Active Directory Schema Administrator.

- *Extending the Schema* in the Microsoft® Windows® 2000 Server Resource Kit, available at http://msdn.microsoft.com (http://msdn.microsoft.com)
- *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit
- Microsoft® Knowledge Base Articles

These articles are accessed using the Knowledge Base Article ID Number Search option at Microsoft® website (http://support.microsoft.com/).

- 216999 *Installing the Remote Server Administration Tools in Windows® 2000*
- 314978 *Using the Adminpak.msi to Install a Server Administration Tool in Windows® 2000*
- 247078 *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers*
- 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority*
- 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed*

iLO requires a secure connection to communicate with the directory service. This requires the installation of the Microsoft® CA. Refer to the following Microsoft® technical references:

- Appendix D—Configuring Digital Certificates on Domain Controllers for Secure LDAP and SMTP Replication (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 iLO management processors:

1. Install Active Directory. For more information, refer to *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit.
2. Install the Microsoft® Admin Pack (the ADMINPAK.MSI file, which is located in the i386 subdirectory of the Windows® 2000 Server or Advance Server CD). For more information, refer to the Microsoft® Knowledge Base Article 216999.

3. In Windows® 2000, the safety interlock that prevents accidental writes to the schema must be temporarily disabled. The schema extender utility can do this if the remote registry service is running and the user has sufficient rights. This can also be done by setting `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesParameters\Schema Update Allowed` in the registry to a non-zero value (refer to the "Order of Processing When Extending the Schema" section of *Installation of Schema Extensions* in the Windows® 2000 Server Resource Kit) or by the following steps. This step is not necessary if you are using Windows® Server 2003.

   IMPORTANT: Incorrectly editing the registry can severely damage your system. HP recommends creating a back up 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 might need to be expanded for the checkbox to be available.

4. Create a certificate or install Certificate Services. This step is necessary to create a certificate or install Certificate Services because iLO communicates with Active Directory using SSL. Active Directory must be installed before installing Certificate Services.

5. To specify that a certificate be issued to the server running active directory:

   a. Launch Microsoft® Management Console on the server and add the default domain policy snap-in (Group Policy, then browse to Default domain policy object).

   b. Click **Computer Configuration>Windows Settings>Security Settings>Public Key Policies.**

   c. Right-click **Automatic Certificate Requests Settings,** and select **new>automatic certificate request.**

   d. Using the wizard, select the domain controller template, and the certificate authority you want to use.

6. Download the Smart Component, which contains the installers for the schema extender and the snap-ins. The Smart Component can be downloaded from the HP website (http://www.hp.com/servers/lights-out).
7. Run the schema installer application to extend the schema, which extends the directory schema with the proper HP objects.

   The schema installer associates the Active Directory snap-ins with the new schema. The snap-in installation setup utility is a Windows® MSI setup script and will run anywhere MSI is supported (Windows® XP, Windows® 2000, Windows® 98). However, some parts of the schema extension application require the .NET Framework, which can be downloaded from the Microsoft® website (http://www.microsoft.com).

Snap-In Installation and Initialization for Active Directory

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

   For more information on iLO objects, refer to "Directory Services Objects (on page 162)."

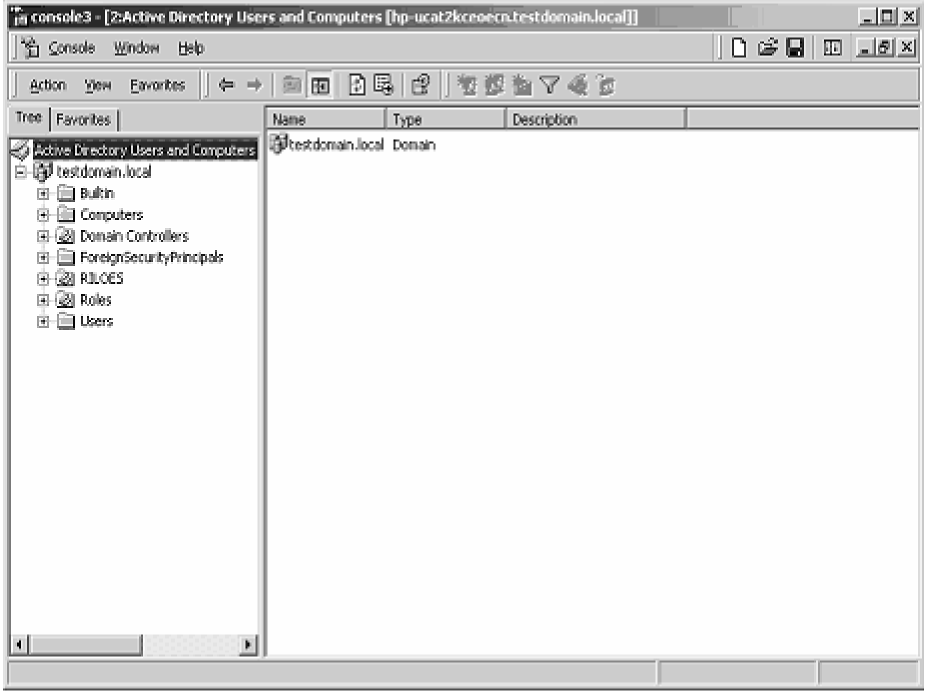
At a minimum, you must create:

- One Role object that will contain one or more users and one or more iLO objects.
- One iLO object corresponding to each iLO management processor that will be using the directory.

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

The following example shows how to set up roles and HP devices in an enterprise directory with the domain *testdomain.local*, which consists of two organizational units, *Roles* and *RILOES*.

Assume that a company has an enterprise directory including the domain *testdomain.local,* arranged as shown in the following screen.



1. Create an organizational unit, which will contain the Lights-Out Devices managed by the domain. In this example, two organizational units are created called *Roles* and *RILOES.*
2. Use the HP provided Active Directory Users and Computers snap-ins to create Lights-Out Management objects in the *RILOES* organizational unit for several iLO devices.

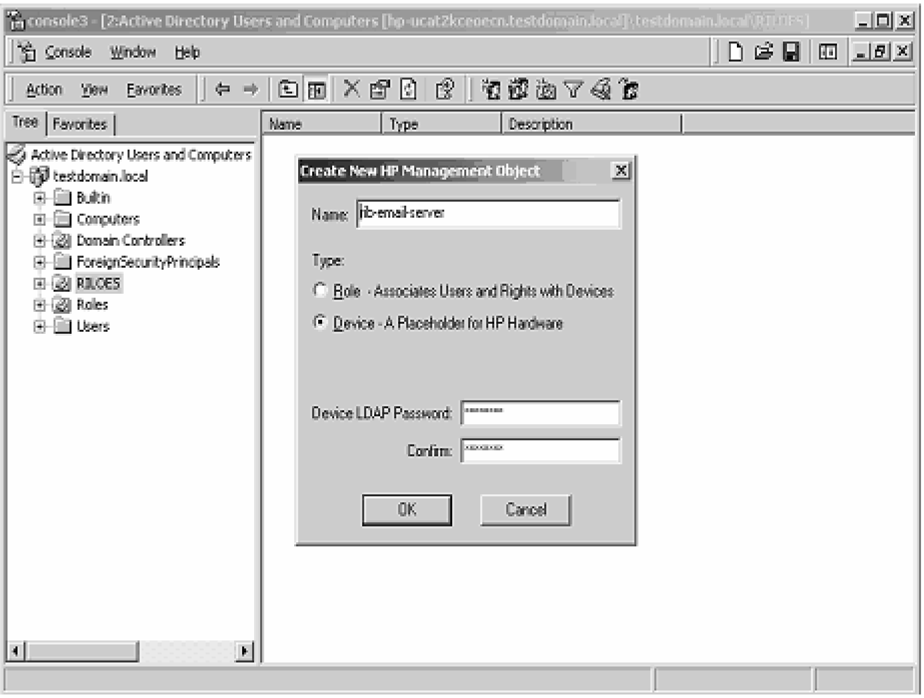
a. Right-click the RILOES organizational unit found in the *testdomain.local* domain, and select **NewHPObject.**

b. Select **Device** for the type on the Create New HP Management Object dialog box.

c. Enter an appropriate name in the Name field of the dialog box. In this example, the DNS host name of the iLO device, *rib-email-server,* will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII*.

d. Enter and confirm a password in the Device LDAP Password and Confirm fields. The device will use this password to authenticate to the directory, and should be unique to the device. This password is the password that is used in the Directory Settings screen of the iLO.

e. Click **OK.**



Create New HP Management Object

Name: rib-email-server

Type:

○ Role - Associates Users and Rights with Devices

● Device - A Placeholder for HP Hardware

Device LDAP Password: ********

Confirm: ********

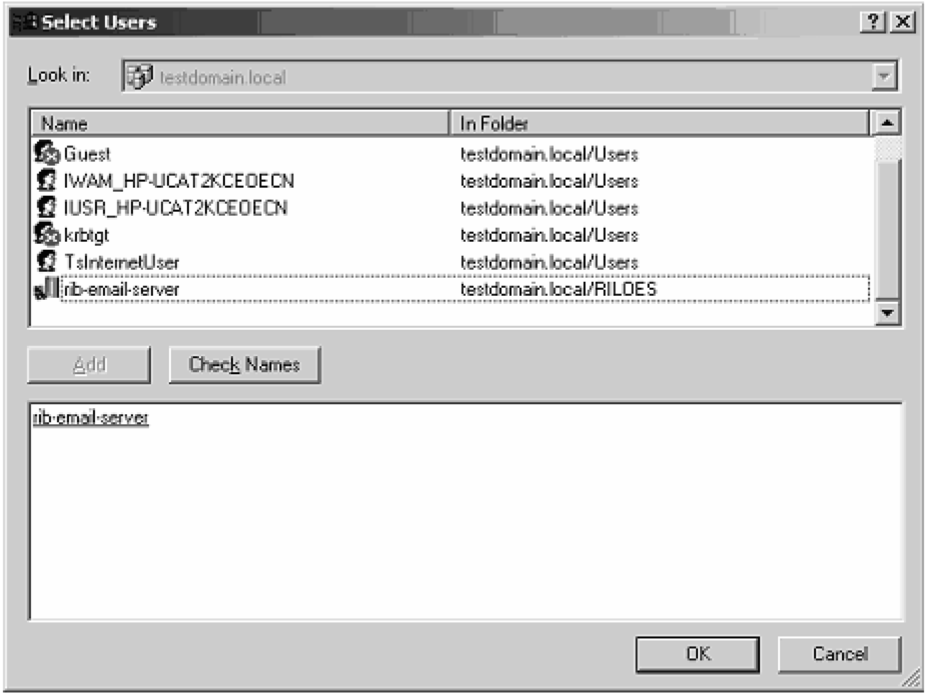
console3 - [2:Active Directory Users and Computers [hp-ucat2kceoecn.testdomain.local]\testdomain.local\RILOES]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Name
Type
Description
Active Directory Users and Computers
testdomain.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
RILOES
Roles
Users
OK
Cancel

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

   a. Right-click the Roles organizational unit, select **New** then **Object.**
   b. Select **Role** for the type field in the Create New HP Management Object dialog box.
   c. Enter an appropriate name in the Name field of the New HP Management Object dialog box. In this example, the role will contain users trusted for remote server administration and will be called *remoteAdmins*. Click **OK.**
   d. Repeat the process, creating a role for remote server monitors called *remoteMonitors*.

4. 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 *testdomain.local* domain, and select **Properties.**
   b. Select the **HP Devices** tab, then click **Add.**

c. Using the Select Users dialog box, select the Lights-Out Management object created in step 2, *rib-email-server* in folder testdomain.local/RILOES. Click **OK** to close the dialog, then click **Apply** to save the list.

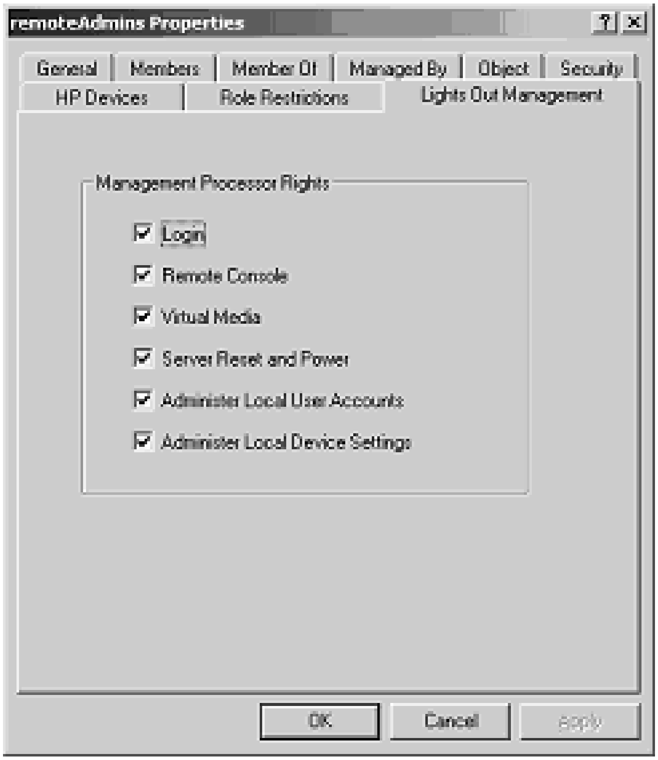


Look in: testdomain.local

Name	In Folder
Guest	testdomain.local/Users
IWAM_HP-UCAT2KCEOECN	testdomain.local/Users
IUSR_HP-UCAT2KCEOECN	testdomain.local/Users
krbtgt	testdomain.local/Users
TsInternetUser	testdomain.local/Users
rib-email-server	testdomain.local/RILOES

rib-email-server

d. 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.



Management Processor Rights

☑ Login

☑ Remote Console

☑ Virtual Media

☑ Server Reset and Power

☑ Administer Local User Accounts

☑ Administer Local Device Settings

5. Use the Lights Out Management tab to set the rights for the role. All users and groups within a role will have the rights assigned to the role on all of the iLO devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the iLO functionality. Select the boxes next to each right, and then click **Apply.** Click **OK** to close the property sheet.

6. Using the same procedure as in step 4, edit the properties of the *remoteMonitors* role, add the *rib-email-server* device to the Managed Devices list on the HP Devices tab, and add users to the *remoteMonitors* role using the Members tab. Then, on the Lights Out Management tab, select the box next to the Login. Click **Apply** and **OK.** Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any iLO 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 is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure iLO and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the Directory Settings screen.

```
RIB Object DN = cn=rib-email-
server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 =
cn=Users,dc=testdomain,dc=local
```

For example, to gain access, user *Mel Moore*, with the unique ID *MooreM*, located in the users organizational unit within the *testdomain.local* domain, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the iLO. They would enter `testdomain\moorem`, or `moorem@testdomain.local`, or `Mel Moore`, in the Login Name field of the iLO login screen, and use their Active Directory password in the Password field of that screen.

Directory Services Objects

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and user or groups already contained within the directory service. User management of iLO requires three basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

NOTE: After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

After the snap-in is installed, iLO objects and iLO roles can be created in the directory. Using the Users and Computers tool, the user will:

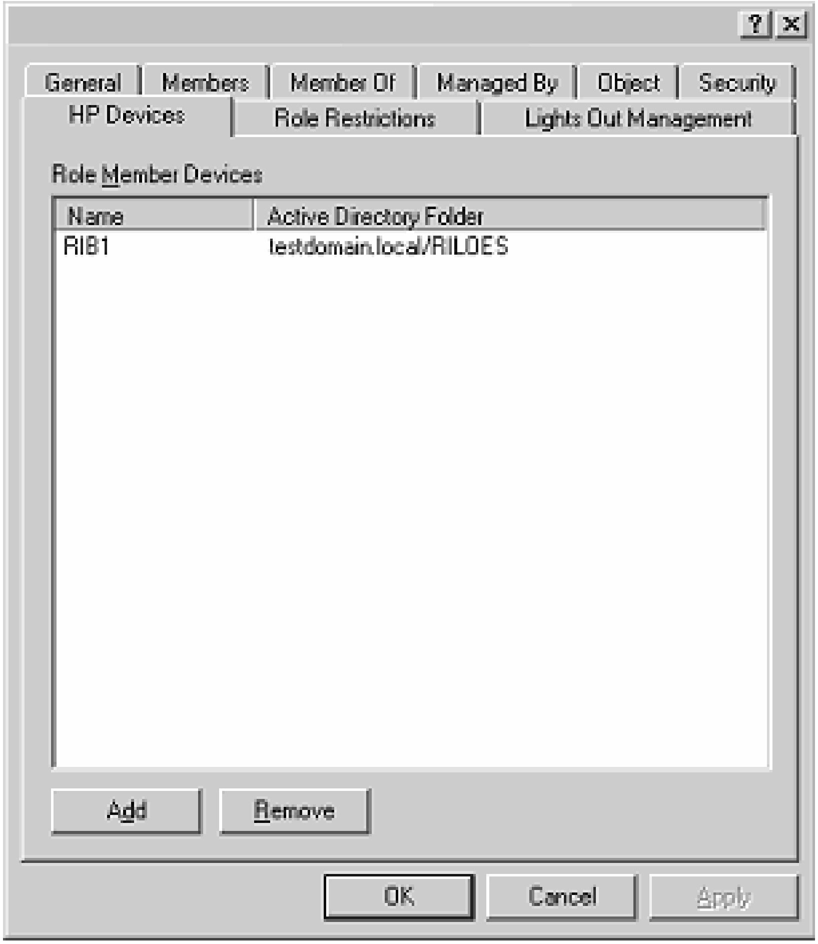
- Create iLO and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

Active Directory Snap-Ins

The following sections discuss the additional management options available within Active Directory Users and Computers after the HP snap-ins have been installed.

HP Devices

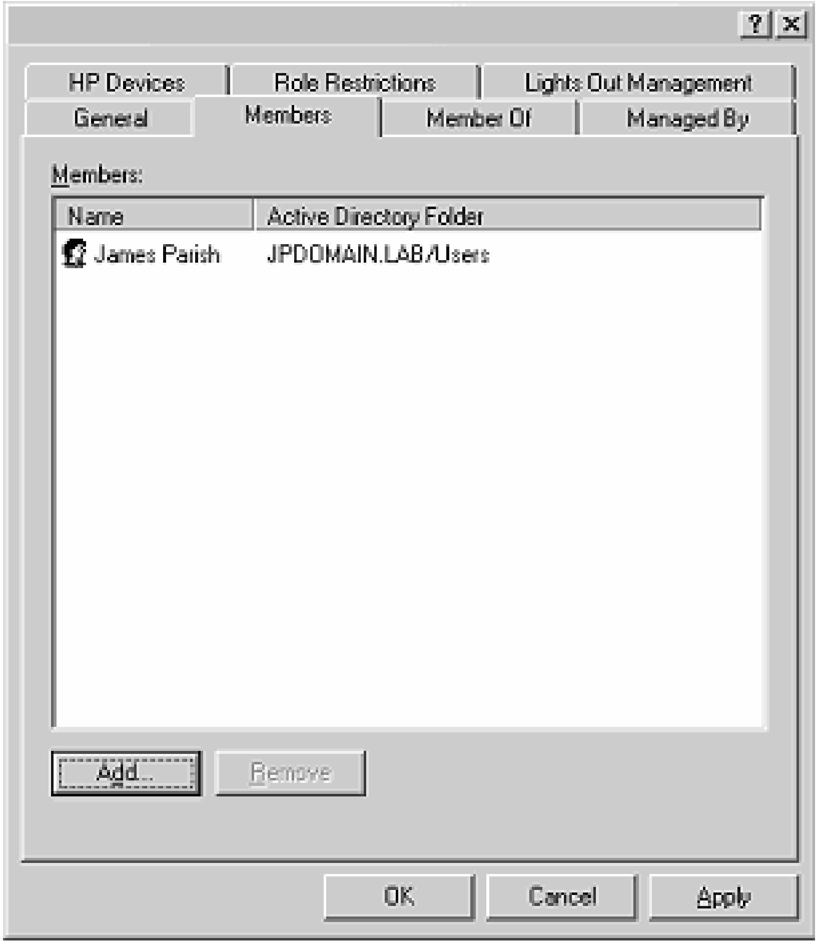
The HP Devices tab is used to add the HP devices to be managed within a role. Clicking **Add** enables you to browse to a specific HP device and add it to the list of member devices. Clicking **Remove** enables you to browse to a specific HP device and remove it from the list of member devices.



Name	Active Directory Folder
RIB1	testdomain.local/RILOES

Members

After user objects are created, the Members tab enables you to manage the users within the role. Clicking **Add** enables you to browse to the specific user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.

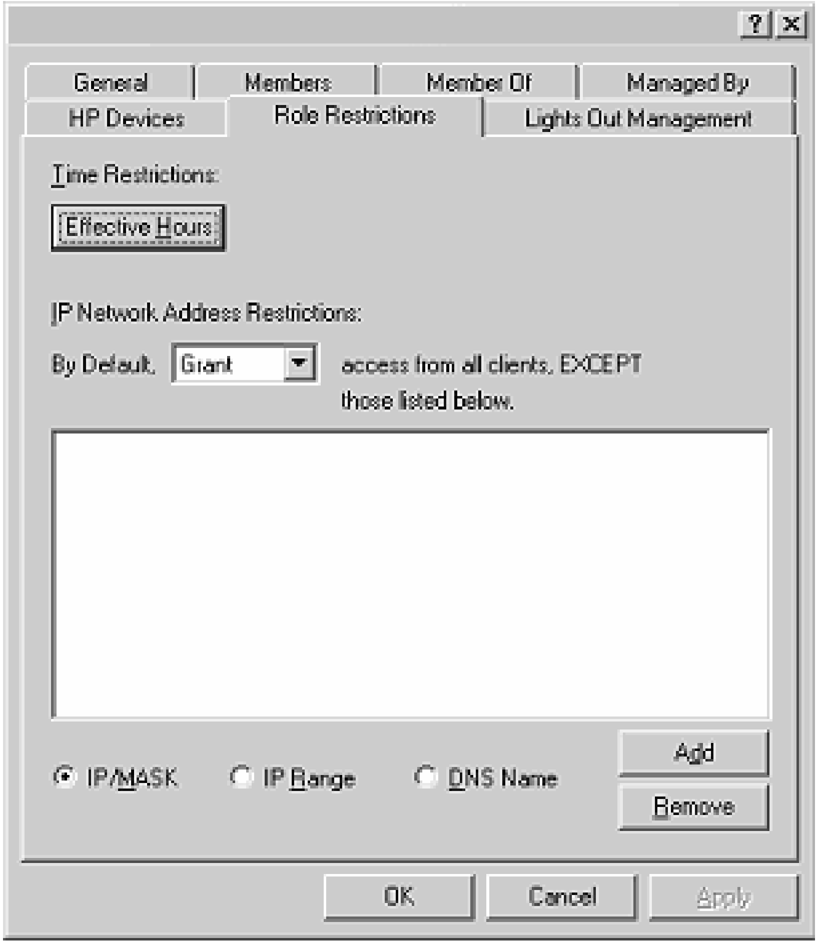


Name	Active Directory Folder
James Parish	JPDOMAIN.LAB/Users

Active Directory Role Restrictions

The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

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



Time Restrictions:

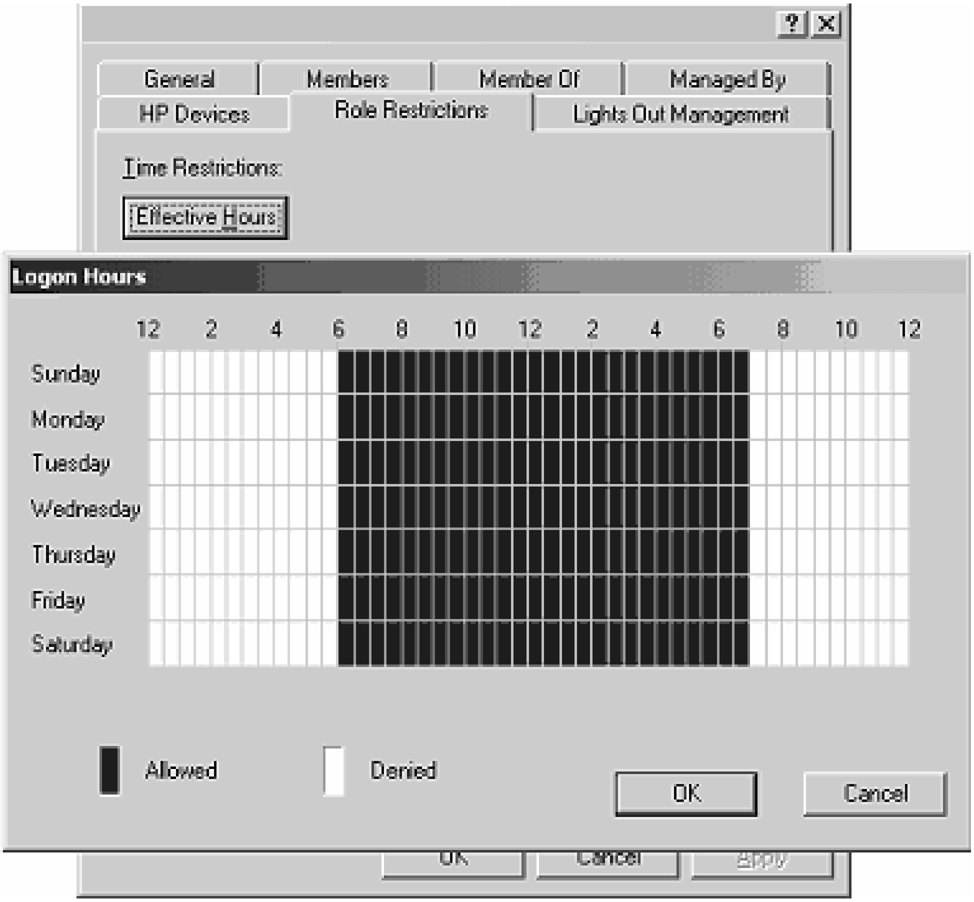
IP Network Address Restrictions:

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

● IP/MASK ○ IP Range ○ DNS Name

Time Restrictions

You can manage the hours available for logon by members of the role by clicking **Effective Hours** in the Role Restrictions tab. In the Logon Hours pop-up window, you can select the times available for logon for each day of the week in half-hour increments. 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. The default setting is to allow access at all times.



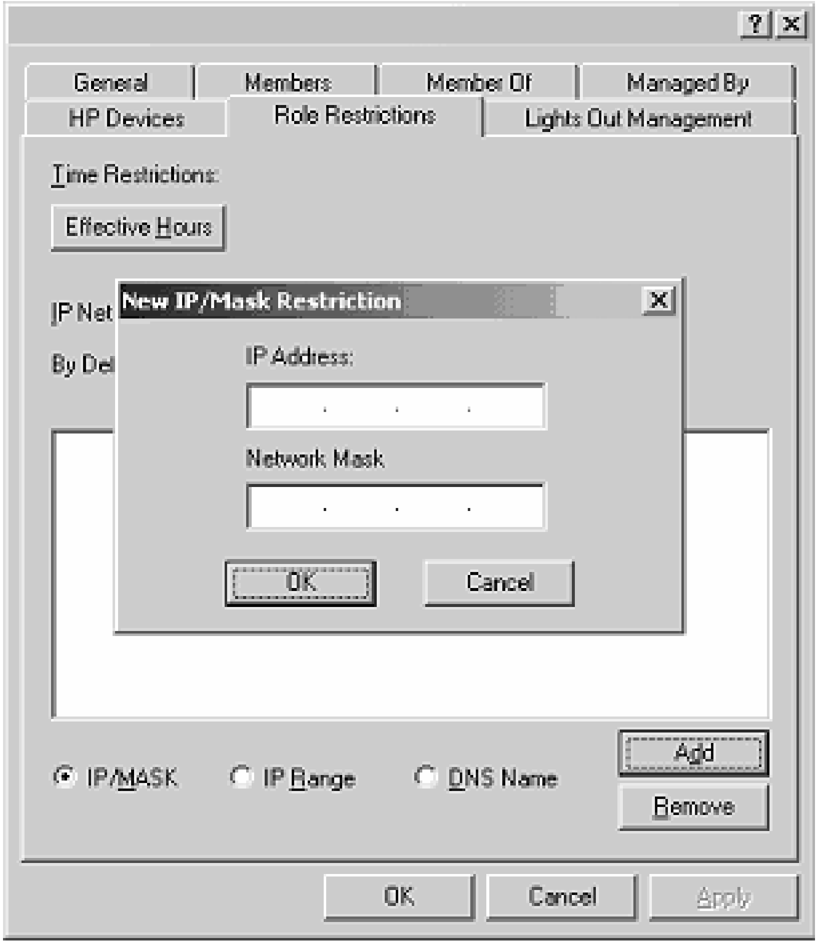
Enforced Client IP Address or DNS Name Access

Access can be granted or denied to an IP address, IP address range, or DNS names.

1. 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.
2. Select the addresses to be added, select the type of restriction, and click **Add.**
3. In the new restriction pop-up window, enter the information and click **OK.** The new restriction pop-up window displays.

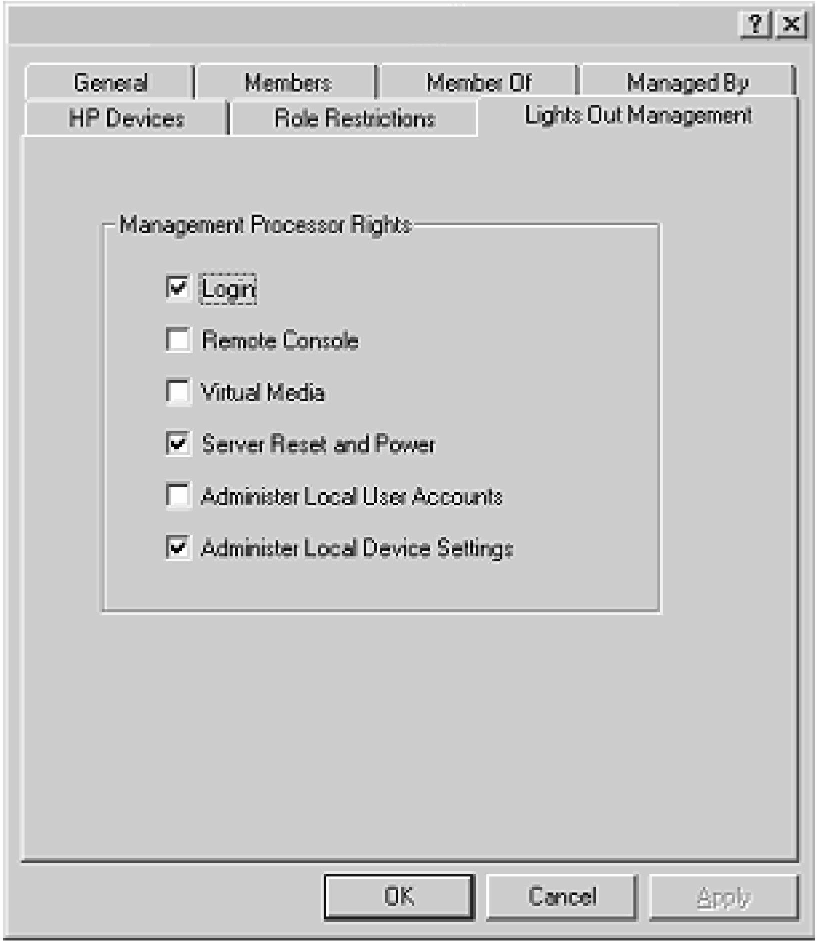
   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com.
4. Click **OK** to save the changes.

To remove any of the entries, highlight the entry in the display list and click **Remove.**



Active Directory Lights-Out Management

After a role is created, rights for the role can be selected. Users and group objects can now be made members of the role, giving the users or group of users the rights granted by the role. Rights are managed on the Lights Out Management 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:

- **Login**—This option controls whether users can log in to the associated devices.
- **Remote Console**—This option enables the user access to the Remote Console.
- **Virtual Media**—This option enables the user access to the iLO virtual media functionality.
- **Server Reset and Power**—This option enables the user access to the iLO Virtual Power button to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option enables the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—This option enables the user to configure the iLO management processor settings. These settings include the options available on the Global Settings, Network Settings, SNMP Settings, and Directory Settings screens of the iLO Web browser.

Directory Services for eDirectory

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

Snap-in Installation and Initialization for eDirectory

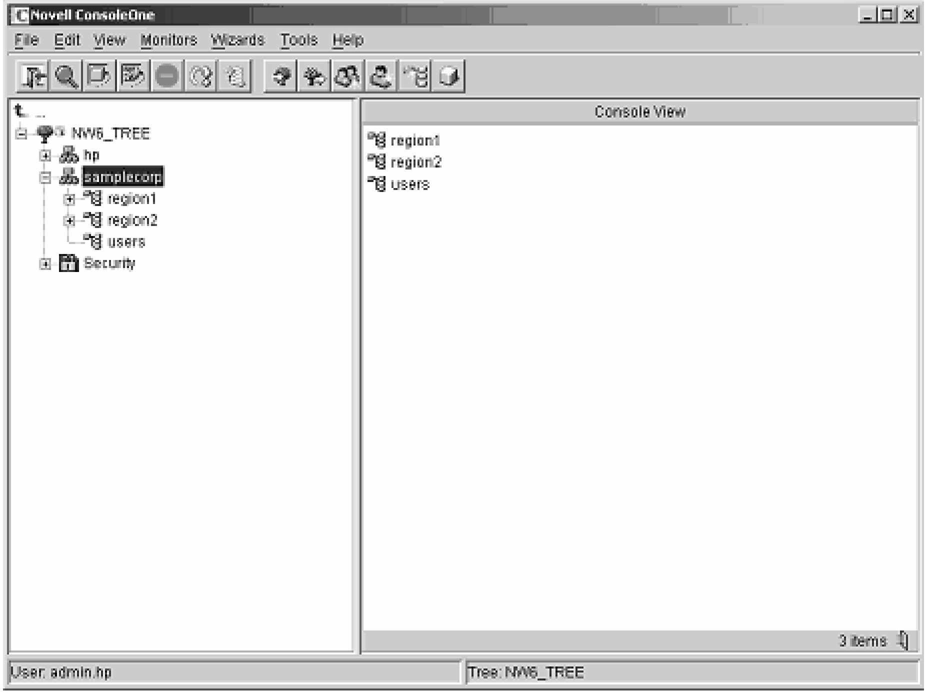
Refer to "Snap-In Installation and Initialization ("Snap-In Installation and Initialization for Active Directory" on page 156)" for step-by-step instructions on using the snap-in installation application.

NOTE: After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

Example: Creating and Configuring Directory Objects for Use with LOM 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*.

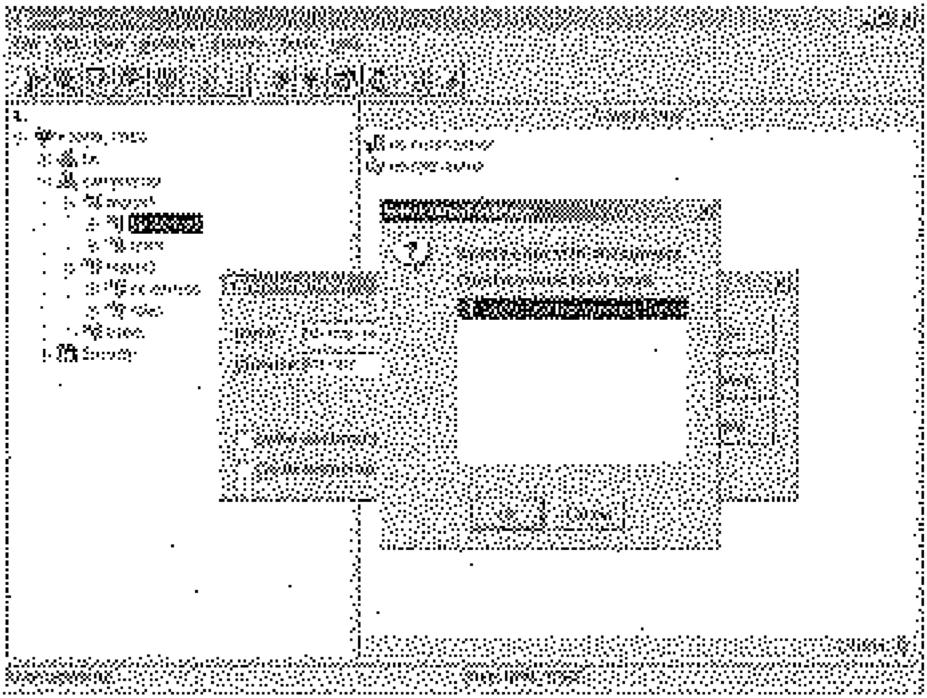
Assume *samplecorp* has an enterprise directory arranged according to the following screen.



1. Begin by creating organizational units in each region, which will contain the Lights-Out Management 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.*
2. Use the HP provided ConsoleOne snap-ins to create Lights-Out Management objects in the *hp devices* organizational unit for several iLO devices.
   a. Right-click the *hp devices* organizational unit found in the *region1* organizational unit, and select **New** then **Object.**
   b. Select **hpqTarget** from the list of classes and click **OK.**
   c. Enter an appropriate name and surname in the **New hpqTarget** dialog box. In this example, the DNS host name of the iLO device, *rib-email-server* will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII*. Click **OK.**

d. The **Select Object Subtype** dialog box is displayed. Select **Lights Out Management Device** from the list, and click **OK.**

e. Repeat the process for several more iLO 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*.



3. 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** then **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 will contain users trusted for remote server administration and will be named *remoteAdmins*. Click **OK.**

d. The **Select Object Subtype** dialog box is displayed. Because this role will be managing the rights to Lights-Out Management devices, select **Lights Out Management Devices** from the list, and click **OK.**

e. 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*.

4. Use the HP provided ConsoleOne snap-ins to assign rights to the role and associate the roles with users and devices.

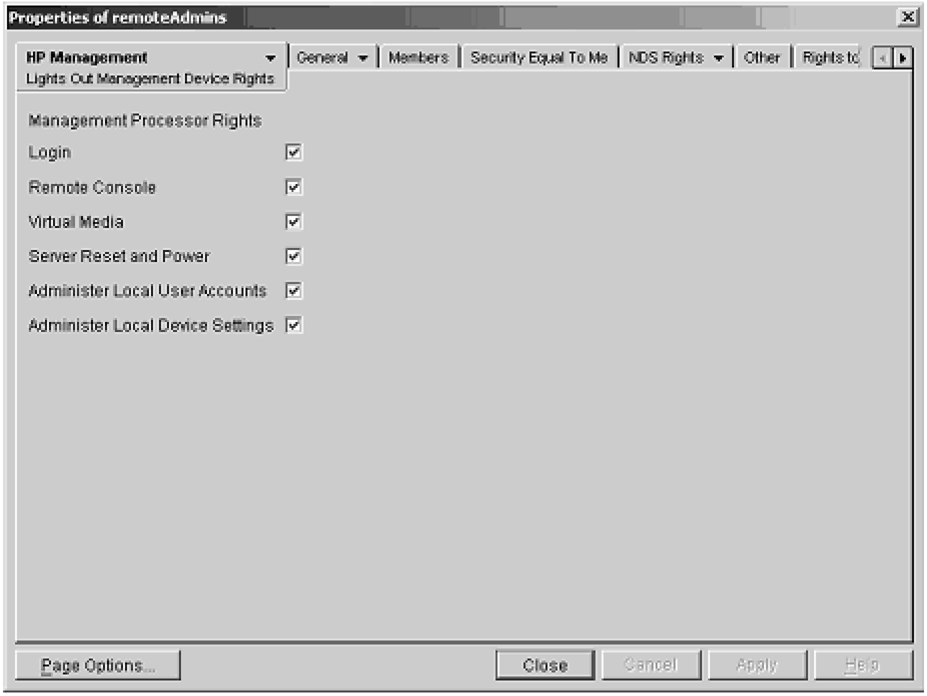
a. Right-click on the *remoteAdmins* role in the *roles* organizational unit in the *region1* organizational unit, and select **Properties.**

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 Lights-Out Management objects created in step 2. Click **OK,** then 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.

e. The devices and users are now associated. Use the **Lights Out Management Device Rights** subtab of the **HP Management** tab 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 devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the iLO functionality. Select the boxes next to each right, and click **Apply.** Click **Close** to close the property sheet.



Management Processor Rights

Login ☑

Remote Console ☑

Virtual Media ☑

Server Reset and Power ☑

Administer Local User Accounts ☑

Administer Local Device Settings ☑

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

   a. Add the three iLO 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. Then, using the **Lights Out Management Device Rights** subtab of the **HP Management** tab, select the check box next to **Login,** and click **Apply** and **Close.** Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any Integrated Lights-Out 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 Integrated Lights-Out device is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure a Integrated Lights-Out device and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the **Directory Settings** screen.

NOTE: Commas, not periods, are used 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
```

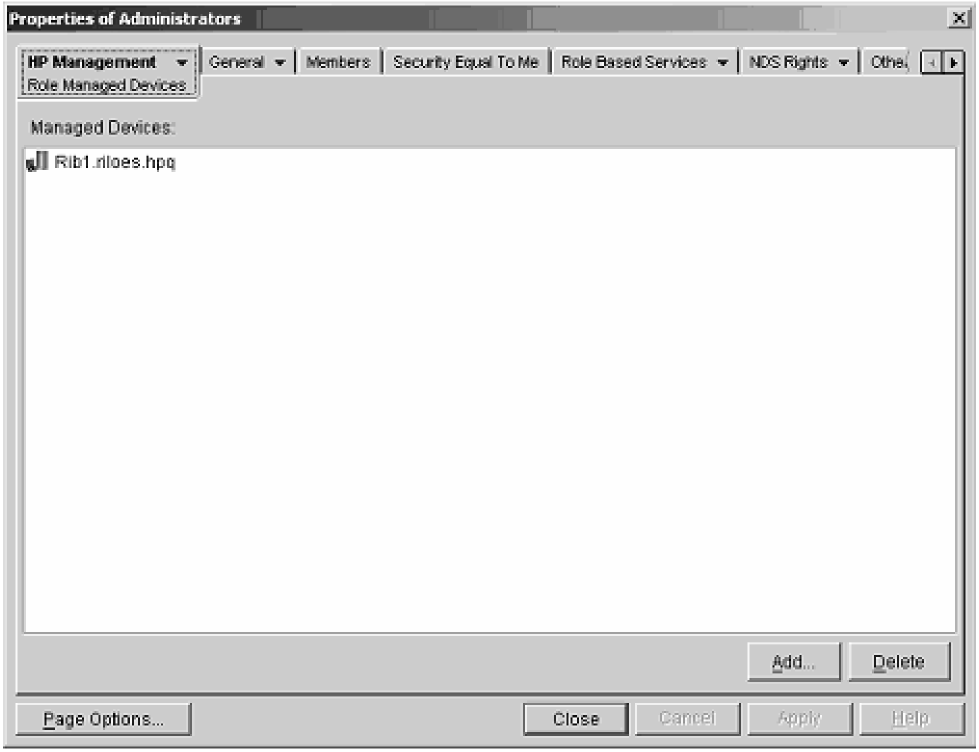
For example, user *CSmith*, located in the *users* organizational unit within the *samplecorp* organization, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the iLO. They would type `csmith` (case insensitive) in the **Login Name** field of the iLO login screen and use their eDirectory password in the **Password** field of that screen 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.

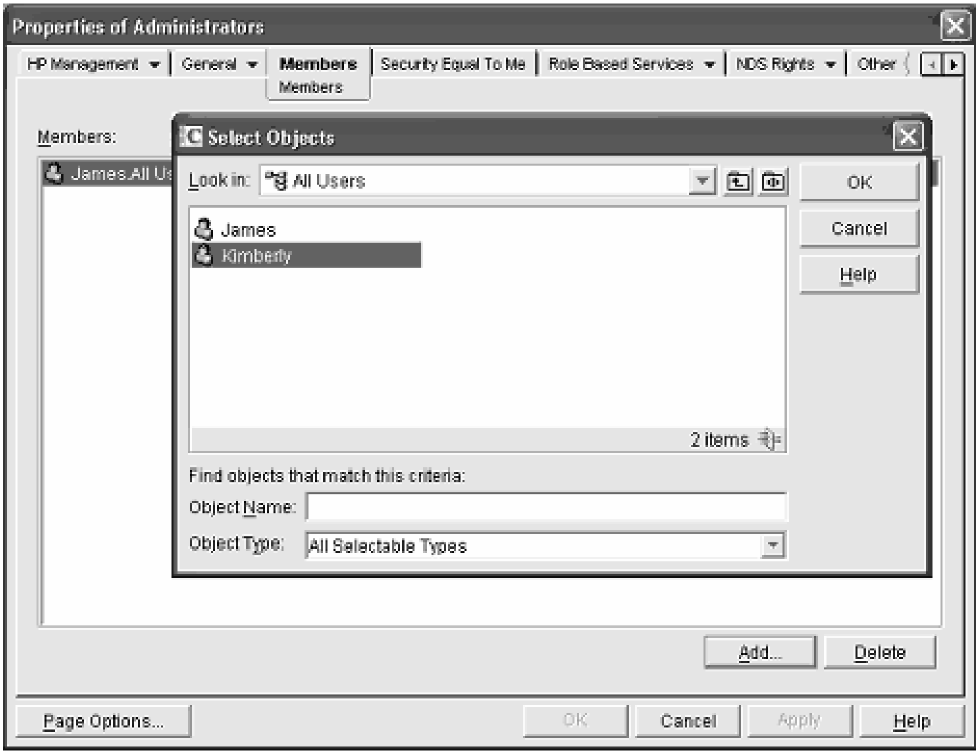
Role Managed Devices

The Role Managed Devices subtab under the HP Management tab is used to add the HP devices to be managed within a role. Clicking **Add** allows you to browse to the specific HP device and add it as a managed device.



Members

After user objects are created, the Members tab allows you to manage the users within the role. Clicking **Add** allows you to browse to the specific user you want to add. Highlighting an existing user and clicking **Delete** removes the user from the list of valid members.



Members: James.All Us

Look in: All Users

Object Name:

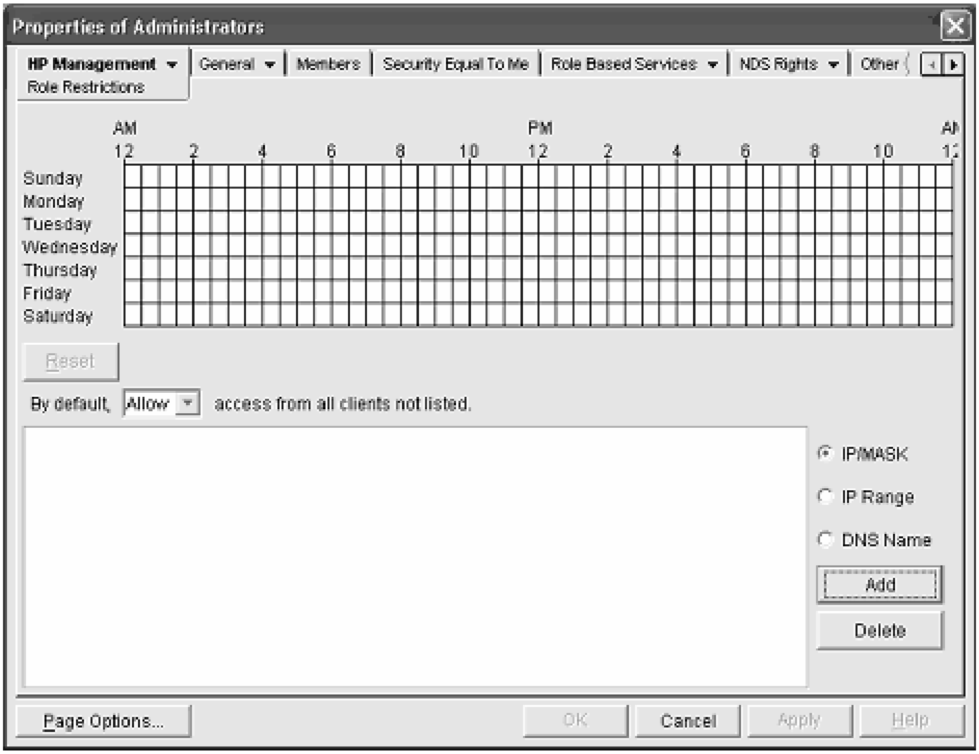
Object Type: All Selectable Types

Role Restrictions

The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask

  - IP Range
- DNS Name



Properties of Administrators

By default, Allow access from all clients not listed.

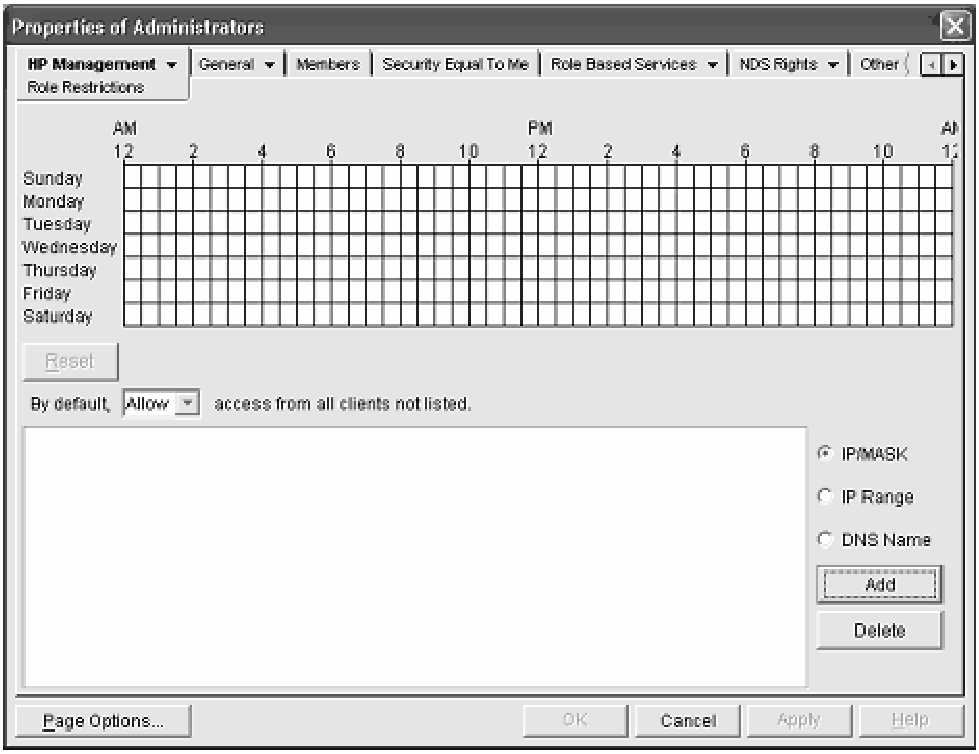
● IP/MASK

eDirectory Role Restrictions

The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

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

- DNS Name



By default, Allow access from all clients not listed.

○ IP/MASK (selected)

Time Restrictions

You can manage the hours available for logon by members of the role by using the time grid displayed in the Role Restrictions subtab. You can select the times available for logon 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.

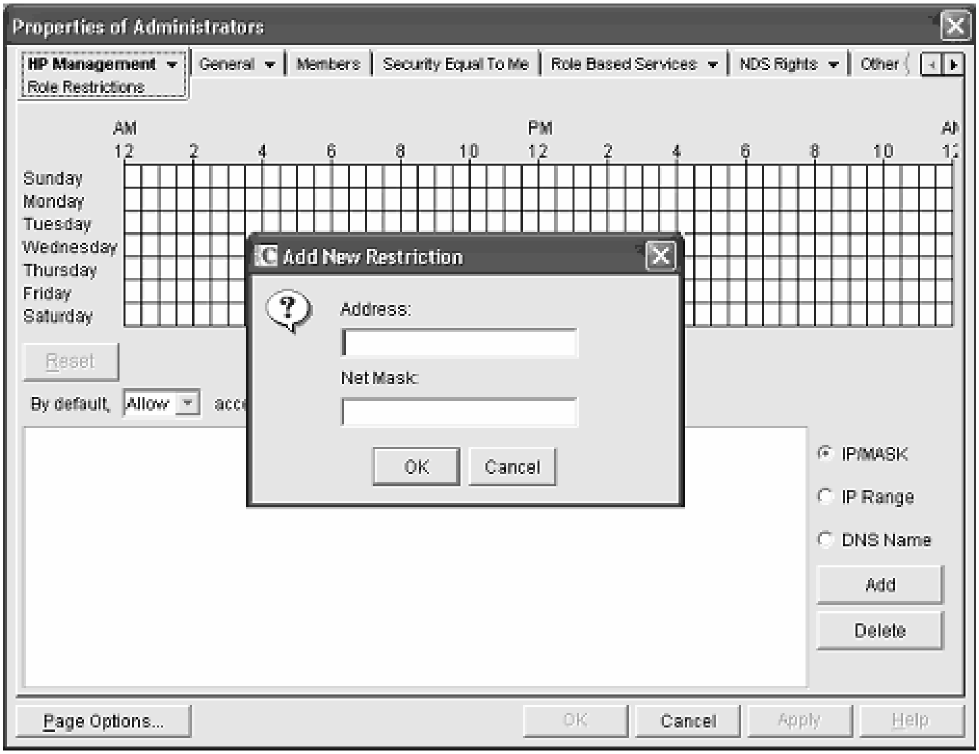
Enforced Client IP Address or DNS Name Access

Access can be granted or denied to an IP address, IP address range, or DNS names.

1. 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.
2. Select the addresses to be added, select the type of restriction, and click **Add.**
3. In the Add New Restriction pop-up window, enter the information and click **OK.** The Add New Restriction pop-up for the IP/Mask option is shown.

   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com.
4. Click **Apply** to save the changes.

To remove any of the entries, highlight the entry in the display field and click **Delete.**

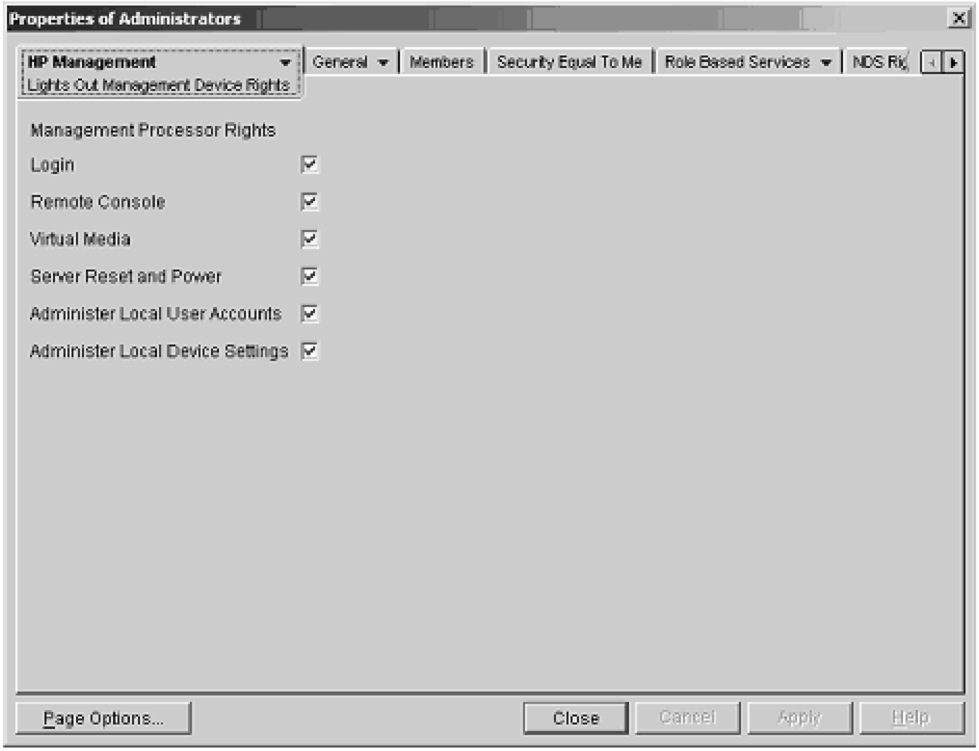


By default, Allow acc

● IP/MASK
○ IP Range
○ DNS Name

Lights-Out Management

After a role is created, rights for the role can be selected. Users and group objects can now be made members of the role, giving the users or group of users the rights granted by the role. Rights are managed on the **Lights Out Management Device Rights** subtab of the **HP Management** tab.



Management Processor Rights

Login ☑

Remote Console ☑

Virtual Media ☑

Server Reset and Power ☑

Administer Local User Accounts ☑

Administer Local Device Settings ☑

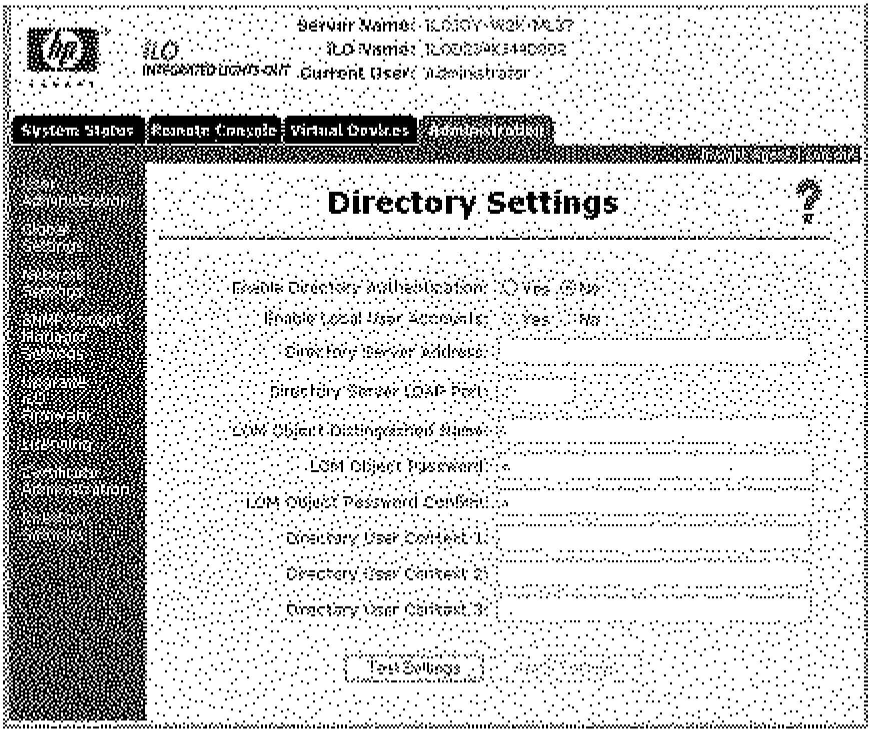
The available rights are:

- **Login**—This option controls whether users can to log in to the associated devices.

  Login access can be used to create a user who is a service provider and who receives alerts from the board but does not have login access to the RILOE II.

- **Remote Console**—This option allows the user access to the Remote Console.
- **Virtual Media**—This option allows the user access to the RILOE II Virtual Floppy and Virtual Media functionality.
- **Server Reset and Power**—This option allows the user to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option allows the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—This option allows the user to configure the RILOE II board settings. These settings include the options available on the **Global Settings, Network Settings, SNMP Settings,** and **Directory Settings** screens of the RILOE II Web browser.

Configuring Directory Settings



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

Directory Settings

Enable Directory Authentication: ○ Yes ● No
Enable Local User Accounts: ○ Yes ○ No
Directory Server Address:
Directory Server LDAP Port:
LOM Object Distinguished Name:
LOM Object Password:
LOM Object Password Confirm:
Directory User Context 1:
Directory User Context 2:
Directory User Context 3:

The Directory Settings screen contains the following settings options:

- Enable Directory Authentication (on page 351)
- Enable Local User Accounts (on page 351)
- Directory Server Address (on page 351)
- Directory Server LDAP Port
- LOM Object Distinguished Name (on page 351)
- LOM Object Password (on page 351)

  NOTE: At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.

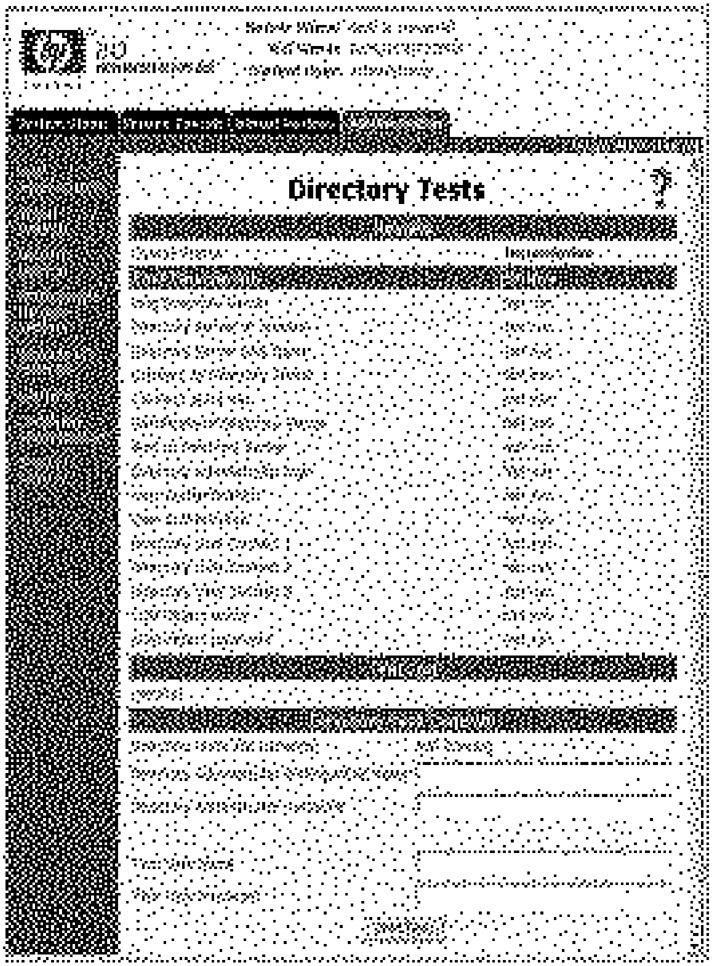
- Directory User Context ("Directory User Context 1, Directory User Context 2, Directory User Context 3" on page 352)

Click **Apply Settings** to save any changes.

To test the communication between the directory server and iLO, click **Test Settings.** Refer to "Testing Directory Settings (on page 352)" for additional information.

Directory Tests

To validate current directory settings for iLO, click **Test Settings** on the Directory Settings page. The Directory Tests page will display.



The test page displays the results of a series of simple tests designed to validate the current directory settings. Additionally, it includes a test log that shows test results as well as any problems that have been detected. After your directory settings are configured correctly, you do not need to re-run these tests. The Directory Tests screen does not require the user to be logged-in as a directory user.

To verify your directory settings:

1. Enter the distinguished name and password of a directory administrator. A good choice would be the same credentials used when creating the iLO objects in the directory. These credentials are not stored by iLO. They are used to verify the iLO object and user search contexts.
2. Enter a test user name and password. Typically, this would be an account intended to access the iLO being tested. It can be the same account as the directory administrator, however the tests will be unable to verify user authentication with a "superuser" account. These credentials are not stored by iLO.
3. Click **Start Test,** several tests begin in the background, starting with a network ping of the directory user through establishing an SSL connection to the server and evaluating user privileges as they would be evaluated during a normal login.

   While the tests are running, the page periodically refreshes. At any time during test execution, you can stop the tests or manually refresh the page.
4. Consult the help link on the page for test details and actions in the event of trouble.

User Login Using Directory Services

The iLO login page 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. You must 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 may 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 may be located in one of three searchable contexts, which are configured within Directory Settings.

- Local users—Login-ID

  > **NOTE:** On the iLO login page, the maximum length of the Login Name is 39 characters for local users. For Directory Services users, the maximum length of the Login Name is 256 characters.

Certificate Services

In This Section

Introduction to Certificate Services

Certificate Services are used to issue signed digital certificates to network hosts. The certificates are used to establish SSL connections with the host and verify the authenticity of the host.

Installing Certificate Services allows Active Directory to receive a certificate that allows Lights-Out processors to connect to the directory service. Without a certificate, iLO cannot connect to the directory server.

Each directory server that you want iLO to connect to must be issued a certificate. If you install an Enterprise Certificate Service, Active Directory can automatically request and install certificates for all of the Active Directory controllers on the network.

Installing Certificate Services

1. Select **Start>Settings>Control Panel.**
2. Double-click **Add/Remove Programs.**
3. Click **Add/Remove Windows Components** to start the Windows Components wizard.
4. Select the **Certificate Services** check box. Click **Next.**
5. Click **OK** at the warning that the server cannot be renamed. The Enterprise root CA option is selected because there is no CA registered in the active directory.

6. Enter the information appropriate for your site and organization. Accept the default time period of two years for the `Valid for` field. Click **Next.**
7. Accept the default locations of the certificate database and the database log. Click **Next.**
8. Browse to the c:\I386 folder when prompted for the Windows® 2000 Advanced Server CD.
9. Click **Finish** to close the wizard.

Verifying Directory Services

Because management processors communicate with Active Directory using SSL, it is necessary to create a certificate or install Certificate Services. You must install an enterprise CA because you will be issuing certificates to objects within your organizational domain.

To verify that certificate services is installed:

1. Select **Start>Programs>Administrative Tools>Certification Authority.**
2. If Certificate Services is not installed an error message appears.

Configuring Automatic Certificate Request

To specify that a certificate be issued to the server:

1. Select **Start>Run,** and enter `mmc`.
2. Click **Add.**
3. Select **Group Policy,** and click **Add** to add the snap-in to the MMC.
4. Click **Browse,** and select the Default Domain Policy object. Click **OK.**
5. Select **Finish>Close>OK.**
6. Expand **Computer Configuration>Windows Settings>Security Settings>Public Key Policies.**
7. Right-click **Automatic Certificate Requests Settings,** and select **New>Automatic Certificate Request.**

8. Click **Next** when the Automatic Certificate Request Setup wizard starts.
9. Select the **Domain Controller** template, and click **Next.**
10. Select the certificate authority listed. (It is the same CA defined during the Certificate Services installation.) Click **Next.**
11. Click **Finish** to close the wizard.

Directory-Enabled Remote Management

In This Section

Introduction to Directory-Enabled Remote Management

This section is for administrators who are familiar with directory services and the iLO product. You must be familiar with the “Directory Services (on page 143)" section and comfortable with setting up and understanding the examples.

Directory-enabled remote management allows you to:

- Create Lights-Out Management Objects

  Administrators must create one LOM device object to represent each device that will use the directory service to authenticate and authorize users. Refer to the "Directory Services (on page 143)" section for additional information on creating LOM device objects for Active Directory ("Directory Services for Active Directory" on page 153) and eDirectory ("Directory Services for eDirectory" on page 171). In general, administrators can use the HP provided snap-ins to create objects. It is useful to give the LOM device objects meaningful names, such as the device's network address, DNS name, host server name, or serial number.

- Configure the Lights-Out Management Devices

Every LOM device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. Refer to "Configuring Directory Settings (on page 184)" for details on the specific directory settings. In general, administrators configure each device with the appropriate directory server address, LOM 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 multi-host DNS name.

Using Bulk Import Tools

Adding and configuring large numbers of LOM objects is time consuming. HP provides several utilities to assist in these tasks. Below is a brief description of the utilities available.

- HP Lights-Out Migration Utility

  The HP Lights-Out Migration utility, HPQLOMIG.EXE, imports and configures multiple LOM devices. HPQLOMIG.EXE includes a GUI that provides a step-by-step approach to implementing or upgrading large numbers of management processors. HP recommends using this GUI method when upgrading numerous management processors. For more information, refer to the "Lights-Out Directories Migration Utilities (on page 205)" section.

- HP Lights-Out Migration Command Utility

  The HP Lights-Out Migration Command utility, HPQLOMGC.EXE, offers a command-line approach to migration, rather than a GUI-based approach. This utility works in conjunction with the Application Launch and query features of Insight Manager 7 to configure many devices at a time. Customers that must configure only a few LOM devices to use directory services might also prefer the command-line approach. For more information, refer to the "Lights-Out Directories Migration Utilities (on page 205)" section.

- Insight Manager 7 and Systems Insight Manager can:
  - Manage multiple LOM devices.

  - Discover the LOM devices as management processors using CPQLOCFG to send a RIBCL XML script file to a group of LOM devices to manage those LOM devices. The LOM devices perform the actions designated by the RIBCL file and send a response to the CPQLOCFG log file. For more information, refer to the "Group Administration and iLO Scripting (on page 241)" and the "Remote Insight Command Language (on page 269)" sections.

- CPQLODOS Utility

  LOM devices can be configured for directory support before the associated objects have been created in the directory. Administrators can use CPQLOCFG and tools like the PERL script ("Using Perl with the XML Scripting Interface" on page 255) ilodply.pl to configure many LOM devices. LOM devices will not be able to complete a directory authentication until the associated directory objects are created.

- Traditional Import Utilities

  Administrators familiar with tools such as LDIFDE or the NDS Import/Export Wizard can use these utilities to import or create many LOM device objects in the directory. However, administrators must still configure the devices manually, as described above, but can do so at any time. Programmatic or scripting interfaces can also be used to create the LOM device objects in the same way as users or other objects. The "Directory Services Schema (on page 353)" section provides details on attributes and attribute data formats when creating LOM objects.

Using Existing Groups

Many organizations will have their users and administrators arranged into groups. In many cases, it is convenient to use the existing groups and associate the groups with one or more Lights-Out Management role objects. When the devices are associated with the role objects, the administrator controls access to the Lights-Out devices associated with the role by adding or deleting members from the groups.

When using Microsoft® Active Directory, it is possible to place one group within another or 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. New users can be added to either the existing group or the role.

Novell eDirectory does not allow nested groups. In eDirectory, any user that 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. New users can be added to either the existing object or the role.

When using trustee or directory rights assignments to extend role membership, users must be able to read the LOM object representing the LOM device. Some environments require the same trustees of a role to also be read trustees of the LOM object to successfully authenticate users.

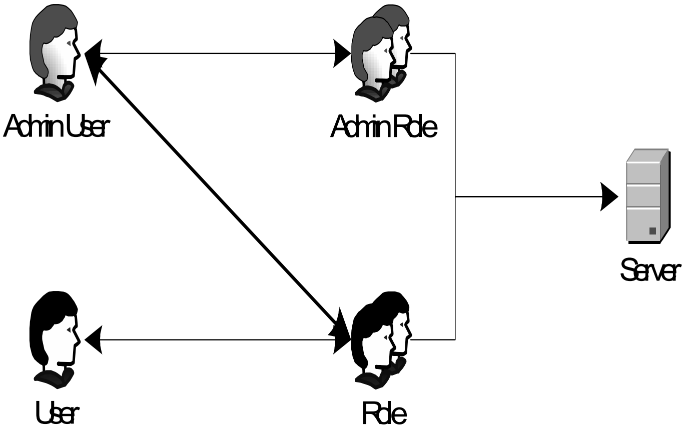
Using Multiple Roles

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, then the user has the right, even if the user is in another role that does not grant that right.

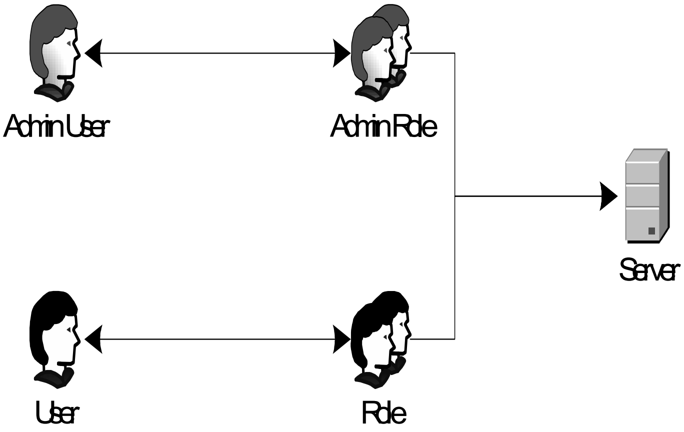
Typically, a directory administrator creates a base role with the minimum number of rights assigned and then creates additional roles to add additional rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization can have two types of users, administrators of the LOM device or host server and users of the LOM 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 LOM administrators in that role, as well as the administrative role.

An admin user gains the login right from the regular user group. More advanced rights are assigned through the Admin role, which assigns additional rights—Server Reset and Remote Console.



The Admin role assigns all 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 allow administrators to limit the scope of a role. A role only grants rights to those users that 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, refer to "Active Directory Role Restrictions (on page 165)" or "eDirectory Role Restrictions (on page 179, "Role Restrictions" on page 178)" sections.

Role Time Restrictions

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

LOM devices use local host time to enforce time restrictions. If the LOM 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 LOM 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 allows the LOM device to compensate for leap year and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing LOM firmware, can cause the LOM device clock to not be set. Also, the host time must be correct for the LOM device to preserve time across firmware flashes.

IP Address Range Restrictions

IP address range restrictions enable the administrator 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. An address range can be specified 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 the administrator to specify a range of addresses that are granted or denied access by the restriction. This format has similar capabilities as an IP address range but might 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 with the bits of the subnet mask, match the restriction subnet address, then 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.

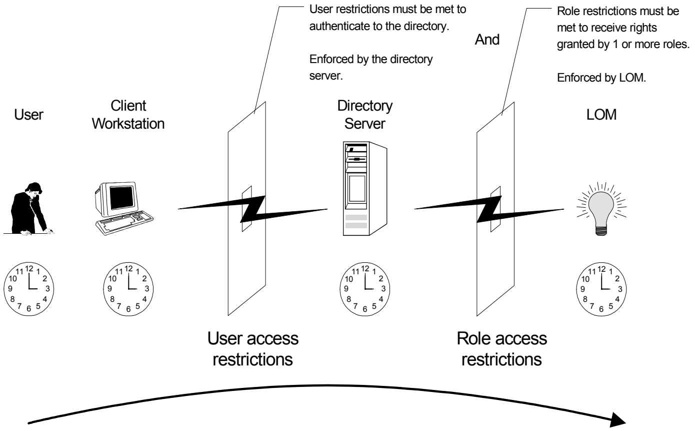
Role Address Restrictions

Role address restrictions are enforced by the LOM 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

Two sets of restrictions potentially limit a directory user's access to LOM 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 LOM 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.

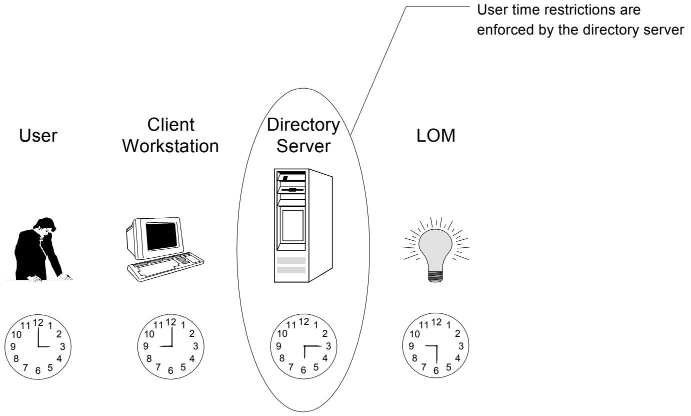
Role restrictions must be met to receive rights granted by 1 or more roles.

Enforced by LOM.

How User Time Restrictions are Enforced

Administrators 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, then 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 authentication mechanism.



User Address Restrictions

Administrators can place network address restrictions on a directory user account, and these restrictions are enforced by the directory server. Refer to the directory service documentation for details on the enforcement of address restrictions on LDAP clients, such as a user logging in to a LOM device.

Network address restrictions placed on the user in the directory might not be enforced in the expected manner if the directory user logs in through a proxy server. When a user logs in to a LOM device as a directory user, the LOM device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when accessing the LOM device. However, because the user is proxied at the LOM device, the network address of the authentication attempt is that of the LOM device, not that of the client workstation.

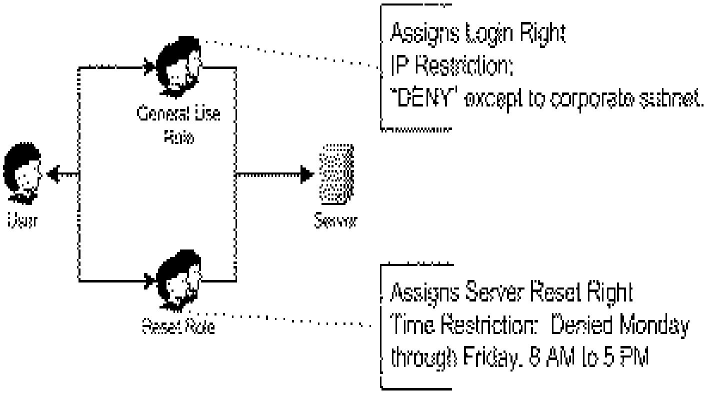
Creating Multiple Restrictions and Roles

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 the administrator to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which LOM administrators are allowed to use the LOM device from within the corporate network but are only able to reset the server outside of regular business hours.

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

In the example, security policy dictates general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.

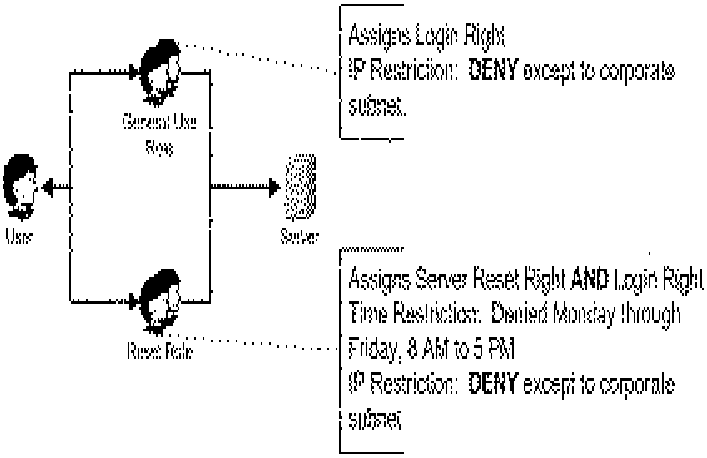


Assigns Login Right
IP Restriction:
"DENY" except to corporate subnet.

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, then 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 on-going administration might create another role that grants users from addresses outside the corporate network the login right, which could unintentionally grant the LOM 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.

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

Lights-Out Directories Migration Utilities

In This Section

Introduction to Lights-Out Migration Utilities

For customers with previously installed management processors, HP created two utilities to simplify the migration of these processors to management by Directory Services. The two utilities are the HPQLOMIG utility and the HPQLOMGC utility. These utilities automate some of the migration steps necessary for the management processors to support Directories Services. The utilities:

- Discover management processors in the network (HPQLOMIG only).
- Upgrade the firmware on the management processors to the version that supports Directory Services.
- Name the management processors to identify them in the directory.
- Create objects in the directory corresponding to each management processor and associating them to a role.
- Configure the management processors to enable them to communicate with the directory.

The HPQLOMIG utility automates the process of migrating management processors by creating objects in the directory corresponding to each management processor and associating them to a role. HPQLOMIG has a GUI and provides the user with a wizard approach to implementing or upgrading large amounts of management processors.

HPQLOMGC is a command line utility enabling you to migrate individual management processors. Used in conjunction with Insight Manager 7 or Systems Insight Manager, HPQLOMGC upgrades the firmware of the management processor, if necessary, configures the management processor, and configures the directory settings. It also creates a device object in the directory using the name in the XML file or the network name, depending on whether the user has selected this from the command line, then associates the device object to a role. HPQLOMGC can also be launched by itself or from within a script (for example, a batch file or Perl script).

Compatibility

HPQLOMIG and HPQLOMGC run on Microsoft® Windows® versions that support the Microsoft® .NET Framework. The Microsoft® .NET Framework is required. Additional information and download of the .NET framework can be found at http://www.microsoft.com/net/. Both utilities support the following operating systems:

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Red Hat Linux 7.2
  - Red Hat Linux 7.3
  - Windows® 2000
  - NetWare 6.0

Pre-Migration Checklist

1. Verify your current firmware version supports the HPQLOMIG and HPQLOMGC utilities.

Management Processor	Minimum Firmware Version
RILOE	2.41

Management Processor	Minimum Firmware Version
RILOE II	any version
iLO	1.10

2. Install Microsoft® .NET Framework.
3. Download the management processor firmware supporting Directory Services from the HP website (http://www.hp.com/servers/lights-out).
4. Download the HP Lights-Out Directory Services Smart Component from the HP website (http://www.hp.com/servers/lights-out).
5. Apply the HP Lights-Out schema extensions to the directory.
6. Create a role for the users of the management processor using the HP Lights-Out management snap-in.

HP Lights-Out Directory Package

All of the migration software, as well as the schema extender and management snap-ins, are packaged together in an HP Smart Component. To complete the migration of your management processors, the schema must be extended and the management snap-ins must be installed before the migration tool is run. The Smart Component can be found on the HP Lights-Out Management website (http://www.hp.com/servers/lights-out).

To install the migration utilities, click **LDAP Migration Utility** in the Smart Component. A Microsoft® MSI installer is launched, which installs HPQLOMIG, HPQLOMGC, required DLLs, the license agreement, and other files into the C:\Program Files\Hewlett-Packard\HP Lights-Out Migration Tool directory. You can select a different directory. A sample XML file is also installed, and a shortcut to HPQLOMIG is created on the Start menu.

NOTE: The installation utility will present an error message and exit if it detects that the .NET Framework is not installed.

HPQLOMIG Operation

The command line utility is intended to be used in conjunction with Insight Manager 7 and Systems Insight Manager. If you are not using Insight Manager 7 or Systems Insight Manager, consider using the HPQLOMIG utility.

> **IMPORTANT:** Installing directory support for any management processor requires downloading the HP Smart Component. Refer to the "Pre-Migration Checklist (on page 206)" and the "HP Lights-Out Directory Package" sections for additional information. Extending the schema must be completed by a Schema Administrator.

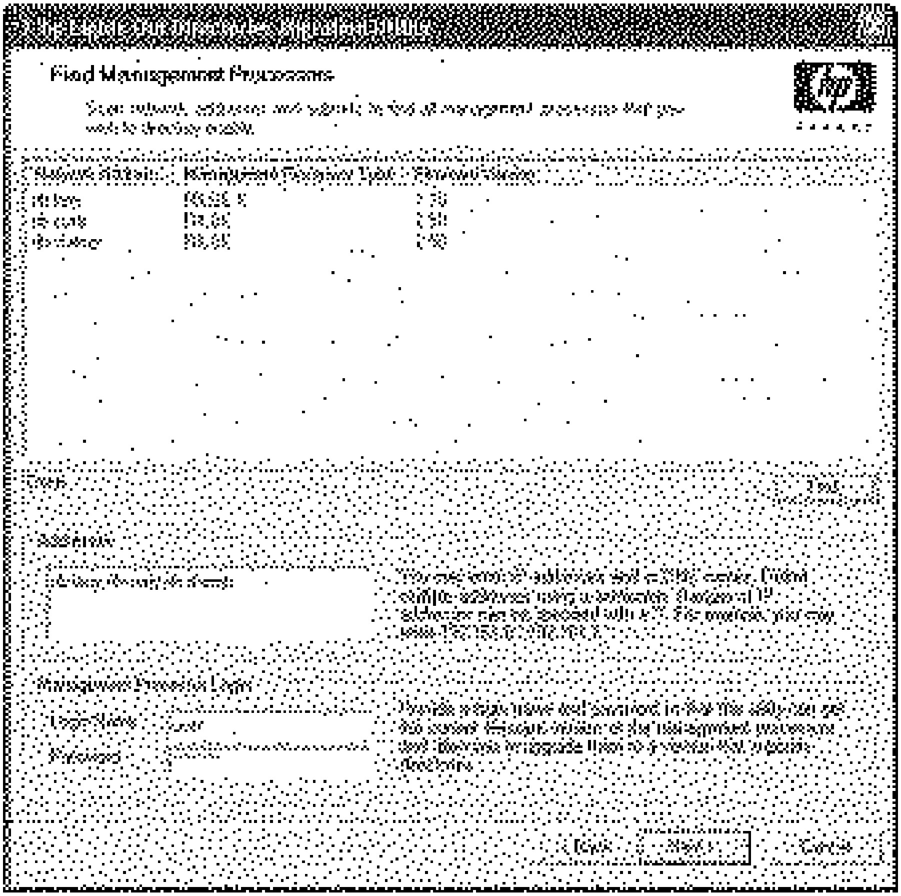
HPQLOMIG requires logon and upgrade firmware privileges for each management processor. Change directory setting privileges are required for directory services.

Finding Management Processors

The first step to migrating is to discover all management processors you want to enable for directory services. You can search for management processors using DNS names, IP addresses, or IP address wildcards. The following rules apply to the variables entered in the Addresses field:

- DNS names, IP addresses, and IP address wildcards must be delimited with a semicolon.
- The IP address wildcard uses the "*" character in the third and fourth octet fields. For example, IP address 16.100.*.* is valid, whereas IP address 16.*.*.* is not. Ranges can also be specified using a hyphen. For example, 192.168.0.2-10 is a valid range. A hyphen is only supported in the rightmost octet.
- After the user clicks **Find,** HPQLOMIG begins pinging and connecting to port 443 (the default SSL port). The purpose of these actions is to quickly determine if the target network address is a management processor. If the device does not respond to the ping or connect appropriately on port 443, then it is determined not to be a management processor.

If you click **Next, Back,** or exit the application during discovery, operations on the current network address are completed but those on subsequent network addresses are cancelled.



Find Management Processors

To start the process of discovering your management processors:

1. Select **Start>Programs>Hewlett-Packard, HPQLOMIG** to start the migration utility.
2. Click **Next** to move past the Welcome screen.
3. Enter the variables to perform the management processor search in the Addresses field.

4. Enter your Login Name>Password and click **Find.**

   IMPORTANT: The HPQLOMIG wizard assumes a common user name and password for management processors are employed. If unique user names and passwords are used, the command line version of the migration utility should be used.

Upgrading Firmware on Management Processors

The upgrade firmware screen enables you to update the management processors to the firmware version that supports directories. This screen also enables you to designate the location of the firmware image for each management processor by either typing the path or clicking **Browse.**

IMPORTANT: Binary images of the firmware for the management processors are required to be accessible from the system that is running the migration utility. These binary images can be downloaded from the H (http://www.hp.com/servers/lights-out)P website.

Management Processor	Minimum Firmware Version
RILOE	2.50
RILOE II	1.10
iLO	1.40

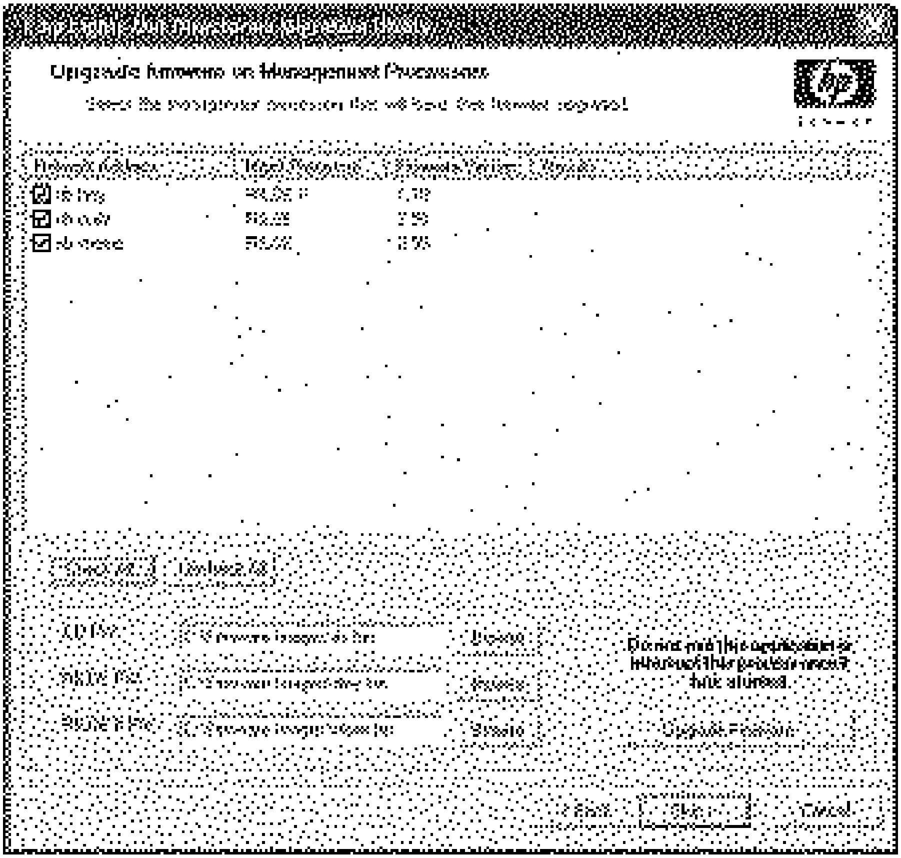
The upgrade process might take a long time, depending on the number of management processors selected. The firmware upgrade of a single management processor can take as long as five minutes to complete. If an upgrade fails, a message is displayed in the Results column and HPQLOMIG continues to upgrade the other discovered management processors.

IMPORTANT: HP recommends testing the upgrade process and verifying the results in a test environment before running the utility on a production network. An incomplete transfer of the firmware image to a management processor could result in having to locally reprogram the management processor using a floppy diskette.

To upgrade the firmware on your management processors:

1. Select the management processors to be upgraded.
2. For each discovered management processor type, enter the correct pathname to the firmware image or browse to the image.

3. Click **Upgrade Firmware.** The selected management processors will now be upgraded. Although this utility enables you to upgrade hundreds of management processors, only 25 management processors are upgraded simultaneously. Network activity is considerable during this process.
4. After the upgrade is complete, click **Next.**



During the firmware upgrade process, all buttons are deactivated to prevent navigation. You can still close the application using the "X" at the top right of the screen. If the GUI is closed while programming firmware, the application will continue to run in the background and complete the firmware upgrade on all selected devices.

Naming Management Processors

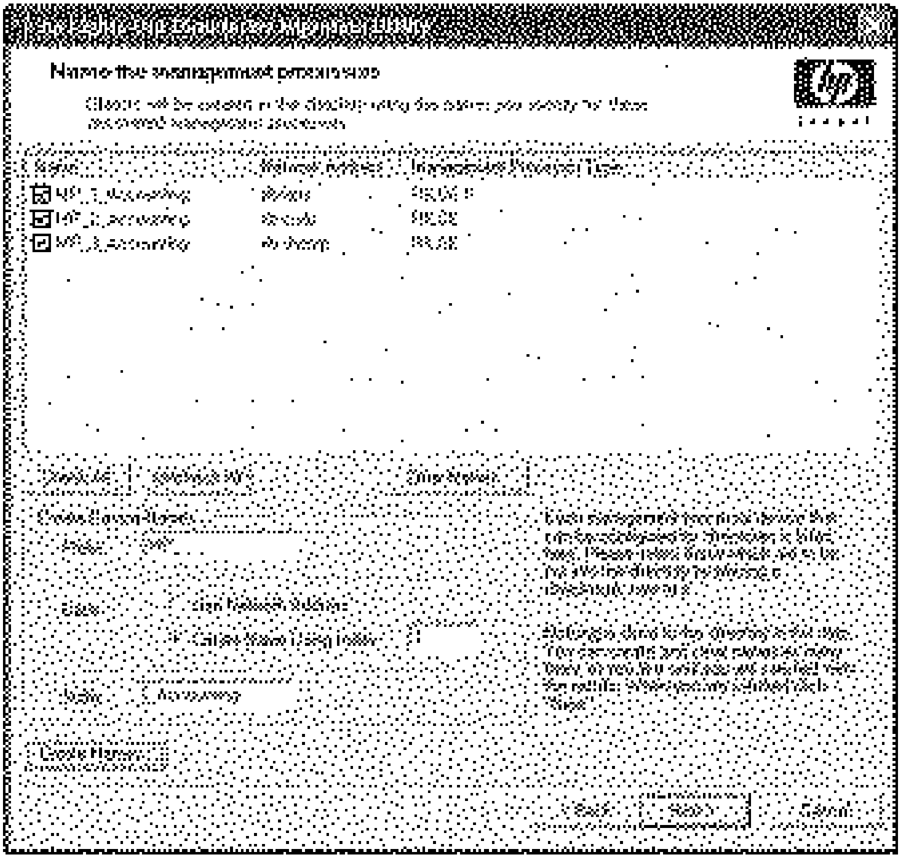
This screen enables you to name Lights-Out Management device objects in the directory and create corresponding device objects for all management processors to be managed. You can create names using one or more of the following:

- The network address
- An index
- A prepend prefix to all
- An append suffix to all

To name the management processors, click the **Name** field and enter the name, or:

1. Select either **Use Network Address** or **Create Name Using Index.**
2. Enter text to either prepend or append all names (optional).
3. Click **Generate Names.** The names display in the Name column as they are generated.
4. To change the names (optional), click **Clear All Names** and rename the management processors.

5. After the names are correct, click **Next.**



Configuring Directories

The Configure Directory screen enables you to create a device object for each discovered management processor and to associate the new device object to a previously defined role. For example, the directory defines a user as a member of a role (such as administrator) who has a collection of privileges on a specific device object (such as a RILOE II card).

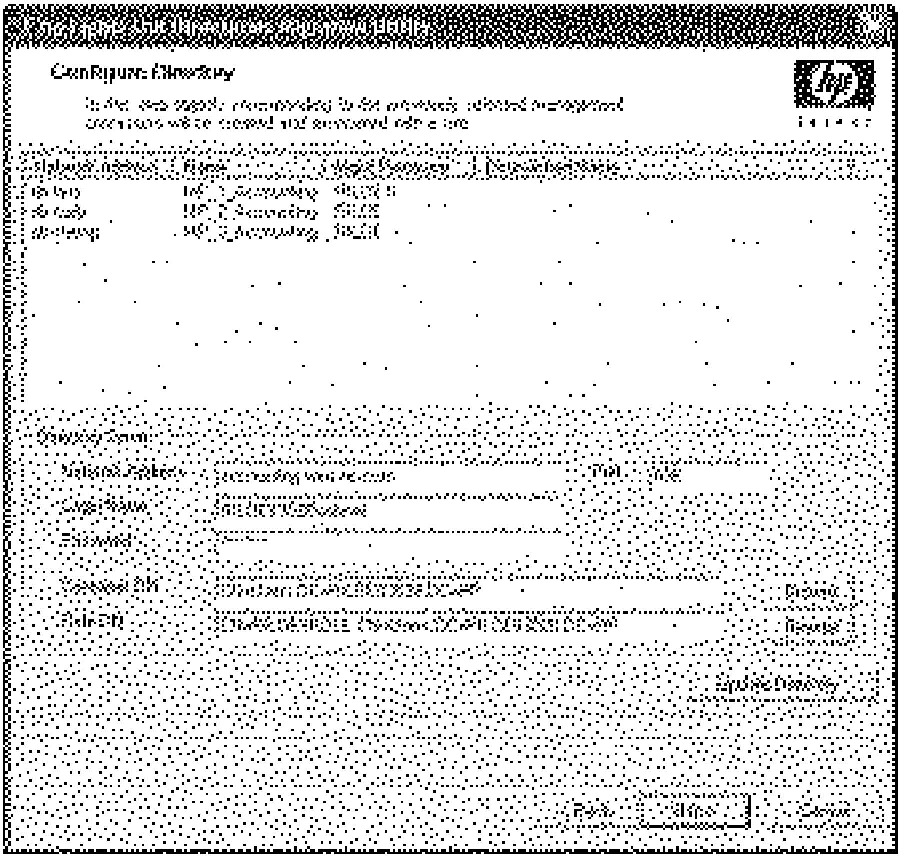
The fields in the Configure Directory screen are:

- **Network Address—**This is the network address of the directory server and can either be a valid DNS name or IP address.
- **Port—**The port is the SSL port to the directory. The default entry is 636. Management processors can only communicate with the directory using SSL.
- **Login Name** and **Password—**These fields are used to log in with an account that has domain administrator access to the directory.
- **Container DN—**After you have the network address, port, and login information, you can click **Browse** to navigate for the Container and Role DNs. The container distinguished name is where the migration utility will create all of the management processor objects in the directory.
- **Role DN—**The role distinguished name is where the role to be associated with the device objects resides and must be created before to running this utility.

To configure the device objects to be associated with a role:

1. Enter the network address, login name, and password for the designated directory server.
2. Enter in the container distinguished name in the Container DN field, or click **Browse.**
3. Associate device objects with a member of a role by entering the role distinguished name in the Role DN field, or click **Browse.**
4. Click **Update Directory.**

5. After the device objects have been associated with a role, click **Next.**



Setting Up Management Processors for Directories

The last step in the migration process is to configure the management processors to communicate with the directory. This screen enables you to create user contexts and designate whether or not Directory Support and Local Accounts are enabled.

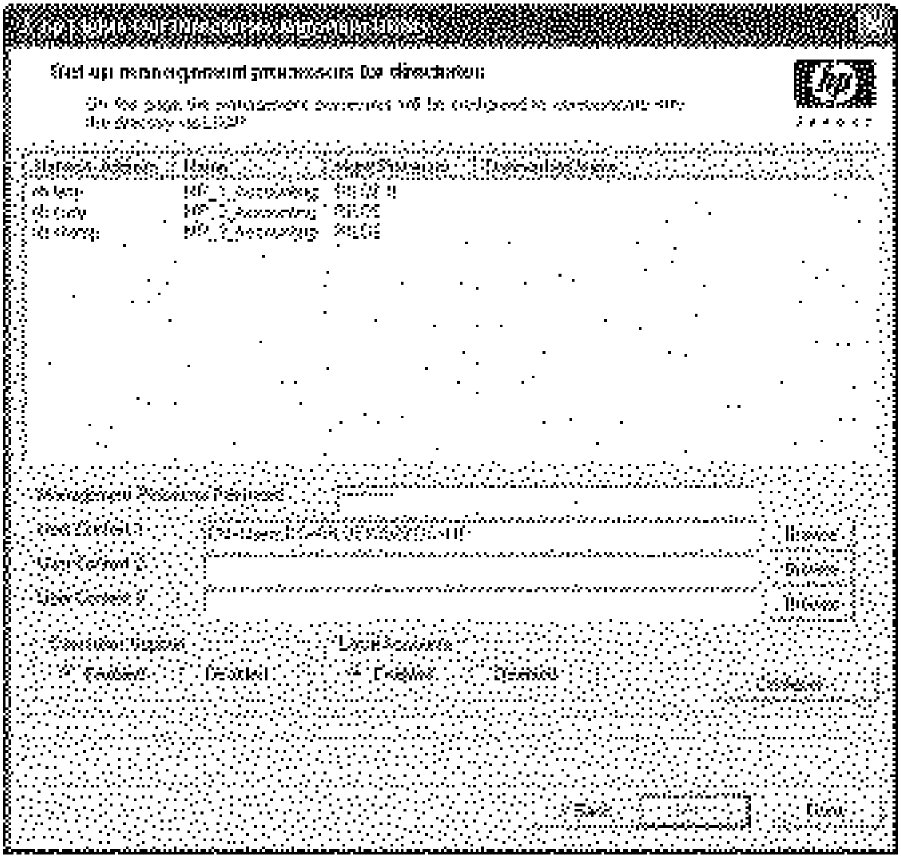
User contexts enable the user to use short or user object names to login rather than the full distinguished name. For example, having a user context as CN=Users,DC=RILOETEST2,DC=HP allows user "John Smith" to log in using John Smith rather than CN=John Smith,CN=Users, DC=RILOETEST2,DC=HP. The @ format is also supported. For example, @RILOETEST2.HP in a context field allows the user to log in using jsmith (assuming that jsmith is the user's short name).

To configure the management processors to communicate with the directory:

1. Enter the user contexts, or click **Browse.**
2. Select whether Directories Support and Local Accounts are **enabled or disabled.**

   Remote access will be disabled if both Directory Support and Local Accounts are disabled. To re-establish access, reboot the server and use RBSU F8 to restore access.
3. Click **Configure.**
4. When completed, click **Done.**

NOTE: The feature associated with the Management Processor Password field is not available at this time. This field is provided for forward compatibility with future releases.



Set up management processors for directories

HPQLOMGC Operation

The command line utility is intended to be used in conjunction with Insight Manager 7 and Systems Insight Manager. If you are not using Insight Manager 7 or Systems Insight Manager, consider using the HPQLOMIG utility. The command line mode does not present a GUI and runs unattended. This mode is intended to work in conjunction with the Application Launch ("Application Launch Using Insight Manager 7" on page 244) functionality.

> **IMPORTANT:** Installing directory support for any management processor requires downloading the HP Smart Component. Refer to the "Pre-Migration Checklist (on page 206)" and the "HP Lights-Out Directory Package" sections for additional information. Extending the schema must be completed by a Schema Administrator.

To implement directory support on a few management processors.

1. Use Insight Manager 7 or Systems Insight Manager to locate all of the management processors in the network.
2. Execute the HPQLOMGC utility.
3. Invoke the XML file to migrate the management processor.

HPQLOMGC goes through three phases to complete the migration of a management processor.

1. **The firmware version is validated and updated if necessary.**

   HPQLOMGC determines the type of management processor and the firmware level. If the firmware does not meet the minimum requirement ("Upgrading Firmware on Management Processors" on page 210), HPQLOMGC upgrades the firmware and resets the management processor. After the management processor resets, HPQLOMGC begins the next phase.

2. **The management processor directory settings are updated.**

   HPQLOMGC uses the scripting interface to send the directory settings to the management processor.

3. **The directory is updated.**

   HPQLOMGC creates a device object in the directory at the location specified by the user. HPQLOMGC uses either the object name specified in the XML file or the network name of the management processor. After the device object is created, the specified role object is then amended to include the newly created device object.

Launching HPQLOMGC Using Application Launch

Application Launch can be used to create tasks associated with administration of management processors. For example, the management processors can be discovered using Application Launch and could be used to automatically configure new management processors as they are added to the network.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task.** A dropdown menu is displayed.
4. Click **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
5. Enter the full path and name for the Lights-Out Migration Command Line Utility in the area provided. For example, if the HPQLOMGC.exe file is in the root directory of the C drive, then the path is: C:\HPQLOMGC.exe.
6. Enter the parameters in the area provided.

   Command line switches enable you to designate items such as the management processor to be upgraded, the XML file to be used, and where a log file is generated.

   -S <network address>—This switch contains the IP address or DNS name of the management processor. By default, the IP address of the management processor is automatically provided. The environment variable <DEVICEIPADDRESS0> can also be used to specify a network address.

   Use the -S switch to override the default behavior. If present, this switch has precedence over the IP address environment variable <DEVICEIPADDRESS0>.

   -F <filename>—This switch contains the path of the XML file that has the management processor directory settings and the location of the firmware images. This switch causes an error if an IP address is not designated.

   -A—This switch uses the network name for the name of the device object created in the directory.

   -V—This switch is optional and sets the HPQLOMGC to Verbose mode.

   -L <filename>—This switch defines where the log file is generated. This switch causes an error if an IP address is not designated.

   -Q—This switch is optional and sets the HPQLOMGC to Quiet mode.
7. Click **Next.** A screen is displayed with options for naming the task, defining the query association, and setting a schedule for the task.
8. Enter a task name in the Enter a name for this task field.

9. Select the query that had been created earlier, for example "Mgmt Processors."
10. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window is displayed.
11. Click **OK** to set the schedule.

    NOTE: The default schedule for a control task is **Now.**

12. Click **Finish** to save the Application Launch task.
13. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

HPQLOMGC Command Language

When using HPQLOMGC, the directory settings for the management processor are read from an XML file. The script used is a subset of the RIBCL and has been extended to support multiple management processor firmware images. For more information concerning RIBCL for your management processor, refer to the RILOE, RILOE II, or iLO user guide.

The following is an example of an XML file:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="user" PASSWORD="password">
<DIR_INFO MODE="write">
<ILO_CONFIG>
   <UPDATE_RIB_FIRMWARE
   IMAGE_LOCATION="C:\fw\ilo140.brk" />
</ILO_CONFIG>
<RILOE_CONFIG>
   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloe.brk"
   />
</RILOE_CONFIG>
<RILOE2_CONFIG>
   <UPDATE_RIB_FIRMWARE
   IMAGE_LOCATION="C:\fw\riloeii.brk" />
</RILOE2_CONFIG>
<MOD_DIR_CONFIG>
   <DIR_AUTHENTICATION_ENABLED value="YES" />
   <DIR_LOCAL_USER_ACCT value="YES" />
   <DIR_SERVER_ADDRESS
   value="administration.wins.hp.com" />
   <DIR_SERVER_PORT value="636" />
   <DIR_OBJECT_DN
   value="CN=RILOP5,CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_OBJECT_PASSWORD value="aurora" />
   <DIR_USER_CONTEXT_1
   value="CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_USER_CONTEXT_2 value="" />
   <DIR_USER_CONTEXT_3 value="" />
   <DIR_ROLE
   value="CN=RILOEROLE,CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_LOGIN_NAME value="RILOEGRP2\Adminl" />
   <DIR_LOGIN_PASSWORD value="aurora" />
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

ILO_CONFIG

RIBCL allows for only one firmware image per XML file. The command language for HPQLOMGC has been modified to allow for each management processor to have a specified firmware image within a single XML file. These commands must be displayed within a DIR_INFO block, and DIR_INFO must be in write mode. The management processor is reset after the firmware upgrade is complete. To update the firmware, the user must be logged in with the appropriate privilege.

This command line uses the following parameters:

- UPDATE_RIB_FIRMWARE IMAGE_LOCATION ("UPDATE_RIB_FIRMWARE Parameters" on page 302)
- MOD_DIR_CONFIG

Insight Manager 7 Integration

In This Section

Integrating iLO with Insight Manager 7

iLO fully integrates with Insight Manager 7 in key operating environments. Full integration with Insight Manager 7 also provides a single management console for launching a standard Web browser to access. While the operating system is running, you can establish a connection to iLO using Insight Manager 7.

Integration with Insight Manager 7 provides:

- Support for SNMP trap delivery to an Insight Manager 7 console

  Delivery to an Insight Manager Console can be configured to forward SNMP traps to a pager or email.

- Support for SNMP management

  Insight Manager 7 is allowed to access the Insight Management Agents information through iLO.

- Support for a management processor

  Insight Manager 7 adds support for a new device type, the management processor. All iLO devices installed in servers on the network are discovered in Insight Manager 7 as management processors. The management processors are associated with the servers in which they are installed.

- Grouping of iLO management processors

All iLO devices can be grouped together logically and displayed on one page. This capability provides access to iLO from one point in Insight Manager 7.

- iLO hyperlinks

  Insight Manager 7 provides a hyperlink on the server device page to launch and connect to iLO.

- HP Management Agents

  iLO, combined with HP Management Agents, provides remote access to system management information through the iLO Web browser interface.

Functional Overview

Insight Manager 7 enables you to:

- Identify iLO processors.
- Create an association between iLO and its server.
- Create links between iLO and its server.
- View iLO and server information and status.
- Control the amount of detailed information displayed for iLO.
- Draw a visualization of the ProLiant BL p-Class rack infrastructure.

The following sections give a summary of each function. For detailed information on these benefits and how to use Insight Manager 7, refer to the *HP Insight Manager 7 Technical Reference Guide,* provided with Insight Manager 7.

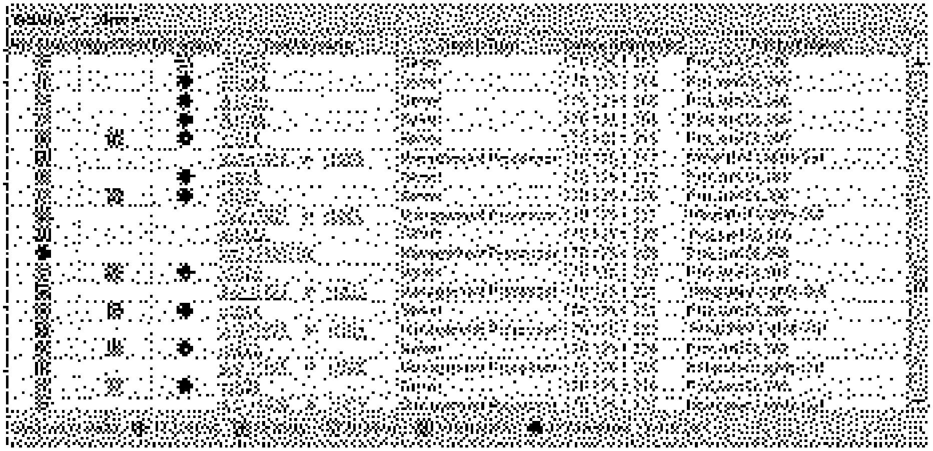
Identification and Association

Insight Manager 7 can identify an iLO processor and create an association between iLO and the server. The administrator of the iLO device can configure iLO to respond to Insight Manager 7 identification requests.

Status

In Insight Manager 7, iLO is identified as a management processor. Insight Manager 7 displays the management processor status within the device list.

The iLO management processor is displayed as an icon in the device list on the same row as its host server. The color of the icon represents the status of the management processor.



For a complete list of device statuses, refer to the *HP Insight Manager 7 Technical Reference Guide,* provided with Insight Manager 7.

Queries

iLO management processors can be queried within Insight Manager 7. The administrator can save and use these queries to create groups of management processors. Refer to the *HP Insight Manager 7 Technical Reference Guide* for further details.

Links

For ease of management, Insight Manager 7 creates links to the following locations:

- iLO and the host server from the Insight Manager 7 home page
- iLO from the Query Results page
- The server from the Query Results page
- The server from the Device Summary page of iLO
- iLO from the Device Summary page of the server

The Home page and Query Results pages display iLO, the server, and the relationship between iLO and the server. For example, the page can display the server, the iLO name next to the server, and *iLO name* **IN** *server* in the Device Name field for iLO.

Clicking the device status icon for either iLO or the server takes you to the summary page of the device. Within the summary page are the status, IP address, and link for the associated device.

Configuring Identification of iLO

iLO enables you to set how much data is returned on a Systems Insight Manager request for more information.

The level of data returned is controlled on the SNMP/Insight Manager Settings screen. The identification data level options are:

- **High**—Associations are present, and all data is present on the summary page.
- **Medium**—Associations are present, but the summary page contains less detail than at high security.
- **Low**—Associations are present, if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.
- **None**—No data is returned to Insight Manager 7.

Display Information	Low	Medium	High	None
Product Name	Y	Y	Y	
Server Serial Number		Y	Y	

Display Information	Low	Medium	High	None
Server State			Y	
Management Processor Status	Y	Y	Y	
Management Processor Serial Number		Y	Y	
iLO Advanced License Status and Data		Y	Y	
Hardware Revision Information			Y	
Firmware Revision Information			Y	
Rack Topology		Y	Y	
Single Sign On*			Y	
Secure Task Execution*			Y	
CIMOM*			Y	
Device Home Page URL			Y	

***NOTE:** Reserved for future integration.

Receiving SNMP Alerts in Insight Manager 7

iLO can be configured to forward alerts from the host operating system management agents, and it can also be configured to send iLO-generated alerts to the Insight Manager 7 console.

Insight Manager 7 provides support for full SNMP management, and iLO supports SNMP trap delivery to an Insight Manager 7 console. You can view the event log, select the event, and view the additional information about the alert.

Configuring receipt of SNMP alerts in Insight Manager 7 is a two-step process. The process requires configuring Insight Manager 7 to receive SNMP alerts from an iLO-managed device and configuring iLO to enable SNMP alerts.

To configure receipt of SNMP alerts in Insight Manager 7:

1. Select **SNMP/Insight Manager Settings** in the Administration tab of the iLO navigation frame to enable SNMP alerting and to provide an SNMP trap IP address to iLO. This IP address should be the address of the computer running Insight Manager 7. Refer to the "Enabling SNMP Alerts (on page 96)" section for details.
2. Configure iLO as a managed device for Insight Manager 7. Adding iLO to Insight Manager 7 enables the NIC interface on iLO to function as a dedicated management port, isolating management traffic from the remote host server NIC interface.
    a. Start Insight Manager 7. Click **Settings.** By default, the Automatic Discovery screen is displayed. Use this screen to discover any iLO that will be managed by Insight Manager 7. If the IP address does not already appear in the Ping Inclusion Ranges section, enter the IP address.
    b. Click **Execute Discovery Now** to add iLO to Insight Manager 7. The Status section displays the system being updated.
    c. After the discovery is complete, subsequent queries will display the device as a management processor.
    d. You might need to select **Edit Device** from the Discovery tab and edit the monitor community string (for example, by changing it to "public") so that iLO is displayed in the list of monitored devices.
    e. iLO traps are displayed in a query for major, uncleared events. You can click the orange button at the top of the screen to issue this query. Click the event description to obtain further information about the event.

    NOTE: HP Insight Agents for iLO must be installed on the remote host server to enable management of iLO. Refer to "Installing iLO Device Drivers (on page 24)" for additional details about installing and configuring agents.

Port Matching

Insight Manager 7 is configured to start an HTTP session to check for iLO at port 80. The port can be changed. If you want to change the port number, you must also change it in Network Settings and Insight Manager 7.

To change the port number in Insight Manager 7, add the port to the \ADDITIONALWSDISC.PROPS file. Port 80 does not need an entry in this props file, but any other port designated for iLO must be specified so that Insight Manager 7 can use it during HTTP identification. The format of the entries is:

```
Port=Description,Reserved 1,Reserved 2,Reserved 3,Class
Name
```

where:

- *Port* is the number of the additional HTTP port to be added into discovery.
- *Description* is the description of the Web server to be displayed in the list of links on the device page.
- *Reserved 1* is reserved and should be set to a space.
- *Reserved 2* is reserved and should be set to true.
- *Reserved 3* is reserved and should be set to false.
- *Class Name* specifies the name of the Insight Manager 7 Java™ class that does the processing for the additional management processor port. This information should not be changed.

Example:

```
80=iLO, ,true,false,compaq.ID.MgmtProc.MgmtProcessorPars
er
```

Reviewing iLO Advanced License Information in Insight Manager 7

Insight Manager 7 provides a report showing the license status of the iLO management processors. You can use this report to determine how many and which iLO devices are licensed for the iLO Advanced.

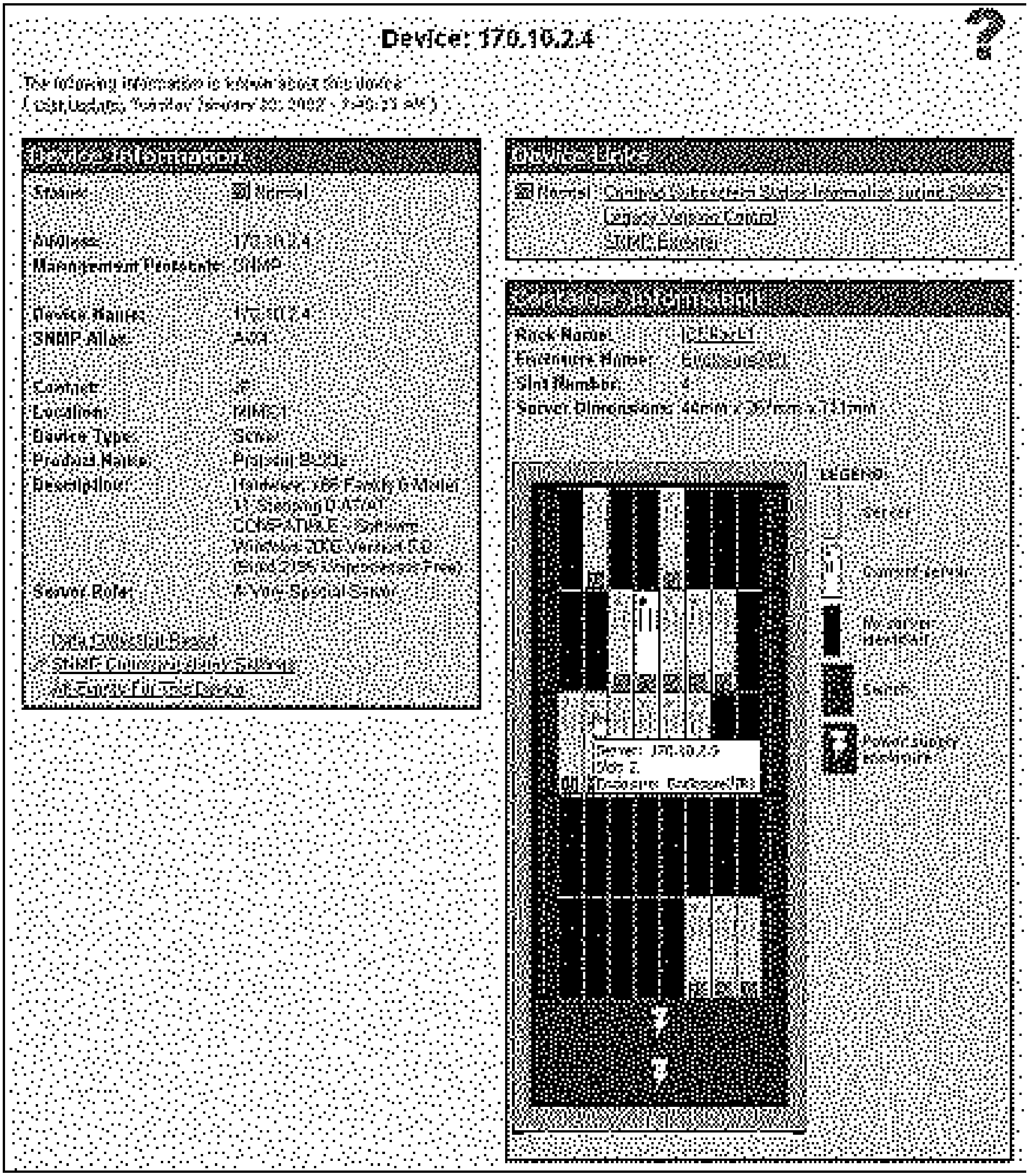
To view this report:

1. Click **Devices.**
2. Click **Reports.**
3. Click **Device License Information—All Servers.**

The license information of the management processors appears. To be sure that this data is current, run the device identification task for your management processors. Refer to the Insight Manager 7 documentation for additional details about initiating tasks.

ProLiant BL p-Class Rack Visualization

Insight Manager 7 can draw a visualization of the ProLiant BL p-Class rack, enclosures, and servers using information from iLO. The SNMP/Insight Manager setting for the level of data to be returned must be Medium or High for Insight Manager 7 to draw the visualization.



Device: 170.10.2.4

The following information is known about this device:
(Last Update: [illegible])

Device Information

Status: Normal

Address: 170.10.2.4
Management Protocols: SNMP

Device Name: 170.10.2.4
SNMP Alias: [illegible]

Contact: [illegible]
Location: [illegible]
Device Type: Server
Product Name: ProLiant BL10e
Description: Hardware: x86 Family 6 Model 11 Stepping 0 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
Server Role: A Very Special Server

Data Collection Reports
SNMP Community String Settings
All Events For This Device

Device Links

Normal [illegible]
[illegible]
[illegible]

[illegible]

Rack Name: [illegible]
Enclosure Name: [illegible]
Slot Number: [illegible]
Server Dimensions: [illegible]

Systems Insight Manager Integration

In This Section

Integrating iLO with Systems Insight Manager

iLO fully integrates with HP Systems Insight Manager in key operating environments. Full integration with Systems Insight Manager also provides a single management console for launching a standard Web browser to access. While the operating system is running, you can establish a connection to iLO using Systems Insight Manager.

Integration with Systems Insight Manager provides:

- Support for SNMP trap delivery to a Systems Insight Manager console

  Delivery to a Systems Insight Manager console can be configured to forward SNMP traps to a pager or email.

- Support for SNMP management

  Systems Insight Manager is allowed to access the Insight Management Agents information through iLO.

- Support for a management processor

Systems Insight Manager adds support for a new device type, the management processor. All iLO devices installed in servers on the network are discovered in Systems Insight Manager as management processors. The management processors are associated with the servers in which they are installed.

- Grouping of iLO management processors

  All iLO devices can be grouped together logically and displayed on one page. This capability provides access to iLO from one point in Systems Insight Manager.

- iLO hyperlinks

  Systems Insight Manager provides a hyperlink on the server device page to launch and connect to iLO.

- HP Management Agents

  iLO, combined with HP Management Agents, provides remote access to system management information through the iLO Web browser interface.

Systems Insight Manager Functional Overview

Systems Insight Manager enables you to:

- Identify iLO processors.
- Create an association between iLO and its server.
- Create links between iLO and its server.
- View iLO and server information and status.
- Control the amount of detailed information displayed for iLO.
- Draw a visualization of the ProLiant BL p-Class rack infrastructure.

The following sections give a summary of each function. For detailed information on these benefits and how to use Systems Insight Manager, refer to the *HP Systems Insight Manager Technical Reference Guide,* provided with Systems Insight Manager.

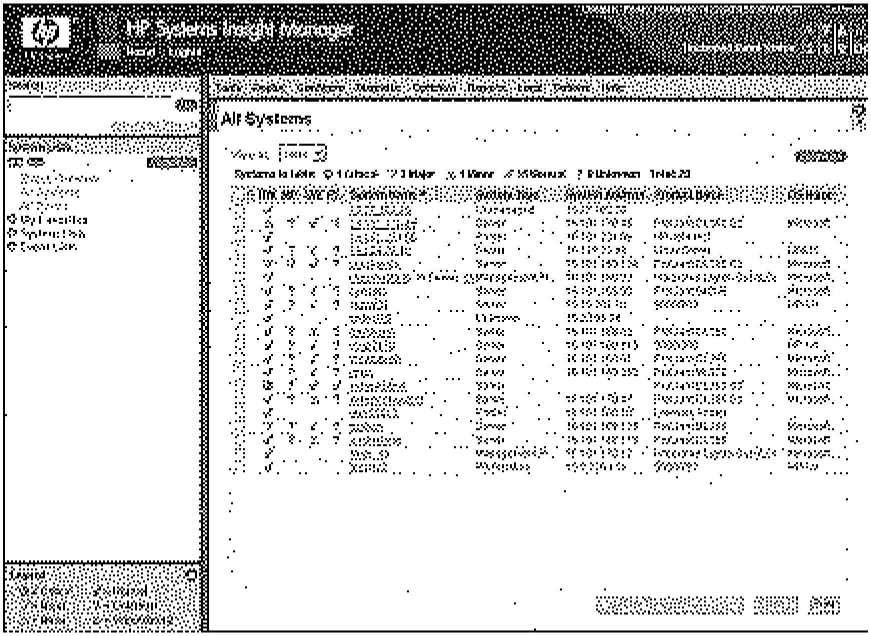
System Insight Manager Identification and Association

Systems Insight Manager can identify an iLO processor and create an association between iLO and server. The administrator of the iLO device may configure iLO to respond to Systems Insight Manager identification requests.

System Insight Manager Status

In Systems Insight Manager, iLO is identified as a management processor. Systems Insight Manager displays the management processor status within the systems list.

The iLO management processor is displayed as an icon in the device list on the same row as its host server. The color of the icon represents the status of the management processor.



For a complete list of device statuses, refer to the *HP Systems Insight Manager Installation and User Guide.*

System Insight Manager Links

For ease of management, Systems Insight Manager creates links to the following locations:

- iLO and the host server from any System list
- The server from the System Page of iLO
- iLO from the System Page of the server

The Systems List pages display iLO, the server, and the relationship between iLO and server. For example, the page can display the server, the iLO name next to the server, and *iLO name* **IN** *server* in the System Name field for iLO.

Clicking on a status icon for iLO takes you to the iLO Web interface. Clicking on the hardware status icon takes you to the Insight Management Agents for the device. Clicking on the iLO or server name takes you to the System Page of the device. Within the System Page are the Identity, Links, and Event tabs. These tabs provide identity and status information, event information, and links for the associated device.

System Insight Manager Systems Lists

iLO management processors can be viewed within Systems Insight Manager. The administrator can create and use customized system lists to group management processors. Refer to the *HP Systems Insight Manager Installation and User Guide* for further details.

Configuring System Insight Manager Identification of iLO

iLO enables you to set how much data is returned on an Systems Insight Manager request for more information. Refer to "Configuring Identification of iLO (on page 226)."

Receiving SNMP Alerts in Systems Insight Manager

iLO can be configured to forward alerts from the host operating system management agents, and it can also be configured to send iLO-generated alerts to Systems Insight Manager.

Systems Insight Manager provides support for full SNMP management, and iLO supports SNMP trap delivery to Systems Insight Manager. You can view the event log, select the event, and view the additional information about the alert.

Configuring receipt of SNMP alerts in Systems Insight Manager is a two-step process. The process requires Systems Insight Manager to discover iLO and configuring iLO to enable SNMP alerts.

1. To enable iLO to send SNMP traps click **SNMP/Insight Manager Settings** on the Administration tab of the iLO navigation frame to enable SNMP alerting and to provide an SNMP trap IP address to iLO. This IP address should be the address of the computer running Systems Insight Manager. Refer to the "Enabling SNMP Alerts (on page 96)" section for details.
2. To discover iLO in Systems Insight Manager configure iLO as a managed device for Systems Insight Manager. Adding iLO to Systems Insight Manager allows the NIC interface on iLO to function as a dedicated management port, isolating management traffic from the remote host server NIC interface.
    a. Start Systems Insight Manager. Click **Options>Discovery>Automatic Discovery** to discover any iLO devices to be managed by Systems Insight Manager.
    b. Select **IP range pinging** and, if the IP address does not already appear in the Ping Inclusion Ranges section, enter the IP address.
    c. Click **Save and Run** to add iLO to Systems Insight Manager. After the discovery is complete, subsequent queries will display the device as a management processor.

d. You may need to edit the SNMP monitor community string (for example, by changing it to "public") so that iLO is displayed in the list of monitored devices. The SNMP read community string can be changed by accessing the Systems Protocol Settings page. Click Options>Protocol Settings>System Protocol Settings.

   Another option is to click **Options>Protocol Settings>Global Protocol Settings** and set community strings to use during discovery under Default SNMP Settings. When set, you can use steps a through c to run Discovery again.

For major, uncleared events, iLO traps are displayed in All Events. You can also use the orange button at the top of the screen to obtain the major uncleared events. Click the **Event Type** to obtain further information about the event.

NOTE: HP Insight Agents for iLO must be installed on the remote host server to enable management of iLO. Refer to "Installing iLO Device Drivers (on page 24)" for additional details about installing and configuring agents.

System Insight Manager Port Matching

Systems Insight Manager is configured to start an HTTP session to check for iLO at port 80. The port can be changed. If you want to change the port number, you must also change it in Network Settings and Systems Insight Manager.

To change the port number in Systems Insight Manager, add the port to the config\identification\additionalWsDisc.props file in the directory where Systems Insight Manager is installed. The entry must start with the HTTP port for iLO. No entry needs to be in this file for iLO if it remains at the standard Port 80. It is very important that the entry is on a single line and the port number is first, with all other items identical to the following example (including capitalization).

The following example shows what the entry is if iLO is to be discovered at port 55000 (this should all be on one line in the file):

```
55000=iLO, ,true,false,com.hp.mx.core.tools.identificati
on.mgmtproc.MgmtProcessorParser
```

Reviewing iLO Advanced Pack License Information in Systems Insight Manager

Systems Insight Manager allows you to display the license status of the iLO management processors. You may use this information to determine how many and which iLO devices are licensed for the iLO Advanced Pack.

To view license information, click **Deploy>License Manager>Collect Keys.** To be sure the data is current, run the identify systems task for your management processors. Refer to the Systems Insight Manager documentation for additional details about initiating tasks.

System Insight Manager ProLiant BL p-Class Rack Visualization

HP System Insight Manager provides comprehensive management of ProLiant BL p-Class server blades. HP System Insight Manager enables systems administrators to quickly identify hardware failures, isolate and update systems running out-of-date system software, and easily access onboard management resources. In addition, HP System Insight Manager 4.1 and above provides visualization support for ProLiant BL p-Class server blades which enables you to quickly view the configuration of the server blades within a server blade enclosure and speeds access to the HP Insight Management Agents, Version Control Agents, and iLO Remote Console.

Group Administration and iLO Scripting

In This Section

Lights-Out Configuration Utility

The Lights-Out Configuration Utility (CPQLOCFG.EXE) is a Windows®-based utility that connects to iLO using a secure connection over the network. RIBCL scripts are passed to iLO over the secure connection to CPQLOCFG. This utility requires a valid user ID and password with the appropriate privileges. The CPQLOCFG utility can be launched from Insight Manager 7 or Systems Insight Manager for Group Administration or used independently from a command prompt for batch processing. This utility can be downloaded from the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Version 2.20 or later of CPQLOCFG.EXE is required to configure iLO Directory Settings using RIBCL scripts.

Insight Manager 7 and System Insight Manager discover iLO devices as management processors. The Lights-Out Configuration Utility sends a RIBCL file to a group of iLO processors to manage the user accounts for those iLO processors. iLO processors then perform the action designated by the RIBCL file and send a response to the log file.

The Lights-Out Configuration Utility is used to execute RIBCL scripts on iLO and must reside on the same server as Insight Manager 7 or Systems Insight Manager. The Lights-Out Configuration Utility generates two types of error messages: runtime and syntax.

- Runtime errors occur when an invalid action is requested. Runtime errors are logged to the following directories:

  - Insight Manager 7—C:\PROGRAM FILES\INSIGHT MANAGER 7
  - Systems Insight Manager—
    C:\PROGRAM FILES\INSIGHT MANAGER\HP\SYTEMS
- Syntax errors occur when an invalid XML tag is encountered. When a syntax error occurs, the Lights-Out Configuration Utility stops running and logs the error in the runtime script and output log file.

  Syntax errors take the format of "Syntax error: expected 'x' but found 'y'" as shown in the following example: `Syntax error: expected USER_LOGIN=userlogin` but found `USER_NAME=username`.

Refer to the RIBCL section ("Remote Insight Command Language" on page 269) for a complete listing of errors.

Group Administration Using the Lights-Out Configuration Utility

The IT administrator can manage multiple iLO processors through Insight Manager 7. The components of Group Administration are:

- Insight Manager 7
  - RIBCL ("Remote Insight Command Language" on page 269)
  - Lights-Out Configuration Utility (on page 241)
  - Query Definition in Insight Manager 7 ("Query Definition in Insight Manager 7" on page 243)
  - Application Launch ("Application Launch Using Insight Manager 7" on page 244)
- System Insight Manager
  - RIBCL ("Remote Insight Command Language" on page 269)
  - Lights-Out Configuration Utility (on page 241)
  - Create a Customized List (on page 245)
  - Create a Custom Command (on page 245)

- Create a Task (on page 246)

Using the Lights-Out Configuration Utility with Insight Manager 7

Insight Manager 7 can manage the group administration of iLO devices using query definitions ("Query Definition in Insight Manager 7" on page 243) and Application Launch ("Application Launch Using Insight Manager 7" on page 244).

Query Definition in Insight Manager 7

To group all of the LOM devices, log in to Insight Manager 7 and create a query.

To create the query:

1. Log in to Insight Manager 7.
2. Click **Device** in the navigation bar on the top left side of the screen.
3. Click **Queries,** then click **Device.**
4. Locate the Personal Queries section in the main window. If a query category exists, proceed to step 7, otherwise proceed to step 5.
5. Click **New** to create a new category. For this example, the name of the new category is RIB Cards. Click **Create Category.**
6. Click **Queries** to return to the Device Queries screen.
7. Click **New,** within the appropriate query category, to open the Create/Edit Query screen where the query definition is created.
8. Define the query name, for example "Mgmt Processors."
9. Select **Device(s) of type** and then select **Devices by product name.** In the criteria windows, set the product name to **Integrated Lights-Out.**
10. Click **type** in the Query Description field. A pop-up window opens where you define the device type.
11. Select **Management Processor** and click **OK.**
12. Click **Save** to return to the Device Query screen.
13. Find the newly created query in the appropriate query category and click the query name to run it for verification.

14. Click **Overview** on the left side of the screen after the verification has taken place. The initial page for devices opens.

Application Launch Using Insight Manager 7

The Application Launch combines the RIBCL, the Lights-Out Configuration Utility, and the query definition to manage the Group Administration of iLO management processors.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task.** A drop-down menu is displayed.
4. Click **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
5. Enter the full path and name for the Lights-Out Configuration Utility in the area provided. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
6. Enter the parameters in the area provided. Insight Manager 7 requires the following parameters for the Lights-Out Configuration Utility:

   -F is the full path of the RIBCL file name.

   -V is the verbose message (optional).

   If the RIBCL file is in the root directory of on the C:\ drive, then the parameters are:

   ```
   -F C:\MANAGEUSERS.xml -V
   ```

   > **NOTE:** The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

7. Click **Next.** A screen displays the options for naming the task, defining the query association, and setting a schedule for the task.
8. Enter a task name in the Enter a name for this task field.
9. Select the query that had been created earlier, for example "Mgmt Processors."

10. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window is displayed.
11. Click **OK** to set the schedule.

    NOTE: The default schedule for a control task is **Now.**

12. Click **Finish** to save the Application Launch task.
13. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

Lights-Out Configuration Utility for Systems Insight Manager

Using CPQLOFGC with System Insight Manager requires:

1. Creating a customized list
2. Creating a custom command
3. Creating a task

Create a Customized List

A customized list allows you to create a list of a group of management processors and run a task on that list. To create a customized list:

1. In the Systems List pane in the left window, click **Customize.**
2. In the Customize Lists window, select System List using the Show dropdown menu and click **New List.**
3. Select the search parameters using the **Search for** and **where** dropdown menus. Click **Go.**
4. When the systems display, click **Save As.**
5. Enter a name for your list and where it is to be saved.
6. Click **OK.**

Create a Custom Command

To create a custom command:

1. Click **Tools>Custom Commands>New Custom Command.**

2. In the New Custom Command screen, enter the appropriate information in the **Name, Description,** and **Comments** fields.
3. In the Command field, be sure to enter the full path and the file name of the application. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
4. Enter the Parameters.
5. Enter the Variable Name and Value. Click Add after entering each set of variables and values. To clear an added variable, select the variable, and click **Delete.**
6. After entering the Custom Command information, click **OK.** The new tool is added to the dropdown menu Tools>Custom Commands.

Create A Task

Create a task to execute a custom command on specific systems or events.

1. Select the custom command from the Tools>Custom Commands dropdown menu. The Target Selection page is displayed.
2. Choose targets by selecting either:
   - **All systems in the list**—Selecting an option in the drop-down menu automatically targets all systems in that list.
   - **Individual systems in the list**—Selecting an option in the drop-down menu displays the available systems for the selected list. Select the target system.
3. Click **Apply Selections.** The items selected display in the Verify Target Systems page.

   If the systems selected are not compatible with the tool, the Tool Launch OK column provides a brief explanation of the problem. To change the selected target list click **Change Targets.** If you want to remove the system selected, click **Remove** and you will return to the Select Target Systems page.
4. Click **Next** to specify the tool parameters.

   The Next option displays only if the tool parameters need to be specified.
5. Click either **Schedule** or **Run Now.**

- If you click **Schedule,** the schedule task screen appears. Schedule the task. For more information on the scheduling options, see the HP Systems Insight Manager documentation.

  The Schedule option is available only if the tool can be scheduled.

- If you click **Run Now,** the Task Results screen appears with a summary of the task, the target details, and the status.

Batch Processing Using the Lights-Out Configuration Utility

Group Administration can also be delivered to iLO through batch processing. The components used by batch processing are the Lights-Out Configuration Utility, an RIBCL file, and a batch file.

The following example shows a sample batch file that can be used to perform the Group Administration for iLO:

```
REM Updating the Integrated Lights-Out board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V
```

The Lights-Out Configuration Utility overwrites any existing log files.

Lights-Out Configuration Utility Parameters

- -S is the switch that determines the iLO that is to be updated. This switch is either the DNS name or IP address of the target server.

  Do **not** use this switch if you are launching from Insight Manager 7 or Systems Insight Manager. Insight Manager 7 and Systems Insight Manager will provide the address of the iLO when CPQLOCFG.EXE is launched.

- -F is the switch that gives the full path location and name of the RIBCL file that contains the actions to be performed on the board.
- -U and -P specify the user login name and password.

Be sure that the Lights-Out Configuration Utility is in a directory referenced by the PATH environment variable. Any log files generated are placed in the same directory as the Lights-Out Configuration Utility executable

The switches -L and -V might or might not be set depending on the IT administrator's preferences.

- -L is the switch that defines where the log file will be generated and what the file name will be. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch CPQLOCFG.

  Do **not** use this switch if launching from Insight Manager 7 or Systems Insight Manager.

  > **NOTE:** The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

- -V is the optional switch that turns on the verbose message return. The resulting log file contains all commands sent to the Remote Insight board, all responses from the Remote Insight board, and any errors. By default, only errors and responses from GET commands are logged without this switch.

Refer to the "Remote Insight Command Language (on page 269)" section for information on the syntax of the XML data files. Sample XML scripts are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

Lights-Out DOS Utility

In This Section

Overview of the Lights-Out DOS Utility

CPQLODOS is a command line utility that is a part of the SmartStart Scripting Toolkit. It is intended to be an initial configuration program to set up only those iLO settings necessary to allow one of the other full-featured configuration methods. Because of this limited usage model, it processes only a small subset of the iLO scripting language.

CPQLODOS is a DOS-only tool that requires MS-DOS® 6.22. CPQLODOS can also be executed from a DOS-bootable diskette or a PXE diskette image as part of the SmartStart Scripting Tool kit. Lights-Out scripting is not supported on Linux operating systems or when using the Novell NetWare Client. This utility does not require a user ID or password because it is executed locally.

CPQLODOS enables you to configure features exposed through F8 startup or the GUI. CPQLODOS processes an XML file with the configuration settings to the iLO in the server on which CPQLODOS is executing. The RIBCL should be used to administer user rights and network functionality on the server.

CPQLODOS is primarily a reconfiguration tool. Any existing configuration will be removed. This utility is not intended for continued administration.

CPQLODOS Recommended Usage

HP recommends using CPQLODOS /WRITE_XML=filename.ext to capture the current iLO settings. The output from the /WRITE_XML command should be used as a template for further CPQLODOS scripting.

For security reasons, the /WRITE_XML command does not output the passwords for current user accounts or the iLO Advanced Pack license key.

Edit the template file created with the /WRITE_XML parameter to reflect the desired configuration.

Use CPQLODOS /LOAD_XML=filename.ext to reset the iLO to its factory-default settings, then apply the settings in the XML scripts file.

CPQLODOS General Guidelines

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

Command Line Arguments

All of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allow the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

The following table lists the arguments recognized by CPQLODOS.

Command Line Argument	Description
/HELP or /?	Displays simple help messages
/DETECT	Detects the iLO management processor on the target server
/RESET	Resets the iLO management processor
/VIRT_FLOPPY	Ignores the virtual floppy inserted error
/MIN_FW-xxx	Enables you to set the minimum firmware version on which the iLO management processor runs
/GET_STATUS	Returns the status of the iLO management processor
/GET_HOSTINFO	Retrieves and displays the current host server information on the iLO management processor and displays the server name and number
/GET_USERINFO	Obtains the current users stored in the iLO management processor board and displays the names, login names, and security mask information
/GET_NICCONFIG	Retrieves and displays the NIC settings stored in the iLO management processor
/GET_DHCPCONFIG	Retrieves and displays the DHCP settings stored in the iLO management processor
/GET_DIRCONFIG	Retrieves and displays the DIRECTORY settings in the iLO management processo
/WRITE_XML=path\file name.ext	Reads the settings on the iLO management processor and writes the NIC, DHCP, DIRECTORY, and user settings into an XML hardware configuration script file
/LOAD_XML=path\file name.ext	Loads the script file and applies its changes to the current configuration on the iLO management processor
/VERIFY_XML	Verifies the accuracy of the script file and generates an error message for any incorrect data

RIBCL XML Commands for CPQLODOS

CPQLODOS uses the same RIBCL XML commands as CPQLOCFG for the <MOD_NETWORK_SETTINGS>, and the <MOD_DIR_CONFIG> XML scripting language blocks. Only those parameters unique to CPQLODOS are discussed. For more information on <MOD_NETWORK_SETTINGS>, and <MOD_DIR_CONFIG> refer to:

- MOD_NETWORK_SETTINGS (on page 289)
- MOD_DIR_CONFIG

The following XML blocks are unique to CPQLODOS:

- CPQLODOS (on page 252)
- ADD_USER
- SET_LICENSE (on page 254)

CPQLODOS

This command is used to start and end a CPQLODOS session. It can be used only once in a script, and it must be the first and last statement in an XML script.

Example:

```
<CPQLODOS VERSION="2.0">
</CPQLODOS>
```

CPQLODOS Parameter

VERSION is a numeric string that indicates the version of CPQLODOS necessary to process this script. The VERSION string is compared to the version that CPQLODOS can process. An error is returned if the version of CPQLODOS and the version of the script do not match. The VERSION parameter can never be blank.

CPQLODOS Runtime Error

The possible CPQLODOS error messages include `Version must not be blank.`

ADD_USER

This command is used to add a user to iLO. If multiple ADD_USER commands are in the XML script, CPQLODOS will use only the settings from the last command.

Example:

```
<ADD_USER
   USER_NAME = "James Madison"
   USER_LOGIN = "jmadison"
   PASSWORD = "president">
</ADD_USER>
```

ADD_USER Parameters

USER_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

There are no user privilege parameters when ADD_USER is used with CPQLODOS. The added user will have all privileges.

ADD_USER Runtime Errors

- Login name is too long. Maximum length is 39 characters.
- Password is too short. Minimum length is 8 characters.
- Password is too long. Maximum length is 39 characters.
- Blank user name not allowed. Maximum length is 39 characters.

- Blank user login name not allowed. Maximum length is 39 characters.

SET_LICENSE

This command is used to apply the iLO Advanced Pack License key to the iLO. On a ProLiant BL p-class server, this parameter is not necessary because the advanced features are activated by default.

Example:

```
<SET_LICENSE>
   <LICENSE_KEY VALUE = "12345ABCDE12345FGHIJ12345"/>
</SET_LICENSE>
```

SET_LICENSE Parameter

LICENSE_KEY is the text value of the iLO Advanced Pack activation key. This is a 25-byte, alphanumeric string. Do not include any hyphens or spaces in the string.

SET_LICENSE Runtime Errors

The possible SET_LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

Perl Scripting

In This Section

Using Perl with the XML Scripting Interface

The scripting interface provided enables administrators to manage virtually every aspect of the device in an automated fashion. Primarily, administrators use tools like the `cpqlocfg.exe` to assist deployment efforts. Administrators using a non-Windows® client can use Perl scripts to send XML scripts to the Lights-Out devices. Administrators can also use Perl to perform more complex tasks than `cpqlocfg.exe` can perform.

This section discusses how to use Perl scripting in conjunction with the Lights-Out XML scripting language. Perl scripts require a valid user ID and password with appropriate privileges. Sample XML scripts for Lights-Out devices and a sample Perl script are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

XML Enhancements

Previous versions of iLO firmware do not return properly formatted XML syntax. This issue has been addressed in iLO 1.50 when the client parsing utility is properly configured. If the iLO firmware determines the client utility being used does not support the return of properly formatted XML syntax, the following message appears:

```
<INFORM>Scripting utility should be updated to the
latest version.</INFORM>
```

This message informs the customer to update to a later version of the cpqlocfg scripting utility. The latest version of cpqlocfg.exe is currently 2.21.

For customers using a utility other than cpqlocfg.exe, such as Perl scripts, the following steps can help ensure the iLO firmware returns properly formatted XML. Assuming the version of firmware is 1.50, `<LOCFG version="2.21">` should be incorporated into the script sent to iLO. This tag can be placed in either the Perl script or the XML script. Placement of this tag is important. If placing this tag in the Perl script, the tag should be sent after `<?xml version="1.0"?>` and before the XML script is sent. If placing the tag in the XML script, the tag should be placed before `<RIBCL version="2.0">.` If you are using the Perl script provided by HP, then the bold line in the following example can be added to return properly formatted XML syntax.

- Perl script modification

```
…
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr =>
$host);
open(F, "<$file") || die "Can't open $file\n";

# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
#Send tag to iLO firmware to insure properly formatted
XML is returned.
print $client '<LOCFG version="2.21">' . "\r\n";
…
```

- XML script modification

```
<!--
The bold line could be added for the return of properly
formatted XML.
-->
<LOCFG version="2.21"/>
<RIBCL version="2.0">
   <LOGIN USER_LOGIN="Adminname" PASSWORD = "password">
      <!--
      Add XML script here.
      -->
   </LOGIN>
</RIBCL>
</LOCFG>
```

Opening an SSL Connection

Perl scripts must open an SSL connection to the device's HTTPS port, by default port 443. For example:

```
use Socket;
use Net::SSLeay qw(die_now die_if_ssl_error);

Net::SSLeay::load_error_strings();
Net::SSLeay::SSLeay_add_ssl_algorithms();
Net::SSLeay::randomize();

#
# opens an ssl connection to port 443 of the passed host
#
sub openSSLconnection($)
{
   my $host = shift;
   my ($ctx, $ssl, $sin, $ip, $nip);

   if (not $ip = inet_aton($host))
   {
      print "$host is a DNS Name, performing lookup\n" if
      $debug;
      $ip = gethostbyname($host) or die "ERROR: Host
      $hostname not found.\n";
   }
   $nip = inet_ntoa($ip);
   print STDERR "Connecting to $nip:443\n";

   $sin = sockaddr_in(443, $ip);
   socket  (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR:
   socket: $!";
   connect (S, $sin) or die "connect: $!";

   $ctx = Net::SSLeay::CTX_new() or die_now("ERROR:
   Failed to create SSL_CTX $! ");
   Net::SSLeay::CTX_set_options($ctx,
   &Net::SSLeay::OP_ALL);
   die_if_ssl_error("ERROR: ssl ctx set options");
   $ssl = Net::SSLeay::new($ctx) or die_now("ERROR:
   Failed to create SSL $!");
   Net::SSLeay::set_fd($ssl, fileno(S));
```

```
    Net::SSLeay::connect($ssl) and
    die_if_ssl_error("ERROR: ssl connect");
    print STDERR 'SSL Connected ';
    print 'Using Cipher: ' .
    Net::SSLeay::get_cipher($ssl) if $debug;
    print STDERR "\n\n";

    return $ssl;
}
```

Sending the XML Header and Script Body

After the connection is established, the first line of script sent must be an XML document header, which tells the device's HTTPS Web server that the following content is an XML script. The header must match the header used in the example exactly. After the header has been completely sent, the remainder of the script can be sent. In this example, the script is sent all at once. For example:

```
# usage: sendscript(host, script)
# sends the xmlscript script to host, returns reply
sub sendscript($$)
{
    my $host = shift;
    my $script = shift;
    my ($ssl, $reply, $lastreply, $res, $n);

    $ssl = openSSLconnection($host);

    # write header
    $n = Net::SSLeay::ssl_write_all($ssl, '<?xml
    version="1.0"?>'."\r\n");
     rint "Wrote $n\n" if $debug;

    # write script
    $n = Net::SSLeay::ssl_write_all($ssl, $script);
    print "Wrote $n\n$script\n" if $debug;

    $reply = "";
    $lastreply = "";

    READLOOP:
    while(1)
    {
      $n++;
      $reply .= $lastreply;
      $lastreply = Net::SSLeay::read($ssl);
      die_if_ssl_error("ERROR: ssl read");
      if($lastreply eq "")
      {
      sleep(2); # wait 2 sec for more text.
      $lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
      }
      sleep(2); # wait 2 sec for more text.
      $lastreply = Net::SSLeay::read($ssl);
      last READLOOP if($lastreply eq "");
      }
      print "READ: $lastreply\n" if $debug;
      if($lastreply =~ m/STATUS="(0x[0-9A-
      F]+)"[\s]+MESSAGE=
      '(.*)'[\s]+\/>[\s]*(([\s]|.)*?)<\/RIBCL>/)
      {
      if($1 eq "0x0000")
      {
      print STDERR "$3\n" if $3;
      }
      else
      {
      print STDERR "ERROR: STATUS: $1, MESSAGE: $2\n";
      }
      }
   }
   $reply .= $lastreply;
   closeSSLconnection($ssl);
   return $reply;
}
```

PERL scripts can also send a portion of the XML script, wait for the reply, and send more XML later. Using this technique, it is possible to use the reply produced by an earlier command as input to a later command. However, the PERL script must send data within a few seconds or the device will time out and disconnect.

When using the XML scripting interface with PERL scripts, the following restrictions apply:

- PERL scripts must send the XML header before sending the body of the script.
- PERL scripts must provide script data fast enough to prevent the device from timing out.
- XML scripts cannot contain the update firmware command, which requires extra work on the part of the PERL script to open the file containing the firmware image and send it to the device.
- Only one XML document is allowed per connection, which means one pair of RIBCL tags.
- The device will not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

HPONCFG Online Configuration Utility

In This Section

HPONCFG

HPONCFG is an online configuration tool for Linux and Microsoft® Windows® used to set up, configure, and operate iLO and RILOE II from the host. The utility runs in a command line mode and must be executed from the operating system administrator or root context.

HPONCFG takes RIBCL scripts and passes them to the iLO in the host system instead of over the network. HPONCFG replaces the control panel applet used with RILOE.

You can download HPONCFG from the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

HPONCFG Supported Operating Systems

HPONCFG is supported on:

- Windows® NT Server
- Windows® 2000 Server
- Windows® 2003 Server
- Red Hat Linux 7.2
- Red Hat Linux 7.3

- Red Hat Linux 8.0
- SLES 7
- United-Linux 1.0

HPONCFG Requirements

HPONCFG requires that the appropriate management interface driver be installed. The drivers are provided with SmartStart or can be downloaded from the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

HPONCFG is supported on the following firmware:

- iLO 1.41 or later
- RILOE II 1.13 or later

HPONCFG Installation and Usage

Before installing and running HPONCFG, be sure the appropriate management interface driver is installed. Refer to the "HPONCFG Requirements (on page 262)" section. For both iLO-based servers and RILOE II-based servers, sm2user.dll must be loaded on the server. This file is automatically loaded along with the HP Insight Management Agents.

During execution, HPONCFG will display an error message if the sm2user.dll file cannot be found. This file can be installed separately from the component HP Insight Management Agents for Windows® 2000 or Windows® Server 2003, component number CP003732, which can be downloaded as a part of the ProLiant Support Pack on the HP website (http://h18004.www1.hp.com/support/files/server/us/download/18416.html).

After downloading the ProLiant Support Pack, extract the contents to a temporary directory. In the temporary directory, locate CP003732.exe. Extract the contents of CP003732.exe to a temporary directory. In the temporary directory, locate the subdirectory cqmgserv. The sm2user.dll file can be found in this subdirectory. Copy sm2user.dll to the Winnt\system32\ directory on the server.

Windows Server Installation

1. To install HPONCFG, run the self-extracting executable delivered in the Softpaq from within a directory of your choice on the managed server.

   Choose the directory from which the HPONCFG utility is executed. This directory will also contain the XML formatted input scripts and store the output files from execution of the utility.

2. Unzip all files in the delivered zip file HPONCFG.ZIP to the same directory.

Linux Server Installation

1. Copy the file hponcfg-1.00.tar.gz to a temporary directory on the managed server.
2. Use the tar utility to extract all of the files. The package contains the following files:
   - hponcfg-1.0.rh72-0.1.i386.rpm (RPM package for Red Hat 7.2)
   - hponcfg-1.0.rh73-0.1.i386.rpm (RPM package for Red Hat 7.3)
   - hponcfg-1.0.rh8-0.1.i386.rpm (RPM package for Red Hat 8.0)
   - hponcfg-1.0.sles7-0.1.i386.rpm (RPM package for SLES 7)
   - hponcfg-1.0.ul10-0.1.i386.rpm (RPM package for United Linux 1.0)
3. Install the appropriate package using the RPM installation utility. The HPRSM RPM package must be installed before installing the HPONCFG RPM package.

   Example:

   HPNOCFG RPM can be installed on Red Hat 8.0 by using the following command:

   ```
   rpm -ivh hponcfg-1.0.rh8-0.1.i386.rpm
   ```
4. Unzip all files in the delivered zip file, HPONCFG sample scripts.zip, to a working directory.
5. After installation, run the HPONCFG executable found in the /sbin directory.

Using HPONCFG

Start the HPONCFG configuration utility from the command line. When using Microsoft® Windows®, cmd.exe is available by selecting **Start>Run>cmd.** HPONCFG displays a usage page if HPONCFG is entered with no command line parameters. HPONCFG accepts a correctly formatted XML script. Refer to the "Remote Insight Command Language (on page 269)" section for more information on formatting XML scripts. HPONCFG sample scripts are included in the HPONCFG package.

The command line format is:

```
HPONCFG [/help][/?][/reset][/f filename][/l filename][/w
filename][/get_hostinfo][/m firmwarelevel][/mouse |
/mouse /dualcursor | /mouse /allusers]
```

HPONCFG Command Line Parameters

HPONCFG accepts the following command line parameters:

- /help or /?—Displays the help page.
- /reset—Resets the RILOE II or iLO to factory default values.
- /f filename—Sets the RILOE II or iLO configuration from the information given in the XML input file that has name "filename."
- /w filename—Writes the RILOE II or iLO configuration obtained from the device to the XML output file that has name "filename."
- /l filename—Log replies to the text log file that has name "filename."
- /get_hostinfo—Gets the host information. Returns the server name and server serial number.
- /m—Indicates to HPONCFG the minimum firmware level that should be present in the management device ito execute the RIBCL script. If at least this level of firmware is not present, HPONCFG returns an error without performing any additional action.
- /mouse—Configures the server for optimal mouse handling.

Example HPNOCFG command line:

```
HPONCFG /f add_user.xml /l log.txt > output.txt
```

HPONCFG Usage Model

HPONCFG is best used to configure iLO after the host operating system has been deployed or redeployed to:

- Capture iLO configuration parameters.
- Create a known user account.

Obtaining an Entire Configuration

HPONCFG and RIBCL can retrieve the current Lights-Out configuration. HPONCFG can obtain an entire configuration from an iLO or a RILOE II, except for user passwords. User passwords are not returned for security reasons. If completed successfully, HPONCFG indicates that it obtained the data and generated the output file as requested.

The sample configuration file was generated using the following command:

```
HPONCFG /w config.xml
```

The following is a typical configuration output file:

```
<HPONCFG VERSION = "2.0">
   <!--- Generated 04/15/04 15:20:36 --->
   <MOD_DIR_CONFIG>
      <DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
      <DIR_LOCAL_USER_ACCT VALUE = "Y"/>
      <DIR_SERVER_ADDRESS VALUE = ""/>
      <DIR_SERVER_PORT VALUE = "636"/>
      <DIR_OBJECT_DN VALUE = ""/>
      <DIR_OBJECT_PASSWORD VALUE = ""/>
      <DIR_USER_CONTEXT_1 VALUE = ""/>
      <DIR_USER_CONTEXT_2 VALUE = ""/>
      <DIR_USER_CONTEXT_3 VALUE = ""/>
   </MOD_DIR_CONFIG>
   <MOD_NETWORK_SETTINGS>
      <SPEED_AUTOSELECT VALUE = "Y"/>
      <NIC_SPEED VALUE = "100"/>
      <FULL_DUPLEX VALUE = "Y"/>
      <IP_ADDRESS VALUE = "192.168.1.1"/>
      <SUBNET_MASK VALUE = "255.255.252.0"/>
      <GATEWAY_IP_ADDRESS VALUE = "192.168.1.254"/>
      <DNS_NAME VALUE = "ILOD234KJ44D002"/>
      <PRIM_DNS_SERVER value = "192.168.1.254"/>
      <DHCP_ENABLE VALUE = "Y"/>
      <DOMAIN_NAME VALUE = "corp.net"/>
      <DHCP_GATEWAY VALUE = "Y"/>
      <DHCP_DNS_SERVER VALUE = "Y"/>
      <DHCP_STATIC_ROUTE VALUE = "Y"/>
      <DHCP_WINS_SERVER VALUE = "Y"/>
      <REG_WINS_SERVER VALUE = "Y"/>
      <PRIM_WINS_SERVER value = "192.168.1.254"/>
      <STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY =
      "0.0.0.0"/>
      <STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY =
      "0.0.0.0"/>
      <STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY =
      "0.0.0.0"/>
   </MOD_NETWORK_SETTINGS>
   <ADD_USER
      USER_NAME = "Administrator"
      USER_LOGIN = "Administrator"
      PASSWORD = "">
      </ADD_USER>
      <ADD_USER
      USER_NAME = "supervisor"
      USER_LOGIN = "supervisor"
      PASSWORD = "">
   </ADD_USER>
   <RESET_RIB VALUE = "Y"/>
</HPONCFG>
```

Creating a User Account

If iLO user credentials are unknown, an account on iLO can be created using HPONCFG. HPONCFG runs from the host operating system context, requiring administrator or root access to the operating system.

HPNOCFG can send a specific configuration to the iLO or RILOE II by using the following command:

```
HPONCFG /f add_user.xml /l log.txt
```

Sample add_user.xml input file:

```
<!-- Add user with remote power and access privileges --
>
<RIBCL version="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
   <USER_INFO MODE="write">
   <ADD_USER USER_NAME="Adam Smith" USER_LOGIN="Adam"
   PASSWORD="password">
      <ADMIN_PRIV="N">
      <REMOTE_CONS_PRIV="Y"
      <RESET_SERVER_PRIV="Y"
      <VIRTUAL_MEDIA_PRIV="Y"
      <CONFIG_ILO_PRIV="N"
   </ADD_USER>
   </USER_INFO>
</LOGIN>
</RIBCL>
```

Remote Insight Command Language

In This Section

Overview of the Remote Insight Board Command Language

The Remote Insight Board Command Language enables you to write scripts to manage user accounts and to configure settings.

IMPORTANT: Comments should not interrupt a command. If they do, an error message will be generated.

RIBCL and ProLiant BL p-Class Servers

The "Remote Insight Command Language" section describes the XML commands and their parameters common to most LOM products and servers. For more information on ProLiant BL p-class server and rack XML commands, refer to the "BL p-Class Configuration ("ProLiant BL p-Class Configuration" on page 31)" section.

RIBCL Sample Scripts

Sample scripts for all iLO commands described in this section are available for download from the HP website (http://www.hp.com/servers/lights-out).

RIBCL General Guidelines

In this section, all of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allows the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are as follows:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

XML Header

The XML header ensures the connection is an XML connection, not an HTTP connection. The XML header is built into the cpqlocfg utility and has the following format:

```
<?xml version=”1.0”?>
```

Data Types

The three data types that are allowed in the parameter are:

- String

- Specific string
- Boolean string

String

A string is any text enclosed in quotes. It can include spaces, numbers, or any printable character. A string may start with either a double or single quote and it must end with the same type of quote. The string may contain a quote if it is different from the string delimiter quotes.

For example, if a string is started with a double quote, a single quote can be used within the string and the string must be closed with a double quote.

Specific String

A specific string is one that is required to contain certain characters. In general, you have a choice of words that are accepted as correct syntax and all other words produce an error.

Boolean String

A Boolean string is a specific string that specifies a "yes" or "no" condition. Acceptable Boolean strings are "yes," "y," "no," "n," "true," "t," "false," and "f." These strings are not case sensitive.

Response Definitions

Every command that is sent to iLO generates a response. The response indicates whether the command succeeded or failed. Some commands generate additional information. The additional information is displayed in execution sequence, provided that no error occurred.

Example:

```
<RESPONSE
   STATUS=“0x0001”
   MSG=“There has been a severe error.”
```

```
/>
```

- RESPONSE

  This tag name indicates that iLO is sending a response to the previous commands back to the client application to indicate the success or failure of the commands that have been sent to iLO.

- STATUS

  This parameter contains an error number. The number “0x0000” indicates that there is no error.

- MSG

  This element contains a message describing the error that happened. If no error occurred, the message “No error” is displayed.

RIBCL

This command is used to start and end an RIBCL session. You can use it only once to start an RIBCL session, and it must be the first command to display in the script. The RIBCL tags are required to mark the beginning and the end of the RIBCL document.

Example:

```
<RIBCL VERSION="2.0">
</RIBCL>
```

RIBCL Parameter

VERSION is a string that indicates the version of the RIBCL that the client application is expecting to use. The VERSION string is compared to the version of the RIBCL that is expected, and an error is returned if the string and the version do not match. The preferred value for the VERSION parameter is "2.0." The VERSION parameter is no longer checked for an exact match; however, this parameter can never be blank.

RIBCL Runtime Errors

The possible RIBCL error messages include:

Version must not be blank.

LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level will be used when performing RIBCL actions. The specified user must have a valid account on the respective iLO to execute RIBCL commands. The user's privileges are checked against the required privilege for a particular command, and an error is returned if the privilege level does not match.

Example:

```
<LOGIN USER_LOGIN="username" PASSWORD="password">
</LOGIN>
```

Alternatively, the CPQLOCFG utility can specify the login information as parameters on its command line:

```
cpqlocfg  -u <username> -p <password>
```

When using this format, the utility returns an `Overriding credentials` warning message but still shows the error log message entry as `Login name must not be blank.`

LOGIN Parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters.

LOGIN Runtime Errors

The possible runtime error messages include:

- User login name was not found.
- Password must not be blank.

- Logged-in user does not have required privilege for this command.

USER_INFO

The USER_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local user information database into memory and prepares to edit it. Only commands that are USER_INFO type commands are valid inside the USER_INFO command block. The USER_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If database is open for writing by another application, then this call will fail.

Example:

```
<USER_INFO MODE="write">
   ……… USER_INFO commands ……
</USER_INFO>
```

USER_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of iLO information. Read mode prevents modification of the iLO information.

USER_INFO Runtime Error

None

ADD_USER

The ADD_USER command is used to add a local user account. The USER_NAME and USER_LOGIN parameters must not exist in the current user database. Use the MOD_USER command to change an existing user's information. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

All of the attributes that pertain to the user are set using the following parameters.

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="loginname" PASSWORD="password">
   <USER_INFO MODE="write">
   <ADD_USER
      USER_NAME="User"
      USER_LOGIN="username" PASSWORD="password">
      <ADMIN_PRIV value ="No"/>
      <REMOTE_CONS_PRIV value ="Yes"/>
      <RESET_SERVER_PRIV value ="No"/>
      <VIRTUAL_MEDIA_PRIV value ="No"/>
      <CONFIG_ILO_PRIV value ="No"/>
   </ADD_USER>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

ADD_USER Parameters

USER_NAME is the actual name of the user. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

The following parameters are not applicable to a user's privileges in the iLO firmware versions 1.40 and higher. The parameters will parse correctly, but user privileges will not be affected.

VIEW_LOGS_PRIV is a Boolean parameter that gives the user permission to view the iLO system logs. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to view logs. If this parameter is used, the Boolean string value must never be blank.

CLEAR_LOGS_PRIV is a Boolean parameter that gives the user permission to clear the event log. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to clear the iLO event log. If this parameter is used, the Boolean string value must never be blank.

EMS_PRIV is a Boolean parameter that gives the user permission to use the Windows® Server 2003 EMS service. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to use EMS services. If this parameter is used, the Boolean string value must never be blank.

UPDATE_ILO_PRIV is a Boolean parameter that allows the user to copy a new firmware image into the iLO system ROM. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO. If this parameter is used, the Boolean string value must never be blank.

CONFIG_RACK_PRIV is a Boolean parameter that gives the user permission to configure and manage the server rack resources. This parameter is applicable to ProLiant BL p-Class servers only. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to manage or configure rack resources. If this parameter is used, the Boolean string value must never be blank.

DIAG_PRIV is a Boolean parameter that gives the user permission to view diagnostic information about iLO. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have diagnostic privileges. If this parameter is used, the Boolean string value must never be blank.

ADD_USER Runtime Errors

The possible ADD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.

- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.
- User name cannot be blank.
- User login ID cannot be blank.
- Boolean value not specified.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_USER

The DELETE_USER command is used to remove an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname"
   PASSWORD="password">
   <USER_INFO MODE="write">
   <DELETE_USER USER_LOGIN="username"/>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

DELETE_USER Parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

DELETE_USER Runtime Errors

The possible DELETE_USER errors include:

- User information is open for read-only access. Write access is required for this operation.
- Cannot delete user information for currently logged in user.
- User login name was not found.
- User login name must not be blank.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER

The GET_USER command will return a local user's information, excluding the password. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve other user accounts; else the user can only view their individual account information.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_USER USER_LOGIN="username"/>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_USER Parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

GET_USER Runtime Errors

The possible GET_USER error messages include:

- User login name must not be blank.

- User login name was not found.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER Return Messages

A possible GET_USER return message includes:

```
<RESPONSE
   STATUS="0x0000"
   MSG="No Errors"
/>
   <GET_USER
   USER_NAME="Admin User"
   USER_LOGIN= "username"
   ADMIN_PRIV="N"
   REMOTE_CONS_PRIV="Y"
   RESET_SERVER_PRIV="N"
   VIRTUAL_MEDIA_PRIV="N"
   CONFIG_ILO_PRIV value ="No"
/>
```

MOD_USER

The MOD_USER command is used to modify an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege. A user without the administrative privilege can only modify their individual account password.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="write">
   <MOD_USER USER_LOGIN="loginname">
      <USER_NAME value="username"/>
      <USER_LOGIN value="newloginname"/>
      <PASSWORD value="password"/>
      <ADMIN_PRIV value="No"/>
      <REMOTE_CONS_PRIV value="Yes"/>
```

```
            <RESET_SERVER_PRIV value="No"/>
            <VIRTUAL_MEDIA_PRIV value="No"/>
            <CONFIG_ILO_PRIV value="Yes"/>
         </MOD_USER>
         </USER_INFO>
         </LOGIN>
      </RIBCL>
```

MOD_USER Parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

If the following parameters are not specified, then the parameter value for the specified user is preserved.

USER_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

MOD_USER Runtime Errors

The possible MOD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.
- User information is open for read-only access. Write access is required for this operation.
- User login name must not be blank.
- Cannot modify user information for currently logged user.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS

The GET_ALL_USERS command will return all USER_LOGIN parameters in the user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve all user accounts.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_ALL_USERS />
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_ALL_USERS Parameters

None

GET_ALL_USERS Runtime Error

The possible GET_ALL_USERS error messages include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS Return Messages

A possible GET_ALL_USERS return message is:

```
<RESPONSE
   STATUS="0x0000"
   MESSAGE='No Error'
/>
<GET_ALL_USERS>
   <USER_LOGIN VALUE="username"/>
   <USER_LOGIN VALUE="user2"/>
   <USER_LOGIN VALUE="user3"/>
   <USER_LOGIN VALUE="user4"/>
   <USER_LOGIN VALUE="user5"/>
   <USER_LOGIN VALUE="user6"/>
   <USER_LOGIN VALUE="user7"/>
   <USER_LOGIN VALUE="user8"/>
   <USER_LOGIN VALUE="user9"/>
   <USER_LOGIN VALUE="user10"/>
   <USER_LOGIN VALUE=""/>
   <USER_LOGIN VALUE=""/>
</GET_ALL_USERS>
```

A possible unsuccessful request is:

```
<RESPONSE
   STATUS = "0x0001"
   MSG = "Error Message"/>
```

GET_ALL_USER_INFO

The GET_ALL_USER_INFO command will return all local users information in the user database, excluding passwords. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have administrative privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_ALL_USER_INFO />
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_ALL_USER_INFO Parameters

None

GET_ALL_USER_INFO Runtime Errors

The possible GET_ALL_USER_INFO error message include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USER_INFO Return Messages

A possible GET_ALL_USER_INFO return message is:

```
<GET_ALL_USER_INFO/>
   <GET_USER
   USER_NAME="Admin"
   USER_LOGIN="Admin"
   ADMIN_PRIV="Y"
   CONFIG_RILO_PRIV="Y"
   LOGIN_PRIV="Y"
   REMOTE_CONS_PRIV="Y"
   RESET_SERVER_PRIV="Y"
   VIRTUAL_MEDIA_PRIV="Y"
/> ......
The same information will be repeated for all the users.
</GET_ALL_USER_INFO>
```

A possible unsuccessful request is:

```
<RESPONSE
   STATUS = "0x0001"
MSG = "Error Message"/>
```

RIB_INFO

The RIB_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the iLO configuration information database into memory and prepares to edit it. Only commands that are RIB_INFO type commands are valid inside the RIB_INFO command block. The RIB_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:

```
<RIB_INFO MODE="write">
……… RIB_INFO commands ……
</RIB_INFO>
```

RIB_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of iLO information. Read mode prevents modification of iLO information.

RIB_INFO Runtime Errors

None

RESET_RIB

The RESET_RIB command is used to reset iLO. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
   <RIB_INFO MODE = "write">
   <RESET_RIB/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

RESET_RIB Parameters

None

RESET_RIB Runtime Errors

The possible RESET_RIB error message include:

User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_NETWORK_SETTINGS

The GET_NETWORK_SETTINGS command requests the respective iLO network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="read">
   <GET_NETWORK_SETTINGS/>
   </RIB_INFO>
   </LOGIN>
 </RIBCL>
```

GET_NETWORK_SETTINGS Parameters

None

GET_NETWORK_SETTINGS Runtime Errors

None

GET_NETWORK_SETTINGS Return Messages

A possible GET_NETWORK_SETTINGS return message is:

```
<GET_NETWORK_SETTINGS
   <SPEED_AUTOSELECT VALUE="Y"/>
   <NIC_SPEED VALUE="100"/>
   <FULL_DUPLEX VALUE="N"/>
   <DHCP_ENABLE VALUE="Y"/>
   <DHCP_GATEWAY VALUE="Y"/>
   <DHCP_DNS_SERVER VALUE="Y"/>
   <DHCP_STATIC_ROUTE VALUE="Y"/>
```

```
      <DHCP_WINS_SERVER VALUE="Y"/>
      <REG_WINS_SERVER VALUE="Y"/>
      <IP_ADDRESS VALUE="111.111.111.111"/>
      <SUBNET_MASK VALUE="255.255.255.0"/>
      <GATEWAY_IP_ADDRESS VALUE="111.111.111.1"/>
      <DNS_NAME VALUE="test"/>
      <DOMAIN_NAME VALUE="test.com"/>
      <PRIM_DNS_SERVER VALUE="111.111.111.242"/>
      <SEC_DNS_SERVER VALUE="111.111.111.242"/>
      <TER_DNS_SERVER VALUE="111.111.111.242"/>
      <PRIM_WINS_SERVER VALUE="111.111.111.246"/>
      <SEC_WINS_SERVER VALUE="111.111.111.247"/>
      <STATIC_ROUTE_1 DEST VALUE="0.0.0.0"/> <GATEWAY
      VALUE="0.0.0.0"/>
      STATIC_ROUTE_2 DEST VALUE="0.0.0.0"/> GATEWAY
      VALUE="0.0.0.0"/>
      STATIC_ROUTE_3 DEST VALUE="0.0.0.0"/> GATEWAY
      VALUE="0.0.0.0"/>
      WEB_AGENT_IP_ADDRESS VALUE=""/>
   </GET_NETWORK_SETTINGS>
```

A possible unsuccessful request is:

```
   <RESPONSE
      STATUS = "0x0001"
      MSG = "Error Message"/>
```

MOD_NETWORK_SETTINGS

MOD_NETWORK_SETTINGS is used to modify network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

iLO scripting firmware does not attempt to decipher if the network modifications are appropriate for the network environment. When modifying network settings, be aware of the network commands provided to the management processor. In some cases, the management processor ignores commands and no error is returned. For example, when a script includes the command to enable DHCP and a command to modify the IP address, the IP address is ignored. Changing the network settings to values that are not correct for the network environment might cause a loss of connectivity to the iLO.

The iLO management processor reboots to apply the changes after the script has successfully completed. If connectivity is lost to the iLO, use RBSU to reconfigure the network settings to values that are compatible with the network environment. For more information, refer to "iLO RBSU (on page 22)."

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_NETWORK_SETTINGS>
      <ENABLE_NIC value="Yes"/>
      <SPEED_AUTOSELECT value="No"/>
      <SHARED_NETWORK_PORT VALUE="No"/>
      <NIC_SPEED value="100"/>
      <FULL_DUPLEX value="Yes"/>
      <DHCP_ENABLE value="Yes"/>
      <IP_ADDRESS value="192.168.132.25"/>
      <SUBNET_MASK value="255.255.0.0"/>
      <GATEWAY_IP_ADDRESS value="192.168.132.2"/>
      <DNS_NAME value="demorib"/>
      <DOMAIN_NAME value="internal.net"/>
      <DHCP_GATEWAY value="No"/>
      <DHCP_DNS_SERVER value="No"/>
      <DHCP_WINS_SERVER value="No"/>
      <DHCP_STATIC_ROUTE value="No"/>
      <REG_WINS_SERVER value="No"/>
      <REG_DDNS_SERVER value="No"/>
      <PING_GATEWAY value="Yes"/>
      <PRIM_DNS_SERVER value="192.168.12.14"/>
      <SEC_DNS_SERVER value="192.168.12.15"/>
      <TER_DNS_SERVER value="192.168.12.16"/>
      <PRIM_WINS_SERVER value="192.168.145.1"/>
      <SEC_WINS_SERVER value="192.168.145.2"/>
      <STATIC_ROUTE_1 DEST="192.168.129.144"
      GATEWAY="192.168.129.1"/>
      <STATIC_ROUTE_2 DEST="192.168.129.145"
      GATEWAY="192.168.129.2"/>
      <STATIC_ROUTE_3 DEST="192.168.129.146"
      GATEWAY="192.168.129.3"/>
   </MOD_NETWORK_SETTINGS>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

MOD_NETWORK_SETTINGS Parameters

If the following parameters are not specified, then the parameter value for the specified setting is preserved. Zero values are not permitted in some fields. Consequently, an empty string deletes the current value in some fields.

ENABLE_NIC enables the NIC to reflect the state of iLO. The values are "Yes" or "No." It is case insensitive.

SHARED_NETWORK_PORT is used to set the iLO Shared Network Port value. The values are "Yes" or "No." The Shared Network Port command is supported on ProLiant 3xx G4 series servers.

SPEED_AUTOSELECT is a Boolean parameter to enable or disable the iLO transceiver to auto-detect the speed and duplex of the network. This parameter is optional, and the Boolean string must be set to "Yes" if this behavior is desired. If this parameter is used, the Boolean string value must never be left blank. The possible values are "Yes" or "No." It is case insensitive.

FULL_DUPLEX is used to decide if the iLO is to support full-duplex or half-duplex mode. It is only applicable if SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

NIC_SPEED is used to set the transceiver speed if SPEED_AUTOSELECT was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

DHCP_ENABLE is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

IP_ADDRESS is used to select the IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET_MASK is used to select the subnet mask for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY_IP_ADDRESS is used to select the default gateway IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS_NAME is used to specify the DNS name for the iLO. If an empty string is entered, the current value is deleted.

DOMAIN_NAME is used to specify the domain name for the network where the iLO resides. If an empty string is entered, the current value is deleted.

DHCP_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_DNS_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_WINS_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_STATIC_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG_WINS_SERVER specifies if the iLO must be register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM_DNS_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_DNS_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER_DNS_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM_WINS_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_WINS_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC_ROUTE_1, STATIC_ROUTE_2, and STATIC_ROUTE_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.
- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

WEB_AGENT_IP_ADDRESS specifies the address for the Web-enabled agents. If an empty string is entered, the current value is deleted.

MOD_NETWORK_SETTINGS Runtime Errors

The possible MOD_NETWORK_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_GLOBAL_SETTINGS

The GET_GLOBAL_SETTINGS command requests the respective iLO global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

GET_GLOBAL_SETTINGS Parameters

None

GET_GLOBAL_SETTINGS Runtime Errors

None

GET_GLOBAL_SETTINGS Return Messages

A possible GET_GLOBAL_SETTINGS return message is:

```
<GET_GLOBAL_SETTINGS>
   <SESSION_TIMEOUT="120">
   <ILO_FUNCT_ENABLED VALUE="Y"/>
   <F8_PROMPT_ENABLED="Y"/>
   <F8_LOGIN_REQUIRED="Y"/>
   <REMOTE_CONSOLE_PORT_STATUS VALUE="2"/>
   <REMOTE_CONSOLE_ENCRYPTION VALUE="Y"/>
   <PASSTHROUGH_CONFIG VALUE=”3”/>
   <HTTPS_PORT VALUE="443"/>
   <HTTP_PORT VALUE="80"/>
   <REMOTE_CONSOLE_PORT VALUE="23"/>
   <TERMINAL_SERVICES_PORT VALUE="3389"/>
   <VIRTUAL_MEDIA_PORT VALUE="17988"/>
   <MIN_PASSWORD VALUE="8"/>
   <REMOTE_KEYBOARD_MODEL VALUE="US"/>
   <SSH_PORT value="22"/>
   <SSH_STATUS value="YES"/>
   <SERIAL_CLI_STATUS value="3"/>
   <SERIAL_CLI_SPEED value="1"/>
</GET_GLOBAL_SETTINGS>
```

This reply differs from RILOE II.

MOD_GLOBAL_SETTINGS

MOD_GLOBAL_SETTINGS is used to modify global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_GLOBAL_SETTINGS>
      <SESSION_TIMEOUT value="60"/>
      <ILO_FUNCT_ENABLED value="Yes"/>
      <F8_PROMPT_ENABLED value="Yes"/>
      <F8_LOGIN_REQUIRED="Y"/>
      <REMOTE_CONSOLE_PORT_STATUS value="2"/>
      <REMOTE_CONSOLE_ENCRYPTION value="Y"/>
      <PASSTHROUGH_CONFIG value=”3”/>
      <HTTPS_PORT value="443"/>
      <HTTP_PORT value="80"/>
      <REMOTE_CONSOLE_PORT value="23"/>
      <TERMINAL_SERVICES_PORT VALUE="3389"/>
      <VIRTUAL_MEDIA_PORT value="17988"/>
      <MIN_PASSWORD VALUE="8"/>
      <REMOTE_KEYBOARD_MODEL VALUE="US"/>
      <VIRTUAL_MEDIA_PORT value="55"/>
      <SSH_PORT value="22"/>
      <SSH_STATUS value="YES"/>
      <SERIAL_CLI_STATUS value="3"/>
      <SERIAL_CLI_SPEED value="1"/>
   </MOD_GLOBAL_SETTINGS>
   </RIB_INFO>
   </LOGIN>
```

MOD_GLOBAL_SETTINGS Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

SESSION_TIMEOUT determines the maximum session timeout value in minutes. The accepted values are 15, 30, 60 and 120.

ILO_FUNCT_ENABLED determines if the Lights-Out functionality is enabled or disabled for iLO. The possible values are "Yes" or "No." It is case insensitive.

F8_PROMPT_ENABLED determines if the F8 prompt for ROM-based configuration is displayed during POST. The possible values are "Yes" or "No."

F8_LOGIN_REQUIRED determines if login credentials are required to access the RBSU for iLO. The possible values are "Yes" or "No."

REMOTE_CONSOLE_PORT_STATUS determines the behavior of remote console service. The possible values are:

- **0**—No change
- **1**—Disabled (The remote console port is disabled. This will prevent remote console and telnet sessions from being utilized.)
- **2**—Automatic (This is the default setting. The remote console port will remain closed unless a remote console session is started.)
- **3**—Enabled (The remote console port is always enabled. This will allow remote console and telnet sessions to be utilized)

REMOTE_CONSOLE_ENCRYPTION determines if remote console data encryption is enabled or disabled. The possible values are "Yes" and "No."

PASSTHROUGH_CONFIG determines the behavior of a Microsoft® Terminal Services client. The possible values are:

- **0**—No change
- **1**—Disabled (The Terminal Services feature is disabled.)
- **2**—Automatic (The Terminal Services client will be launched when remote console is started.)
- **3**—Enabled (This is the default setting. The terminal services feature is enabled but will not automatically be launched when remote console is started.)

HTTPS_PORT specifies the HTTPS (SSL) port number.

HTTP_PORT specifies the HTTP port number.

REMOTE_CONSOLE_PORT specifies the port used for remote console.

TERMINAL_SERVICES_PORT specifies the port used for terminal services.

VIRTUAL_MEDIA_PORT specifies the port used for virtual media.

NOTE: If port changes are detected, the iLO management processor will be rebooted to apply the changes after the script has completed successfully.

MIN_PASSWORD command specifies how many characters are required in all user passwords. The value can be from zero to 39 characters.

REMOTE_KEYBOARD_MODEL determines the remote keyboard language translation used during remote console operation. The possible values are:

US	Belgian	British
Danish	Finnish	French
French Canadian	German	Italian
Japanese	Latin American	Portuguese
Spanish	Swedish	Swiss French
Swiss German		

SSH_PORT specifies the port used for SSH connection on iLO. The processor must be reset if this value is changed.

SSH_STATUS determines if SSH is enabled. The valid value are Yes or No, which enables or disables SSH functionality.

SERIAL_CLI_STATUS specifies the status of the CLI. The possible values are:

- **0**—No change
- **1**—Disabled
- **2**—Enabled (no authentication required)
- **3**—Enabled (authentication required)

SERIAL_CLI_SPEED specifies the CLI port speed. The possible values are :

- **0**—No change
- **1**—9,600 bps
- **2**—19,200 bps

- **3**—38,400 bps
- **4**—57,600 bps
- **5**—115,200 bps

MOD_GLOBAL_SETTINGS Runtime Errors

The possible MOD_GLOBAL_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.
- Unrecognized keyboard model.

GET_SNMP_IM_SETTINGS

The GET_SNMP_IM_SETTINGS command requests the respective iLO SNMP IM settings. For this command to parse correctly, the GET_SNMP_IM_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

GET_SNMP_IM_SETTINGS Parameters

None

GET_SNMP_IM_SETTINGS Runtime Errors

None

GET_SNMP_IM_SETTINGS Return Messages

A possible GET_SNMP_IM_SETTINGS return message is:

```
<GET_SNMP_IM_SETTINGS>
   <SNMP_ADDRESS_1 VALUE=“192.168.125.121”/>
   <SNMP_ADDRESS_2 VALUE=“192.168.125.122”/>
   <SNMP_ADDRESS_3 VALUE=“192.168.125.123”/>
   <OS_TRAPS VALUE=“Yes”/>
   <RIB_TRAPS VALUE=“No”/>
   <SNMP_PASSTHROUGH_STATUS VALUE=“No”/>
   <WEB_AGENT_IP_ADDRESS VALUE=“192.168.125.120”/>
   <CIM_SECURITY_MASK VALUE=“3”/>
</GET_SNMP_IM_SETTINGS>
```

MOD_SNMP_IM_SETTINGS

MOD_SNMP_IM_SETTINGS is used to modify SNMP and Insight Manager settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION=“2.0”>
   <LOGIN USER_LOGIN=“adminname” PASSWORD=“password”>
   <RIB_INFO MODE=“write”>
   <MOD_SNMP_IM_SETTINGS>
      <WEB_AGENT_IP_ADDRESS value=“192.168.125.120”/>
      <SNMP_ADDRESS_1 value=“192.168.125.121”/>
      <SNMP_ADDRESS_2 value=“192.168.125.122”/>
      <SNMP_ADDRESS_3 value=“192.168.125.123”/>
      <OS_TRAPS value=“Yes”/>
      <RIB_TRAPS value=“No”/>
      <SNMP_PASSTHROUGH_STATUS value=“No”/>
      <CIM_SECURITY_MASK value=“3”/>
   </MOD_SNMP_IM_SETTINGS>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

MOD_SNMP_IM_SETTINGS Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

WEB_AGENT_IP_ADDRESS is the address for the Web-enabled agents. The value for this element has a maximum length of 50 characters. It can be any valid IP address. If an empty string is entered, the current value is deleted.

SNMP_ADDRESS_1, SNMP_ADDRESS_2, and SNMP_ADDRESS_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address and has a maximum value of 50 characters.

OS_TRAPS determines if the user should receive SNMP traps that are generated by the operating system. The possible values are "Yes" and "No." By default, the value is set to "No."

RIB_TRAPS determines if the user should receive SNMP traps that are generated by the RIB. The possible values are "Yes" and "No." By default, the value is set to "No."

SNMP_PASSTHROUGH_STATUS determines if iLO can receive/ send SNMP request from/ to the host OS. By default, the value is set to "Yes."

CIM_SECURITY_MASK accepts an integer between 0 and 4. The possible values are:

- **0**—No change
- **1**—None (No data is returned.)
- **2**—Low (Name and status data are returned. Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.)
- **3**—Medium (iLO and server associations are present but the summary page contains less detail than at high security.)
- **4**—High (Associations are present and all data is present on the summary page.)

Each value indicates the level of data returned over the HTTP port.

MOD_SNMP_IM_SETTINGS Runtime Errors

The possible MOD_SNMP_IM_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

CLEAR_EVENTLOG

The CLEAR_EVENTLOG command clears the iLO Event Log. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <CLEAR_EVENTLOG/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

CLEAR_EVENTLOG Parameters

None

CLEAR_EVENTLOG Runtime Errors

The possible CLEAR_EVENTLOG error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

UPDATE_RIB_FIRMWARE

The UPDATE_RIB_FIRMWARE command copies a specified file to iLO, starts the upgrade process and reboots the board after the image has been successfully flashed. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\ILO140.BIN"/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

UPDATE_RIB_FIRMWARE Parameters

IMAGE_LOCATION takes the full path file name of the firmware upgrade file.

UPDATE_RIB_FIRMWARE Runtime Errors

The possible UPDATE_RIB_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.
- IMAGE_LOCATION must not be blank.

- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_FW_VERSION

The GET_FW_VERSION command requests the respective iLO firmware information. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="read">
   <GET_FW_VERSION/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

GET_FW_VERSION Parameters

None

GET_FW_VERSION Runtime Errors

None

GET_FW_VERSION Return Messages

The following information is returned within the response:

```
<GET_FW_VERSION
   FIRMWARE_VERSION = <firmware version>
   FIRMWARE_DATE = <firmware date>
   MANAGEMENT_PROCESSOR = <management processor type>
/>
```

HOTKEY_CONFIG

The HOTKEY_CONFIG command configures the remote console hot key settings in iLO. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Uppercase letters are not supported, and they will be converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. Specifying a blank string removes the current value.

Refer to the "Supported Hot Keys" section for a complete list of supported hotkeys.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <HOTKEY_CONFIG>
      <CTRL_T value="CTRL,ALT,ESC"/>
      <CTRL_U value="L_SHIFT,F10,F12"/>
      <CTRL_V value=""/>
      <CTRL_Y value=""/>
      <CTRL_X value=""/>
      <CTRL_Y value=""/>
   </HOTKEY_CONFIG>
   </RIB_INFO>
   </LOGIN>
```

</RIBCL>

HOTKEY_CONFIG Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

CTRL_T specifies settings for the CTRL_T hot key. The settings must be separated by commas. For example, CTRL_T="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_U specifies settings for the CTRL_U hot key. The settings must be separated by commas. For example, CTRL_U="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_V specifies settings for the CTRL_V hot key. The settings must be separated by commas. For example, CTRL_V="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_W specifies settings for the CTRL_W hot key. The settings must be separated by commas. For example, CTRL_W="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_X specifies settings for the CTRL_X hot key. The settings must be separated by commas. For example, CTRL_X="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_Y specifies settings for the CTRL_Y hot key. The settings must be separated by commas. For example, CTRL_Y="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

HOTKEY_CONFIG Runtime Errors

The possible HOTKEY_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

LICENSE

The LICENSE command activates or deactivates the iLO's advanced features. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

On a ProLiant BL Class server, there is no need for a licensing key. Advanced features are automatically activated.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <LICENSE>
      <ACTIVATE KEY="1111122222333334444455555"/>
   </LICENSE>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

LICENSE Parameters

ACTIVATE followed by a valid KEY value signals the activation of the iLO advanced pack licensing.

KEY specifies the license key value. The key should be entered as one continuous string. Commas, periods, or other characters should not separate the key value. The key will only accept 25 characters; other characters entered to separate key values will be interpreted as a part of the key and result in the wrong key being entered.

DEACTIVATE signals the deactivation of the iLO advanced pack licensing.

LICENSE Runtime Errors

The possible LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

DIR_INFO

The DIR_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local directory information database into memory and prepares to edit it. Only commands that are DIR_INFO type commands are valid inside the DIR_INFO command block. The DIR_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:

```
<DIR_INFO MODE="read">
   ……… DIR_INFO commands ……
</DIR_INFO>
```

DIR_INFO Parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of directory information. Read mode prevents modification of directory information.

DIR_INFO Runtime Errors

None

GET_DIR_CONFIG

The GET_DIR_CONFIG command requests the respective iLO directory settings. For this command to parse correctly, the GET_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
```

```
      <LOGIN USER_LOGIN="adminname" PASSWORD="password">
      <DIR_INFO MODE="read">
      <GET_DIR_CONFIG/>
      </DIR_INFO>
      </LOGIN>
   </RIBCL>
```

GET_DIR_CONFIG Parameters

None

GET_DIR_CONFIG Runtime Errors

None

GET_DIR_CONFIG Return Messages

A possible GET_DIR_CONFIG return message is:

```
<GET_DIR_CONFIG>
   <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
   <DIR_LOCAL_USER_ACCT VALUE="Y"/>
   <DIR_SERVER_ADDRESS VALUE="server1.hprib.labs"/>
   <DIR_SERVER_PORT VALUE="636"/>
   <DIR_OBJECT_DN VALUE="CN=SERVER1_RIB, OU=RIB,
   DC=HPRIB, DC=LABS"/>
   <DIR_USER_CONTEXT1 VALUE="CN=Users0, DC=HPRIB0,
   DC=LABS"/>
   <DIR_USER_CONTEXT2 VALUE="CN=Users1, DC=HPRIB1,
   DC=LABS"/>
   <DIR_USER_CONTEXT3 VALUE=""/>
</GET_DIR_CONFOG>>
```

MOD_DIR_CONFIG

MOD_DIR_CONFIG command is used modify the directory settings on iLO. For this command to parse correctly, the MOD_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <DIR_INFO MODE="write">
   <MOD_DIR_CONFIG>
      <DIR_AUTHENTICATION_ENABLED value="Yes"/>
      <DIR_LOCAL_USER_ACCT value="Yes"/>
      <DIR_SERVER_ADDRESS value="16.141.100.44"/>
      <DIR_SERVER_PORT value="636"/>
      <DIR_OBJECT_DN value="CN=server1_rib, OU=RIB,
      DC=HPRIB, DC=LABS"/>
      <DIR_OBJECT_PASSWORD value="password"/>
      <DIR_USER_CONTEXT_1 value="CN=Users, DC=HPRIB,
      DC=LABS"/>
   </MOD_DIR_CONFIG>
   </DIR_INFO>
   </LOGIN>
</RIBCL>
```

MOD_DIR_CONFIG Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DIR_AUTHENTICATION_ENABLED enables or disables directory authentication. The possible values are "Yes" and "No."

DIR_LOCAL_USER_ACCT enables or disables local user accounts. The possible values are "Yes" and "No."

DIR_SERVER_ADDRESS specifies the location of the directory server. The directory server location is specified as an IP address or DNS name.

DIR_SERVER_PORT specifies the port number used to connect to the directory server. This value is obtained from the directory administrator. The secure LDAP port is 636, but the directory server can be configured for a different port number.

DIR_OBJECT_DN specifies the unique name of iLO in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

DIR_OBJECT_PASSWORD specifies the password associated with the iLO object in the directory server. Passwords are limited to 39 characters.

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2, and DIR_USER_CONTEXT_3 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user could not be located using the first path, then the parameters specified in the second and third paths are used. The values for these parameters are obtained from the directory administrator. Directory User Contexts are limited to 128 characters each.

MOD_DIR_CONFIG Runtime Errors

The possible MOD_DIR_CONFIG error messages include:

- Directory information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

RACK_INFO

The RACK_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the rack infrastructure database into memory and prepares to edit it. Only commands that are RACK_INFO type commands are valid inside the RACK_INFO command block. The RACK_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

This command block is only valid on ProLiant BL Class servers.

Example:

```
<RACK_INFO MODE=”read”>
……… RACK_INFO commands ………
</RACK_INFO>
```

RACK_INFO Parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of rack infrastructure information. Read mode prevents modification of rack infrastructure information.

RACK_INFO Runtime Errors

The possible RACK_INFO error messages include:

- Invalid Mode.
- Server is not a rack server; rack commands do not apply.

MOD_BLADE_RACK

MOD_BLADE_RACK command is used to modify the rack infrastructure settings. For this command to parse properly, the MOD_BLADE_RACK command must appear within a RACK_INFO command block, and RACK_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="write">
   <MOD_BLADE_RACK>
      <RACK_NAME value="CPQ_Rack_1"/>
      <ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
```

```
            <BAY_NAME value="CPQ_Bay_5"/>
            <FACILITY_PWR_SOURCE value="Yes"/>
            <RACK_AUTO_PWR value="Yes"/>
            <LOG_RACK_ALERTS value="Yes"/>
         </MOD_BLADE_RACK>
         </RACK_INFO>
         </LOGIN>
      </RIBCL>
```

MOD_BLADE_RACK Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

RACK_NAME is the name used to logically group together enclosures in a single rack infrastructure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

ENCLOSURE_NAME is the name used to logically group together the ProLiant BL Class servers that compose a single enclosure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

BAY_NAME is the name used to identifying a particular ProLiant BL class server. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

FACILITY_PWR_SOURCE determines the source of power for the blade servers. A value of "Yes" directs the server to use facility power and a value of "No" directs the server to use the server blade power supplies.

RACK_AUTO_PWR determines if the blade server should automatically power when inserted into the enclosure. A value of "Yes" causes the blade server to automatically power up and begin normal booting process if power is available. A value of "No" requires the blade server to be manually powered on.

LOG_RACK_ALERTS determines if alerts from the rack infrastructure should be logged. A value of "Yes" enables rack alerts to be logged in the IML log. A value of "No" disables the logging of rack alerts in the IML log.

MOD_BLADE_RACK Runtime Errors

The possible MOD_BLADE_RACK error messages include:

- Rack information is open for read-only access. Write access is required for this operation.
- Rack Name too long.
- Enclosure Name too long.
- Bay Name too long.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_DIAGPORT_SETTINGS

The GET_DIAGPORT_SETTINGS command requests the respective iLO diagnostic port settings. For this command to parse correctly, the GET_DIAGPORT_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="read">
   <GET_DIAGPORT_SETTINGS/>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

GET_DIAGPORT_SETTINGS Parameters

None

GET_DIAGPORT_SETTINGS Runtime Errors

None

GET_DIAGPORT_SETTINGS Return Messages

A possible GET_DIAGPORT_SETTINGS return message is:

```
<GET_DIAGPORT_SETTINGS>
   <DP_SPEED_AUTOSELECT value="No"/>
   <DP_NIC_SPEED value="100"/>
   <DP_FULL_DUPLEX value="Yes"/>
   <DP_IP_ADDRESS value="192.168.142.56"/>
   <DP_SUBNET_MASK value="255.255.0.0"/>
</GET_DIAGPORT_SETTINGS >
```

MOD_DIAGPORT_SETTINGS

The MOD_DIAGPORT_SETTINGS command is used modify the diagnostic port network settings on iLO. For this command to parse correctly, the MOD_DIAGPORT_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="username" PASSWORD="password">
   <RACK_INFO MODE="write">
   <MOD_DIAGPORT_SETTINGS>
      <DP_SPEED_AUTOSELECT value="No"/>
      <DP_NIC_SPEED value="100"/>
      <DP_FULL_DUPLEX value="Yes"/>
      <DP_IP_ADDRESS value="192.168.142.56"/>
      <DP_SUBNET_MASK value="255.255.0.0"/>
   </MOD_DIAGPORT_SETTINGS>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

MOD_DIAGPORT_SETTINGS Parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DP_SPEED_AUTOSELECT is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

DP_NIC_SPEED is used to set the transceiver speed if DP_SPEED_AUTOSELECT was set to "No." The possible values are 10 or 100. Any other value results in a syntax error.

DP_FULL_DUPLEX is used to decide if the iLO diagnostic port is to support full-duplex or half-duplex mode. It is only applicable if DP_SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

DP_IP_ADDRESS is used to select the IP address for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is *XXX.XXX.XXX.XXX*.

DP_SUBNET_MASK is used to select the subnet mask for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is *XXX.XXX.XXX.XXX*.

The iLO management processor will be rebooted to apply the changes after the script has completed successfully.

MOD_DIAGPORT_SETTINGS Runtime Errors

Possible MOD_DIAGPORT_SETTINGS error messages include:

- iLO information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_TOPOLOGY

The GET_TOPOLOGY command requests the respective iLO to return the current topology of the rack infrastructure. For this command to parse correctly, the GET_TOPOLOGY command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="read">
      <GET_TOPOLOGY/>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

GET_TOPOLOGY Parameters

None

GET_TOPOLOGY Return Message

An example of a successful request follows:

```
<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123"
NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456"
NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789"
NAME="Power_2">
<RIGHT/>
</ICMB>
</RK_TPLGY>
```

SERVER_INFO

The SERVER_INFO command can only appear within a LOGIN command block. Only commands that are SERVER_INFO type commands are valid inside the SERVER_INFO command block.

Example:

```
<SERVER_INFO MODE="read">
……… SERVER_INFO commands ………
</SERVER_INFO>
```

SERVER_INFO Parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and modifying of server functionality. Read mode prevents modification of server functionality.

SERVER_INFO Runtime Errors

None

GET_HOST_POWER_STATUS

The GET_HOST_POWER_STATUS command requests the power state of the server. For this command to parse correctly, the GET_HOST_POWER_STATUS command must appear within a SERVER_INFO command block, and SEVER_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <GET_HOST_POWER_STATUS/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

GET_HOST_POWER_STATUS Parameters

None

GET_HOST_POWER_STATUS Runtime Errors

The possible GET_HOST_POWER_STATUS error messages include:

- Host power is OFF.
- Host power is ON.

GET_HOST_POWER_STATUS Return Messages

The following information is returned within the response:

```
<GET_HOST_POWER
   HOST POWER="OFF"
/>
```

SET_HOST_POWER

The SET_HOST_POWER command is used to toggle the power button of server. For this command to parse correctly, the SET_HOST_POWER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <SET_HOST_POWER HOST_POWER="Yes"/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

SET_HOST_POWER Parameters

HOST_POWER enables or disables the Virtual Power Button. The possible values are "Yes" or "No."

SET_HOST_POWER Runtime Errors

The possible SET_HOST_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Virtual Power Button feature is not supported on this server.
- Host power is already ON.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

RESET_SERVER

The RESET_SERVER command resets the server if the server is turned on. For this command to parse correctly, the SET_HOST_POWER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write.The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <RESET_SERVER/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

RESET_SERVER Parameters

None

RESET_SERVER Errors

The possible RESET_SERVER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Server is currently powered off.
- User does NOT have correct privilege for action. RESET_SERVER_PRIV required.

PRESS_PWR_BTN

This PRESS_PWR_BTN command is used to toggle server power. For this command to parse correctly, the PRESS_PWR_BTN command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <PRESS_PWR_BTN/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

PRESS_PWR_BTN Parameters

There are no parameters for this command.

PRESS_PWR_BTN Runtime Errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

HOLD_PWR_BTN

This HOLD_PWR_BTN command is used to hold the server power button. For this command to parse correctly, the HOLD_PWR_BTN command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <HOLD_PWR_BTN/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

HOLD_PWR_BTN Parameters

There are no parameters for this command.

HOLD_PWR_BTN Runtime Errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.

- User does not have correct privilege for action. RESET_SERVER_PRIV required.

COLD_BOOT_SERVER

This COLD_BOOT_SERVER command is used to cold boot a server. For this command to parse correctly, the COLD_BOOT_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <COLD_BOOT_SERVER/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

COLD_BOOT_SERVER Parameters

There are no parameters for this command.

COLD_BOOT_SERVER Runtime Errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

WARM_BOOT_SERVER

This WARM_BOOT_SERVER command is used to warm boot a server. For this command to parse correctly, the WARM_BOOT_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <WARM_BOOT_SERVER/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

WARM_BOOT_SERVER Parameters

There are no parameters for this command.

WARM_BOOT_SERVER Runtime Errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

GET_UID_STATUS

The UID_STATUS command requests the state of the server UID. For this command to parse correctly, the UID_STATUS command must appear within a SERVER_INFO command block, and SEVER_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <GET UID_STATUS />
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

GET_UID_STATUS Parameters

None

GET_UID_STATUS Response

The following information is returned within the response:

```
<GET_UID_STATUS
   UID="OFF"
/>
```

UID_CONTROL

The UID_CONTROL command toggles the server UID. For this command to parse correctly, the UID_CONTROL command must appear within a SERVER_INFO command block, and SEVER_INFO MODE must be set to write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <UID_CONTROL UID="Yes"/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

UID_CONTROL Parameters

UID determines the state of the UID. A value of "Yes" turns the UID light on, and a value of "No" turns the UID light off.

UID_CONTROL Errors

The possible UID_CONTROL error messages include:

- UID is already ON.
- UID is already OFF.

INSERT_VIRTUAL_MEDIA

This command notifies iLO of the location of a diskette image. The INSERT_VIRTUAL_MEDIA command must display within a RIB_INFO element, and RIB_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN = "adminname" PASSWORD =
   "password">
   <RIB_INFO MODE = "write">
      <INSERT_VIRTUAL_MEDIA "FLOPPY" IMAGE_URL =
      "http://servername/path/to/file"/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

INSERT_VIRTUAL_MEDIA Parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

IMAGE_URL specifies the URL to the diskette image. The URL format is as follows:

```
protocol://username:password@hostname:port/filename,cgi-
helper
```

- The protocol field is mandatory and must be either http or https.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional
- The filename field is mandatory.
- The cgi-helper field is optional.

In addition, the filename field may contain tokens that expand to host specific strings:

- %m expands to the iLO MAC address.
- %i expands to the iLO IP address in dotted-quad form.
- %h expands to the iLO hostname.

Examples:

```
http://john:abc123@imgserver.company.com/disk/win98dos.b
in,/cgi-bin/hpvfhelp.pl
http://imgserver.company.com/disk/boot%m.bin
```

This command only specifies the location of the image to be used. For the image to be connected to the server, the appropriate BOOT_OPTION must be specified using the SET_VM_STATUS command.

If BOOT_OPTION is set to BOOT_ONCE and the server is rebooted, any subsequent server reboots eject the image.

After an image is inserted using this command, the Virtual Media applet cannot connect its Virtual Media devices and subsequent scripts cannot use the INSERT_VIRTUAL_FLOPPY command until the image is ejected.

INSERT_VIRTUAL_FLOPPY Runtime Errors

The possible INSERT_VIRTUAL_FLOPPY error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- IMAGE_URL must not be blank.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- Unable to parse Virtual Media URL
- An invalid Virtual Media option has been given.
- Virtual Media already connected through a script. You must eject or disconnect before inserting new media.

EJECT_VIRTUAL_MEDIA

EJECT_VIRTUAL_MEDIA ejects the Virtual Media image if one is inserted. The EJECT_VIRTUAL_MEDIA command must display within a RIB_INFO element and RIB_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="Password">
   <RIB_INFO MODE="write">
      <EJECT_VIRTUAL_FLOPPY />
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

EJECT_VIRTUAL_MEDIA Parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

EJECT_VIRTUAL_MEDIA Runtime Errors

The possible EJECT_VIRTUAL_MEDIA errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- No image present in the Virtual Media drive.
- An invalid Virtual Media option has been given.

GET_VM_STATUS

GET_VM_STATUS returns the Virtual Media drive status. This command must display within a RIB_INFO element.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
   <RIB_INFO MODE = "read">
      <GET_VM_STATUS DEVICE = "CDROM"/>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_VM_STATUS Parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

GET_VM_STATUS Runtime Errors

The possible GET_VM_STATUS error is:

An invalid Virtual Media option has been given.

GET_VM_STATUS Return Messages

A possible GET_VM_STATUS return message is:

```
VM_APPLET = CONNECTED | DISCONNECTED
DEVICE = FLOPPY | CDROM
BOOT_OPTION = BOOT_ALWAYS | BOOT_ONCE | NO_BOOT
WRITE_PROTECT_FLAG = YES | NO
IMAGE_INSERTED = YES | NO
```

SET_VM_STATUS

SET_VM_STATUS sets the Virtual Media drive status. This command must display within a RIB_INFO element, and RIB_INFO must be in write mode. All the parameters in the command are optional.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
   <RIB_INFO MODE = "write">
   <SET_VM_STATUS DEVICE = "CDROM">
      <VM_BOOT_OPTION value = "BOOT_ONCE"/>
      <VM_WRITE_PROTECT value = "Y"/>
   </ SET_VF_STATUS>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

SET_VM_STATUS Parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

VM_BOOT_OPTION specifies the boot option parameter for the Virtual Media. For the device to act like the RIBLO Virtual Floppy functionality, the possible values are BOOT_ALWAYS, BOOT_ONCE or NO_BOOT. These values control how the Virtual Media device behaves after the server is rebooted. To control the Virtual Media devices in the same way that they are controlled in the Virtual Media applet, the values this parameter are CONNECT or DISCONNECT. This value is case-sensitive.

VM_WRITE_PROTECT sets the write protect flag value for the Virtual Floppy. This value is not significant for the Virtual Media CD-ROM. The possible values are Y or N.

SET_VM_STATUS Runtime Errors

The possible runtime errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- An invalid Virtual Media option has been given.

iLO Parameters

In This Section

iLO Parameters Table

You can record your settings in the Your Value column of the table.

Parameters	Default Value or Setting	Your Value
iLO Status		
Current User		
Terminal Services	Disabled	
iLO Time		
iLO Date		
iLO Firmware Version	*XX.XX*	
iLO Serial Number	iLO*XXXXXXXXXXXX*	
Product Version		
Server Status		
Server Name		
Server ID		
Server Power Status		
Server Video Mode		
Server Keyboard		
Server Mouse		

Parameters	Default Value or Setting	Your Value
User Administration		
User Name	Administrator	
Login Name	Administrator	
Password	A random, eight-character alphanumeric string that is factory assigned	
Administer User Accounts	Yes	
Remote Console Access	Yes	
Virtual Power and Reset	Yes	
Virtual Media	Yes	
Configure iLO Settings	Yes	
Global Settings		
Idle Connection Timeout (minutes)	30 minutes	
Enable Lights-Out Functionality	Yes	
Pass-Through Configuration	Disabled	
Enable iLO ROM-Based Setup Utility	Yes	
Require Login for iLO RBSU	No	
Show iLO during POST	No	
Remote Console Port Configuration	Automatic	
Remote Console Data Encryption	Yes	
SSL Encryption Strength	128-bit	
Current Cipher	Negotiated by the iLO and the browser	
Web Server Non-SSL Port	80	
Web Server SSL Port	443	
Virtual Media Port	17988	

Parameters	Default Value or Setting	Your Value
Remote Console Port	23	
Terminal Services Port	3389	
Secure Shell(SSH) Port	22	
Secure Shell(SSH) Access	Enabled	
Serial Command Line Interface Status	Enabled (authentication required)	
Serial Command Line Interface Speed (bits/second)	9600	
Minimum Password Length	8	
Remote Keyboard Model	US	
Network Settings		
Enable NIC	Yes	
Shared Network Port	No	
Transceiver Speed Autoselect	Yes	
Speed	N/A (autoselect)	
Duplex	N/A (autoselect)	
Enable DHCP	Yes	
Use DHCP Supplied Gateway	Yes	
Use DHCP Supplied DNS Servers	Yes	
Use DHCP Supplied WINS Servers	Yes	
Use DHCP Supplied Static Routes	Yes	
Use DHCP Supplied Domain Name	Yes	
Register With WINS Server	N/A (DHCP)	
Register With DNS Server	N/A (DHCP)	

Parameters	**Default Value or Setting**	**Your Value**
Ping Gateway on Startup	No	
iLO IP Address	N/A (DHCP)	
iLO Subnet Mask	N/A (DHCP)	
iLO Gateway IP Address	N/A (DHCP)	
iLO Subsystem Name	iLO*XXXXXXXXXXXX*, where the 12 *X*s are the server serial number (assigned at the factory)	
Domain Name	N/A (DHCP)	
DHCP Server	N/A (DHCP)	
Primary, Secondary, and Tertiary DNS Server	N/A (DHCP)	
Primary and Secondary WINS Server	N/A (DHCP)	
Static Routes #1, #2, #3	N/A for both the destination and gateway address (DHCP)	
Blade server parameters		
iLO Diagnostic Port Configuration Parameters		
Transceiver Speed Autoselect	Yes	
Speed	N/A (autoselect)	
Duplex	N/A (autoselect)	
IP Address	192.168.1.1	
Subnet Mask	255.255.255.0	
SNMP/Insight Manager Settings		
SNMP Alert Destination(s)	No	
Enable iLO SNMP Alerts	No	
Forward Insight Manager Agent SNMP Alerts	No	

Parameters	**Default Value or Setting**	**Your Value**
Enable SNMP Pass-thru	yes	
Insight Manager Web Agent URL		
Level of Data Returned	Medium	
BL p-Class		
Rack Name	Provided by rack	
Enclosure Name	Provided by rack	
Bay Name	Bay *X* (where *X* is the bay number in which the blade server is located)	
Bay	Provided by rack	
Rack Serial Number	Provided by rack	
Enclosure Serial Number	Provided by rack	
Blade Serial Number	Provided by blade server	
Power Source	Rack Provides Power	
Enable Automatic Power On	On	
Enable Rack Alert Logging (IML)	On	
Directory Settings		
Enable Directory Authentication	No	
Enable Local User Accounts	Yes	
Directory Server Address	0.0.0.0	
Directory Server LDAP Port	636	
LOM Object Distinguished Name		
LOM Object Password		
LOM Object Password Confirm		
Directory User Context 1		

Parameters	Default Value or Setting	Your Value
Directory User Context 2		
Directory User Context 3		

iLO Status

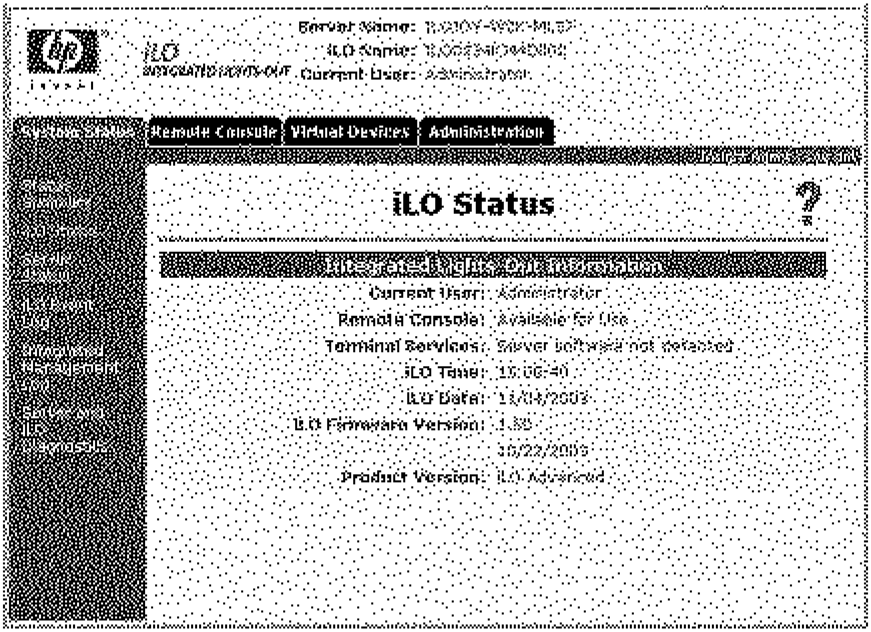
The iLO Status option provides comprehensive iLO status information, including:

- Current user
- Status and availability of the Remote Console
- Status and availability of Terminal Services pass-through
- Date and time currently in use by iLO

  NOTE: Date and time are set during POST and maintained by the MP Management Agents.

- Revision information of the iLO firmware

- Product version (iLO Standard or iLO Advanced) of iLO



Server Name: [illegible]
iLO Name: [illegible]
Current User: Administrator

iLO Status

Integrated Lights-Out Information

Current User: Administrator
Remote Console: Available for Use
Terminal Services: Server software not detected
iLO Time: 15:06:40
iLO Date: 11/04/2003
iLO Firmware Version: 1.50
10/22/2003
Product Version: iLO Advanced

Server Status Parameters

The following parameters provide information about the host server.

Server Name

If the Insight Management agents are being used with the host server operating system, they will provide iLO with the server name.

Server ID

Displays the serial number of the server.

Server Power Status

Displays whether the host is powered ON, or in STANDBY (OFF) mode.

Server Video Mode

Displays the state of the host server video controller as interpreted by Remote Console.

Server Keyboard

Displays the keyboard type as emulated by Remote Console.

Server Mouse

Displays the mouse type as emulated by Remote Console.

User Administration Parameters

The User Administration section enables you to define the users currently configured for access to iLO. Up to 12 users can be specified. User configurations can be added, deleted, or modified by using the Web interface.

User Name

This parameter is the user's real name as it is displayed in the user list and event log. It is not the name used to log in. The maximum length of the user name is 39 characters.

Login Name

This is a case-sensitive name that the user must provide to log in to iLO.

Password

This is a case-sensitive password that the user must provide to log in to iLO. In Security Options, the minimum password length can be assigned. The minimum password can be from 0 to 39 characters. The default minimum password length is eight characters. You must enter the password twice for verification.

Administer User Accounts

This privilege allows a user to add, modify, and delete user accounts. It also allows the user to alter privileges for all users, including granting all permissions to a user.

Remote Console Access

This privilege allows a user to remotely manage the Remote Console of a managed system, including video, keyboard, and mouse controls.

Virtual Power and Reset

This privilege allows a user to power-cycle or reset the host platform.

Virtual Media

This privilege allows a user to use virtual media on the host platform.

Configure iLO Settings

This privilege enables a user to configure most iLO settings, including security settings. It does not include user account administration.

After iLO is correctly configured, revoking this privilege from all users prevents reconfiguration. A user with the Administer User Accounts privilege can enable or disable this privilege. iLO can also be reconfigured if iLO RBSU is enabled.

Idle Connection Timeout (Minutes)

This option specifies the interval of user inactivity, in minutes, before the Web server and Remote Console session are automatically terminated.

Enable Lights-Out Functionality

This option enables connection to iLO. If disabled, all connections to iLO are prevented. The default setting is Yes.

- The iLO 10/100 network and communications with operating system drivers will be turned off if Lights-Out functionality is disabled. The iLO Diagnostic Port for a ProLiant BL p-Class server will be disabled as well.
- If iLO functionality, including the iLO Diagnostic Port, is disabled, you must use the Security Override Switch in the server to enable iLO functionality. Follow the server documentation of the server to locate the Security Override Switch and set it to the override position. Power on the server and use the iLO RBSU to set Enable Lights-Out Functionality.

Enable iLO RBSU

This option enables a user with access (physical or virtual) to the host to configure iLO for that system using iLO RBSU. RBSU is invoked when the host system reboots and performs POST. The default setting is Yes. You can restrict RBSU access to authorized users by selecting **Require Login for iLO RBSU.**

NOTE: If the physical security jumper is set, the RBSU prompt displays during reboot.

Pass-Through Configuration

This option controls the ability of iLO to pass-through a connection between a Microsoft® Terminal Services client and Terminal Services server running on the server that has the iLO installed. There are three options:

- **Automatic** means when remote console is started, the Terminal Services client will be launched.
- **Enabled** means the pass-through feature is enabled but will not launch automatically. You must click the Terminal Svcs button in Remote Console to start the client.

- **Disabled** means that the pass-through feature is off.

Require Login for iLO RBSU

This option specifies whether the user is required to provide a login name and password to access iLO RBSU. The default setting is No.

Show iLO During POST

This option specifies if iLO is displayed during POST. The default setting is No.

Remote Console Port Configuration

This option enables or disables configuring of the port address.

- **Enabled** allows Telnet and Remote Console applet access.
- **Automatic** allows Remote Console applet access but not Telnet access.
- **Disabled** turns off both Telnet and Remote Console applet access.

Remote Console Data Encryption must be set to **No** to use Telnet to access the text Remote Console.

Remote Console Data Encryption

This option enables encryption of Remote Console data. If using a standard Telnet client to access iLO, this setting must be set to No. When using the Remote Console applet, all data is encrypted regardless of this setting.

SSL Encryption Strength

This option displays the current cipher strength setting. The most secure is 128-bit (High).

Current Cipher

This option displays the encryption algorithm currently being used to protect data during transmission between the browser and the iLO.

Web Server Non-SSL Port

The embedded Web server in iLO is configured by default to use port 80 for unencrypted communications. This port setting is configurable in the Global Settings option of the Administration tab.

Web Server SSL Port

The embedded Web server in iLO is configured by default to use port 443 for encrypted communications. This port setting is configurable in the Global Settings option of the Administration tab.

Virtual Media Port

The Virtual Media support in iLO uses a configurable port for its communications. This port can be set in the Global Settings option of the Administration tab. The default setting is to use port 17988.

Remote Console Port

The iLO Remote Console is configured by default to use port 23 for Remote Console communications. This port setting is configurable in the Global Settings option of the Administration tab.

Terminal Services Port

The Terminal Services port is the port that iLO uses to communicate with Terminal Services pass-through software on the server. The iLO Terminal Services pass-through is configured by default to use port 3389 for encrypted communications. If the Terminal Services pass-through port is configured to anything other than the default, the port number in Windows® 2000 must be manually changed to match it. This port setting is configurable in the Global Settings option of the Administration tab.

Secure Shell (SSH) Port

The iLO Secure Shell (SSH) Port is configured by default to use port 22 for SSH communications. This port setting is configurable in the Global Settings option of the Administration tab. Valid values are from 1 to 65535.

Secure Shell (SSH) Status

This setting enables you to specify if the SSH feature on iLO is enabled or disabled. The default is enabled.

Serial Command Line Interface Status

This setting allows you to change the status of the CLI feature through the serial port. Valid settings are:

- Enabled (authentication required)
- Enabled (no authentication)
- Disabled

The default setting is Enabled—authentication required.

Serial Command Line Interface Speed (bits/second)

This setting enables you to change the speed of the serial port for the CLI feature through the serial port. Valid speeds are (bits/s) 9,600, 19,200, 38,400, 57,600 and 115,200. The default setting is 9600 bits/s. The serial port configuration must be set to No parity, 8 data bits, and 1 stop bit (N/8/1) for proper operation. The serial port speed set by this parameter must match the speed of the serial port set in the System ROM RBSU setup.

Minimum Password Length

This option specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from zero to 39. The default setting is eight characters.

Remote Keyboard Model

This setting allows you to specify the language model of the keyboard during a Remote Console session. The default setting is US.

Network Settings Parameters

The following parameters provide information about the iLO network settings.

Enable NIC

This parameter enables the NIC to reflect the state of iLO. The default setting for the NIC is Yes, which is enabled. If DHCP is disabled, you must assign a static IP address to iLO. Assign the IP address using the iLO IP Address parameter.

Shared Network Port

This option only displays on servers that support the iLO Shared Network Port. If the option is available, the help content for iLO Shared Network Port is also displayed. The iLO Shared Network Port option is disabled by default. Selecting this option disables the iLO NIC and directs iLO network traffic over the designated host NIC. Refer to your server documentation for additional information.

Transceiver Speed Autoselect

Autoselect detects the interface speed and sets the interface to operate at 10 Mb/s or 100 Mb/s and at half or full duplex. If necessary, this parameter can be set to manual to allow manual adjustment of speed and duplex settings.

Speed

Use this setting to assign 10-Mb/s or 100-Mb/s connect speeds if Transceiver Speed Autoselect is not enabled.

Duplex

Use this setting to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.

DNS/DHCP

iLO comes preset from HP with DNS/DHCP enabled. To disable DHCP, you must use the iLO RBSU.

> **NOTE:** If you disable DHCP, you will have to manually set up the IP address and the subnet mask using the iLO RBSU.

If DHCP is enabled, the following settings are also enabled:

- Use DHCP Supplied Gateway
- Use DHCP Supplied DNS Servers
- Use DHCP Supplied WINS Servers
- Use DHCP Supplied Static Routes
- Use DHCP Supplied DNS Name

If DHCP has been disabled, these settings may have to be assigned.

Registering with WINS Server

iLO automatically registers with a WINS server. The default setting is Yes. By default, WINS server addresses are assigned by DHCP.

Registering with DNS Server

iLO automatically registers with a DNS server. The default setting is Yes. By default, DNS server addresses are assigned by DHCP.

Ping Gateway on Startup

This option causes iLO to send four ICMP echo request packets to the gateway when iLO initializes. This option ensures that the ARP cache entry for iLO is current on the router responsible for routing packets to and from iLO.

iLO IP Address

Use this parameter to assign a static IP address to iLO on your network. By default, the IP address is assigned by DHCP.

iLO Subnet Mask

Use the subnet mask parameter to assign the subnet mask for the default gateway. By default, the subnet mask is assigned by DHCP.

iLO Gateway IP Address

Use the gateway parameter to assign the IP address of the network router that connects the iLO subnet to another subnet where the management console resides. The default gateway is assigned by DHCP.

iLO Subsystem Name

iLO comes preset with a DNS/WINS name. The DNS/WINS name is "iLO" plus the serial number of the server. This name also is displayed on the tag attached to the bracket of iLO. You can change this value.

Domain Name

Enter the name of the domain in which iLO will participate. By default, the domain name is assigned by DHCP.

DHCP Server

This setting is automatically detected if DHCP is set to Yes. You cannot change this setting.

Primary, Secondary, and Tertiary DNS Server

Use this parameter to assign a unique DNS server IP address on the network. By default, the primary, secondary, and tertiary DNS servers are assigned by DHCP.

Primary and Secondary WINS Server

Use this parameter to assign a unique WINS server IP address on the network. By default, the primary and secondary WINS servers are assigned by DHCP.

Static Route #1, #2, #3

Use this parameter to assign a unique static route destination and gateway IP address pair on the network. Up to three static route pairs can be assigned. By default, the static routes are assigned by DHCP.

SNMP/Insight Manager Settings Parameters

iLO supports SNMP settings on a device level. These parameters are not designated on a per-user basis but are specific to iLO.

SNMP Alert Destinations

Enter the IP address of the remote management PC that will receive SNMP trap alerts from iLO. Up to three IP addresses can be designated to receive SNMP alerts.

Enable iLO SNMP Alerts

iLO alert conditions are detected by iLO and are independent of the host server operating system. These alerts can be Insight Manager SNMP traps. These alerts include major events, such as remote server power outages or server resets. They also include iLO events, such as security disabled or failed login attempt. iLO forwards the alerts to an Insight Manager 7 or Systems Insight Manager console using the destinations provided. The default setting is No.

Forward Insight Manager Agent SNMP Alerts

These alerts are generated by the Insight Management agents, which are provided for each supported network operating system. The agents must be installed on the host server to receive these alerts. These alerts are sent to Insight Manager 7 or Systems Insight Manager clients on the network and are forwarded asynchronously by iLO to the IP addresses that have been configured to receive them. The default setting is Yes.

Enable SNMP Pass-Through

The Enable SNMP pass-through option enables the system to pass SNMP packets from the Insight Management Agent. When set to No, all SNMP traffic is stopped and will not pass-through iLO. The default setting is Yes.

Insight Manager Web Agent URL

The Insight Manager Web Agent URL option enables you to enter the IP address or the DNS name of the host server on which the Insight Manager Web Agents are running. Entering this data in the field provided enables iLO to create a link from the iLO Web pages to the pages of the Web Agent.

Level of Data Returned

The Level of Data Returned option regulates how much data is returned to an anonymous request for iLO information from Insight Manager 7 or Systems Insight Manager. All settings, except the None Data Level, provide sufficient data to allow integration with Insight Manager 7. The Medium and High settings enable Insight Manager 7 and Systems Insight Manager to associate the management processor with the host server. The None Data Level prevents iLO from responding to the Insight Manager 7 and Systems Insight Manager requests. The default setting is Medium.

iLO Advanced License Activation Settings

The following parameter provides information about the licensing of the iLO Advanced Features.

iLO Advanced Pack License Key

The iLO Advanced Pack License Key option is used to enable the iLO Advanced Features including Graphical Remote Console, virtual media (floppy and CD-ROM), and directory support . Enter the 25-character key in this field to enable the features.

ProLiant BL p-Class Parameters

The following parameters provide information about the ProLiant BL p-Class settings.

Rack Name

The rack name is used to logically group together the components that compose a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component.

Enclosure Name

The enclosure name is used to logically group together the server blades that compose a single enclosure. When changed, the enclosure name is communicated to all other server blades connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component.

Bay Name

The bay name is used when logging and alerting to assist in identifying a component or its function.

Bay

The ProLiant BL p-Class enclosure can support one to eight server blades. The bays are numbered from left to right starting with 1 and finishing with 8. The bay number is used to assist in physically identifying the faulty server blade or other error conditions. This information is for viewing only.

Rack Serial Number

The rack serial number identifies the components in the rack as a logical grouping. The serial number is determined during power-up of the various components to create a unique rack serial number. Switching components (server blade enclosure or power supplies) alters the rack serial number.

Enclosure Serial Number

The enclosure serial number identifies the particular server blade enclosure in which a server blade resides.

Blade Serial Number

The blade serial number identifies the serial number for the server blade product.

Power Source

The server blade enclosure can be installed in a rack by using one of two configurations:

- The server blade power supplies can be used to convert normal AC facility power to 48 V DC to power the rack. In this configuration, select the power source as **Rack Provides Power.** This setting enables each server blade, enclosure, and power supply to communicate power requirements to ensure proper power consumption without risking power failures.
- If the facility can provide 48 V DC power directly, without the need for the provided power supplies, then select **Facility Provides 48V.** Each server blade will not be required to communicate with the infrastructure for power when powering on or off.

  NOTE: It is essential that proper power sizing requirements be performed to ensure sufficient power for all the server blades and other components of the rack.

Enable Automatic Power On

Each server blade can be configured to automatically power on when inserted into the enclosure. Depending on the Power Source setting, the server blade communicates with the rack to determine if enough power is available to power on. If the power is available, then the server blade automatically powers on and begins the normal server booting process.

Enable Rack Alert Logging (IML)

As the server blade receives alerts, these events can be logged to the IML. You can view these events by using the iLO System Status—IML tab. Additional IML viewing tools are available to allow viewing from the installed operating system on the server blade.

Directory Settings Parameters

The following parameters provide information about the Directory Settings.

Enable Directory Authentication

This parameter enables or disables directory authentication. If directory support is properly configured, this enables user login to iLO using directory credentials.

Enable Local User Accounts

This option enables a user to log in using a local user account instead of a directory account. By default, this setting is Enabled.

Directory Server Address

This parameter specifies the Directory Server DNS name or IP address. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.

Directory Server LDAP Port

This option sets the port number used to connect to the directory server. The SSL-secured LDAP port number is 636.

LOM Object Distinguished Name

This option specifies the unique name for the iLO in the directory. LOM Object Distinguished Names are limited to 256 characters.

LOM Object Password

This parameter specifies the password for the iLO object to access the directory. LOM Object Passwords are limited to 39 characters.

> **NOTE:** At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.

Directory User Context 1, Directory User Context 2, Directory User Context 3

This parameter enables you to specify up to three searchable contexts used to locate the user when the user is trying to authenticate using the directory. Directory User Contexts are limited to 128 characters each. Directory User Contexts enable you to specify directory user containers that are automatically searched when an iLO login is attempted. This eliminates the requirement of entering a fully distinguished user name at the login screen. For example, the search context, "ou=lights out devices,o=corp" would allow the user "cn=manager,ou=lights out devices,o=corp" to login to iLO using just "manager." Active Directory allows an additional search context format, "@hostname" for example, "@directory.corp."

Testing Directory Settings

After updating the directory settings, click **Apply Settings** to store the settings. When the Test Settings button is enabled, you can validate the current directory settings. To test these settings:

1. Be sure the Enable Directory Authentication setting is enabled.
2. Click **Test Settings.**
3. Enter the fully distinguished name and password of the user used to add iLO to the directory server in the Directory Administrator Distinguished Name and Directory Administrator Password fields.
4. Enter the credentials of an expected directory-based iLO User account in the Test User Name and Test User Password fields.
5. Click **Start Test.**

A series of tests will begin, and the page will automatically refresh as the tests progress. View the test status to diagnose the results, and consult the help page for specific test result details. The test results are cleared if any directory settings are changed, if iLO is reset, or if the tests are restarted.

Directory Services Schema

In This Section

HP Management Core LDAP OID Classes and Attributes

Changes made to the schema during the schema setup process include changes to the:

- Core Classes (on page 353)
- Core Attributes (on page 353)

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

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

Attribute Name	Assigned OID
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core Class Definitions

The following defines the HP Management core classes.

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

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

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	This class defines Policy objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	top
Attributes	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1
Remarks	None

Core Attribute Definitions

The following defines the HP Management core class attributes.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	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

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	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

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	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

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	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, then IP restrictions will be satisfied for unexceptional network clients. If this attribute is FALSE, then IP restrictions will be unsatisfied for unexceptional network clients.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	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 which 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

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	A seven 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.

Lights-Out Management Specific LDAP OID Classes and Attributes

The following schema attributes and classes might depend on attributes or classes defined in the HP Management core classes and attributes.

Lights-Out Management Classes

Class Name	**Assigned OID**
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management 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

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

Lights-Out Management Class Definitions

The following defines the Lights-Out Management core class.

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 Lights-Out Management 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

Lights-Out Management Attribute Definitions

The following defines the Lights-Out Management core class attributes.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Login Right for HP Lights-Out Management products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single Valued
Remarks	Meaningful only on ROLE objects, if TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Remote Console Right for Lights-Out Management 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.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Virtual Media Right for HP Lights-Out Management products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Remote Server Reset and Power Button Right for HP Lights-Out Management 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

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Local User Database Administration Right for HP Lights-Out Management 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

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Configure Devices Settings Right for HP Lights-Out Management 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.

Troubleshooting iLO

In This Section

Minimum Requirements

iLO has the following minimum requirements:

- Windows® clients
  - Windows® 2000
  - Microsoft® Internet Explorer 6.0 with 128-bit encryption
  - Java™ 1.3.1 JVM or later
- Linux clients
  - Red Hat 7.3
  - Netscape 7.10 or Mozilla 1.60 with 128-bit encryption
  - Java™ 1.4.2 JVM or later

To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvml).

> **NOTE:** You will be redirected from the main site to the java.sun.com site. HP recommends using the version specified in the Remote Console help pages. You can obtain the specified version for Internet Explorer either from the java.sun site or on the Management CD.

iLO POST LED Indicators

During the initial boot of iLO, the POST LED indicators flash to display the progress through the iLO boot process. After the boot process is complete, the heartbeat (HB) LED flashes every second. LED 7 also flashes intermittently during normal operation.

The LED indicators (1 through 6) light up after the system has booted to indicate a hardware failure. If a hardware failure is detected, reset iLO. For the location of the LED indicators, refer to the server documentation.

A runtime failure of iLO is indicated by HB and LED 7 remaining in either the On of Off state constantly. A runtime failure of iLO can also be indicated by a repeated flashing pattern on all eight LEDs. If a runtime error occurs, reset iLO.

The LED indicators have the following assignments:

HB	7	6	5	4	3	2	1

LED Indicators	POST Code (Activity Completed)	Description	Failure Indicates
None	00	Set up chip selects.	
1 or 2	02—Normal operation	Determine platform.	
2 and 1	03	Set RUNMAP bit.	
3	04	Initialize SDRAM controller.	
3 and 2	06	Activate the I cache.	
3, 2, and 1	07	Initialize (only) the D cache.	

LED Indicators	POST Code (Activity Completed)	Description	Failure Indicates
4	08	Copy secondary loader to RAM.	Could not copy secondary loader.
4 and 1	09	Verify secondary loader.	Did not execute secondary loader.
4 and 2	0a	Begin secondary loader.	SDRAM memory test failed.
4, 2, and 1	0b	Copy ROM to RAM.	Could not copy boot block.
4 and 3	0c	Verify ROM image in RAM.	Boot block failed to execute.
4, 3, and 1	0d	Boot Block Main started.	Boot block could not find a valid image.
None		Start C Run time initialization.	
4, 3, and 2	0e	Main() has received control.	Main self-test failed.
Varies	Varies	Each subsystem may self-test.	
4, 3, 2, and 1	0f	Start ThreadX.	RTOS startup failed.
None	00	Main_init() completed.	Subsystem startup failed.
HB and 7		Flashes as the iLO processor executes firmware code. It does not change the value of the lower six LEDs.	

The iLO microprocessor firmware includes code that makes consistency checks. If any of these checks fail, the microprocessor executes the FEH. The FEH presents information using the iLO POST LED indicators. The FEH codes are distinguished by the alternating flashing pattern of the number 99 plus the remainder of the error code.

FEH Code	Consistency Check	Explanation
9902	TXAPICHK	An RTOS function was called with an inappropriate value, or was called from an inappropriate caller.
9903	TXCONTEXT	The saved context of one or more threads has been corrupted.
9905	TRAP	A stack probe failed, return address is invalid, or illegal trap instruction has been detected.
9966	NMIWR	An unexpected write to low memory has occurred.
99C1	CHKNULL	The reset vector has been modified.

Event Log Entries

Event Log Display	Event Log Explanation
Server power failed	Displays when the server power fails.
Browser login: *IP address*	Displays the IP address for the browser that logged in.
Server power restored	Displays when the server power is restored.
Browser logout: *IP address*	Displays the IP address for the browser that logged out.
Server reset	Displays when the server is reset.
Failed Browser login – IP Address: *IP address*	Displays when a browser login fails.
iLO Self Test Error: *#*	Displays when iLO has failed an internal test. The probable cause is that a critical component has failed. Further use of iLO on this server is not recommended.
iLO reset	Displays when iLO is reset.
On-board clock set; was *#:#:#:#:#:#*	Displays when the onboard clock is set.
Server logged critical error(s)	Displays when the server logs critical errors.
Event log cleared by: *User*	Displays when a user clears the event log.
iLO reset to factory defaults	Displays when iLO is reset to the default settings.
iLO ROM upgrade to *#*	Displays when the ROM has been upgraded.

Event Log Display	Event Log Explanation
iLO reset for ROM upgrade	Displays when iLO is reset for the ROM upgrade.
iLO reset by user diagnostics	Displays when iLO is reset by user diagnostics.
Power restored to iLO	Displays when the power is restored to iLO.
iLO reset by watchdog	Displays when an error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.
iLO reset by host	Displays when the server resets iLO.
Recoverable iLO error, code *#*	Displays when a non-critical error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.
SNMP trap delivery failure: *IP address*	Displays when the SMNP trap does not connect to the specified IP address.
Test SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Power outage SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Server reset SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Illegal login SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Diagnostic error SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Host generated SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Network resource shortage SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
iLO network link up	Displays when the network is connected to iLO.
iLO network link down	Displays when the network is not connected to iLO.
iLO Firmware upgrade started by: *User*	Displays when a user starts a firmware upgrade.
Host server reset by: *User*	Displays when a user resets the host server.
Host server powered OFF by: *User*	Displays when a user powers off a host server.
Host server powered ON by: *User*	Displays when a user powers on a host server.

Event Log Display	**Event Log Explanation**
Virtual Floppy in use by: *User*	Displays when a user begins using a Virtual Floppy.
Remote Console login: *User*	Displays when a user logs on a Remote Console session.
Remote Console Closed	Displays when a Remote Console session is closed.
Failed Console login - IP Address: *IP address*	Displays a failed console login and IP address.
Added User: *User*	Displays when a local user is added.
User Deleted by: *User*	Displays when a local user is deleted.
Modified User: *User*	Displays when a local user is modified.
Browser login: *User*	Displays when a valid user logs on to iLO using an Internet browser.
Browser logout: User	Displays when a valid user logs off iLO using an Internet browser.
Failed Browser login – IP Address: *IP address*	Displays when a browser login attempt fails.
Remote Console login: *User*	Displays when an authorized user logs on using the Remote Console port.
Remote Console Closed	Displays when an authorized Remote Console user is logged out or when the Remote Console port is closed following a failed login attempt.
Failed Console login – IP Address: *IP address*	Displays when an unauthorized user has failed three login attempts using the Remote Console port.
Added User: *User*	Displays when a new entry is made to the authorized user list.
User Deleted by: *User*	Displays when an entry is removed from the authorized user list. The User section displays the user who requested the removal.
Event Log Cleared: *User*	Displays when the user clears the Event Log.
Power Cycle (Reset): *User*	Displays when the power has been reset.
Virtual Power Event: *User*	Displays when the Virtual Power Button is used.
Security Override Switch Setting is On	Displays when the system is booted with the Security Override Switch set to On.

Event Log Display	**Event Log Explanation**
Security Override Switch Setting Changed to Off	Displays when the system is booted with the Security Override Switch changed from On to Off.
On-board clock set; was previously [NOT SET]"	Displays when the on-board clock is set. Will display the previous time or "NOT SET" if there was not a time setting previously.
Logs full SNMP trap alert failed for: *IP address*	Displays when the logs are full and the SNMP trap alert failed for a specified IP address.
Security disabled SNMP trap alert failed for: *IP address*	Displays when the security has been disabled and the SNMP trap alert failed for a specified IP address.
Security enabled SNMP trap alert failed for: *IP address*	Displays when the security has been enabled and the SNMP trap alert failed for a specified IP address.
Virtual Floppy connected by *User*	Displays when an authorized user connects the Virtual Floppy.
Virtual Floppy disconnected by *User*	Displays when an authorized user disconnects the Virtual Floppy.
License added by: *User*	Displays when an authorized user adds a license.
License removed by: *User*	Displays when an authorized user removes a license.
License activation error by: *User*	Displays when there is an error activating the license.
iLO RBSU user login: *User*	Displays when an authorized user logs in to iLO RBSU.
Power on request received by: *Type*	A power request was received as one of the following types: Power Button Wake On LAN Automatic Power On
Virtual NMI selected by: *User*	Displays when an authorized user selects the Virtual NMI button.
Virtual Serial Port session started by: *User*	Displays when a Virtual Serial Port session is started.
Virtual Serial Port session stopped by: *User*	Displays when a Virtual Serial Port session is ended.

Event Log Display	Event Log Explanation
Virtual Serial Port session login failure from: *User*	Displays when there is a login failure for a Virtual Serial Port session.

MS-DOS® Error Codes

The CPQLODOS utility sends the MS-DOS® shell a 0 (zero) when no error occurred or a 1 (one) when an error is detected. This can be misleading in that an error might have occurred even if a 0 is returned to the shell. The following can cause a 1 to be returned:

- Version incompatibility
- Wrong operating system (MS-DOS® is required)
- No Lights-Out processor found
- Flash in progress
- Virtual floppy inhibited
- Communication error
- XML error

An XML error implies that there was a problem during the XML transport but not that there was a problem with the XML content. XML content errors can go undetected and result in a zero error return.

To work around this issue, use the log feature to capture the output. The captured output will have more details about XML content errors.

Hardware and Software Link-Related Issues

The following sections discuss items to be aware of when attempting to resolve hardware or software link-related issues.

Hardware

iLO uses standard Ethernet cabling, which includes CAT5 UTP with RJ-45 connectors. Straight-through cabling is necessary for a hardware link to a standard Ethernet hub. Use a crossover cable for a direct PC connection.

Software

The iLO Management Port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, then it will reissue the request at 90-second intervals.

The DHCP server must be configured to supply DNS and WINS name resolution. iLO can be configured to work with a static IP address either in the F8 option ROM setup or from the Network Settings Web page.

The default DNS name appears on the network settings tag and can be used to locate iLO without knowing the assigned IP address.

If a direct connection to a PC is used, then a static IP address must be used because there is no DHCP server on the link.

Within the iLO RBSU, you may press the **F1** key inside the DNS/DHCP page for advanced options to view the status of iLO DHCP requests.

Login Issues

Use the following information when attempting to resolve login issues:

- Try the default login, which is located on the network settings tag.
- If you forget your password, an administrator with the Administer User Accounts privilege can reset it.
- If an administrator forgets his or her password, the administrator must use the Security Override Switch or establish an administrator account and password using HPONCFG.
- Check for standard problems, such as:

- Is the password complying with password restrictions? For example, are there case-sensitive characters in the password?
- Is an unsupported browser being used?

Login Name and Password Not Accepted

If you have connected to iLO but it does not accept your login name and password, you must verify that your login information is configured correctly. Have a user who has the Administer User Accounts privilege log in and change your password. If you are still unable to connect, have the user log in again and delete and re-add your user account.

NOTE: The RBSU can also be used to correct login problems.

Directory User Premature Logout

Network errors can cause iLO to conclude that a directory connection is no longer valid. If iLO cannot detect the directory, iLO terminates the directory connection. Any additional attempts to continue using the terminated connection redirects the browser to the Login Page.

Redirection to the Login Page can appear to be a premature session timeout. A premature session timeout can occur during an active session if:

- The network connection is severed.
- The directory server is shut down.

To recover from a premature session timeout, log back in and continue using iLO. If the directory server is unavailable, you must use a local account.

iLO Management Port Not Accessible by Name

The iLO Management Port can register with a WINS server or DDNS server to provide the name-to-IP address resolution necessary to access the iLO Management Port by name. The WINS or DDNS server must be up and running before the iLO Management Port is powered on, and the iLO Management Port must have a valid route to the WINS or DDNS server.

In addition, the iLO Management Port must be configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the DHCP server with the necessary IP addresses. You can also enter the IP addresses through RBSU or by selecting **Network Settings** on the Administration tab. The iLO Management Port must be configured to register with either a WINS server or DDNS server. These options are turned on as factory defaults and can be changed through RBSU or by selecting the **Network Settings** option on the Administration tab.

The clients used to access the iLO Management Port must be configured to use the same DDNS server where the IP address of the iLO Management Port was registered.

If you are using a WINS server and a non-dynamic DNS server, the access to the iLO Management Port might be significantly faster if you configure the DNS server to use the WINS server for name resolution. Refer to the appropriate Microsoft® documentation for more information.

iLO RBSU Unavailable after iLO and Server Reset

If the iLO processor is reset and the server is immediately reset, there is a small chance that the iLO firmware will not be fully initialized when the server performs its initialization and attempts to invoke the iLO RBSU. In this case, the iLO RBSU will be unavailable or the iLO Option ROM code will be skipped altogether. If this happens, reset the server a second time. To avoid this issue, wait a few seconds before resetting the server after resetting the iLO processor.

Inability to Access the Login Page

If you cannot access the login page, you must verify the SSL encryption level of your browser is set to 128 bits. The SSL encryption level in iLO is set to 128 bits and cannot be changed. The browser and iLO encryption levels must be the same.

Inability to Access iLO Using Telnet

If you cannot access iLO using Telnet, you must verify the Remote Console Port Configuration and Remote Console Data Encryption on the Global Settings screen. If Remote Console Port Configuration is set to Automatic, the Remote Console applet enables port 23, starts a session, and then closes port 23 when the session is completed. Telnet cannot automatically enable port 23, so it fails. For more information on Telnet settings, refer to the "Telnet Support (on page 116)" section.

Inability to Access Virtual Media or Graphical Remote Console

Virtual media and graphical Remote Console are only enabled by licensing the optional iLO Advanced Pack. A message is displayed to inform the user that the features are not available without a license. Although up to 10 users are allowed to log into iLO, only one user can access the remote console. A warning message is displayed to say that the Remote Console is already in use.

Inability to Connect to iLO after Changing Network Settings

Verify that both sides of the connection, the NIC and the switch, have the same settings for transceiver speed autoselect, speed, and duplex. For example, if one side is autoselecting the connection, then the other side should as well. The settings for the iLO NIC are controlled in the Network Settings screen.

Inability to Connect to the iLO Diagnostic Port

If you cannot connect to the iLO Diagnostic Port through the NIC, be aware of the following:

- The use of the diagnostic port is automatically sensed when an active network cable is plugged in to it. When switching between the diagnostic and back ports, you must allow one minute for the network switchover to be complete before attempting connection through the Web browser.
- If a critical activity is in progress, the diagnostic port cannot be used until the critical activity is complete. Critical activities include:

  - Firmware upgrade
  - Remote Console session
  - SSL initialization

- If you are using a client workstation that contains more than one enabled NIC, such as a wireless card and a network card, a routing issue might prevent you from accessing the diagnostic port. To resolve this issue:

1. Have only one active NIC on the client workstation. For example, disable the wireless network card.
2. Configure the IP address of the client workstation network to match the iLO Diagnostic Port network.
   a. The IP address setting should be 192.168.1.*X,* where *X* is any number other than 1, because the IP address of the diagnostic port is set at 192.168.1.1.
   b. The subnet mask setting should be 255.255.255.0.

Inability to Connect to the iLO Processor through the NIC

If you cannot connect to the iLO processor through the NIC, try any or all of the following troubleshooting methods:

- Confirm that the green LED indicator (link status) on the iLO RJ-45 connector is on. This indicates a good connection between the PCI NIC and the network hub.
- Look for intermittent flashes of the green LED indicator, which indicates normal network traffic.
- Run the iLO RBSU to confirm that the NIC is enabled and verify the assigned IP address and subnet mask.
- Run the iLO RBSU and use the F1-Advanced tab inside of the DNS/DHCP page to see the status of DHCP requests.
- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with browser software by typing the IP address of the NIC as the URL. You can see the iLO Home page from this address.
- Reset iLO.

NOTE: If a network connection is established, you may have to wait up to 90 seconds for the DHCP server request.

ProLiant BL p-Class servers have a diagnostic port available. Connecting a live network cable to the diagnostic port will cause iLO to automatically switch from the iLO port to the diagnostic port. When switching between the diagnostic and back ports, you must allow one minute for the network switchover to be complete before attempting connection through the Web browser.

Inability to Log into iLO after Installing the iLO Certificate

If the iLO self-signed certificate is installed permanently into some browsers, and the iLO is reset, it may not be possible to log back into iLO because iLO generates a new self-signed certificate every time it is reset. When a certificate is installed into the browser, it is indexed by the name contained in the certificate. This name is unique to each iLO. Every time iLO resets, it generates a new certificate with the same name.

To avoid this problem, the iLO self-signed certificate should not be installed into the browser certificate store. If you want to install the iLO certificate, a permanent certificate should be requested from a CA and imported into the iLO. This permanent certificate can then be installed into the browser certificate store.

In particular, Netscape 7.1 will not display the iLO login screen after iLO is reset, if the self-signed certificate has been installed into the certificate store. In order to log in, the previously stored certificate must first be deleted from the browser certificate store. Netscape 7.1 stores the iLO self-signed certificate in the authorities store, not the website store.

Netscape 7.02 does not allow previously stored certificates to be deleted. Upgrade to Netscape 7.1 if the self-signed certificate is installed in the browser certificate store.

Firewall Issues

iLO communicates through several configurable TCP/IP ports. If these ports are blocked, the administrator must configure the firewall to allow for communications on these ports. Refer to the Global Settings option in the Administration tab to view or change port configurations.

Proxy Server Issues

If the Web browser software is configured to use a proxy server, it will not connect to the iLO IP address. To resolve this issue, configure the browser not to use the proxy server for the IP address of iLO. For example, in Internet Explorer, select **Tools, Internet Options, Connections, LAN Settings, Advanced,** and then enter the iLO IP address or DNS name in the Exceptions field.

Troubleshooting Alert and Trap Problems

Alert	Explanation
Test Trap	This trap is generated by a user through the Web configuration page.
Server Power Outage	Server has lost power.
Server Reset	Server has been reset.
Failed Login Attempt	Remote user login attempt failed.
General Error	This is an error condition that is not predefined by the hard-coded MIB.
Logs	Circular log has been overrun.
Security Override Switch Changed: On/Off	The state of the Security Override Switch has changed (On/Off).
Rack Server Power On Failed	The server was unable to power on because the BL p-Class rack indicated that insufficient power was available to power on the server.
Rack Server Power On Manual Override	The server was manually forced by the customer to power on despite the BL p-Class reporting insufficient power.
Rack Name Changed	The name of the ProLiant BL p-Class rack was changed.

Inability to Receive Insight Manager 7 or Systems Insight Manager Alarms (SNMP Traps) from iLO

A user with the Configure iLO Settings privilege must connect to iLO to configure SNMP trap parameters. When connected to iLO, be sure that the correct alert types and trap destinations are enabled in the SNMP/Insight Manager Settings screen of the iLO console application.

iLO Security Override Switch

The iLO Security Override Switch allows emergency access to the administrator with physical control over the server system board. Setting the iLO Security Override Switch allows login access, with all privileges, without a user ID and password.

The iLO Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure. To set the iLO Security Override Switch, the server must be powered off and disconnected from the power source. Set the switch and then power on the server. Reverse the procedure to clear the iLO Security Override Switch.

A warning message is displayed on the iLO Web pages, indicating that the iLO Security Override Switch is currently in use. An iLO log entry is added recording the use of the iLO Security Override Switch. An SNMP alert may also be sent upon setting or clearing the iLO Security Override Switch.

In the unlikely event that it is necessary, setting the iLO Security Override Switch also enables you to flash the iLO boot block. The boot block is exposed until iLO is reset. HP recommends that you disconnect iLO from the network until the reset is complete.

Depending on the server, the iLO Security Override Switch may be a single jumper or it may be a specific switch position on a dip switch panel. To access the iLO Security Override Switch, refer to the server documentation.

Authentication Code Error Message

Within a Netscape or Mozilla browser, you might receive an incorrect message authentication code error message, which indicates that the public or private keypair and certificate used to initiate the browser's SSL session has changed. This error message can occur when you do not use a customer provided certificate, because iLO generates its own self-signed certificate each time it is rebooted.

To resolve this issue, close and restart the Web browser, or install your own certificates into iLO.

Troubleshooting Mouse Problems

The following sections discuss troubleshooting mouse hardware or software issues.

Local USB Mouse and Linux

If you are running Linux on your server and the local mouse is USB, your mouse will not work in Remote Console. To correct this issue, configure the system to use two mice. Add the following lines to your XF86Config file:

- In the ServerLayout section, add the following:

  ```
  InputDevice    "Mouse1" "SendCoreEvents"
  ```

  For example:

  ```
  Section "ServerLayout"
     Identifier  "Default Layout"
     Screen 0    "Screen0" 0 0
     InputDevice "Mouse0" "CorePointer"
     InputDevice "Mouse1" "SendCoreEvents"
     InputDevice "Keyboard0" "CoreKeyboard"
  EndSection
  ```

- In the InputDevice section, add the following:

  ```
  Section "InputDevice"
     Identifier  "Mouse1"
     Driver      "mouse"
     Option"Protocol" "PS/2"
     Option"Device" "/dev/psaux"
     Option"Emulate3Buttons" "yes"
  EndSection
  ```

After updating the configuration file, you have two InputDevice sections. Each section lists information for the mouse. Adjust the identifier to match the label you used in the ServerLayout section.

Format is operating-system based. You might need to change the format of the examples for your operating system. For example, Red Hat 3.0 uses Mouse0 for the default label, but SUSE 8 uses Mouse[1]. Follow the naming conventions for your operating system. Use a unique label for each mouse. The Input Device section describes your currently working USB mouse and is a good guide to use when configuring the second mouse. After saving the changes, restart the system.

Mouse Issue Using SuSE Linux

United Linux 1.0 powered SuSE Linux Enterprise 8.0 users might experience mouse issues when rebooting with Remote Console. To correct this issue, select PS/2 mouse (Aux-port) type when prompted by YaST mouse configuration application in text mode.

If iLO Remote Console is closed and use of the mouse wheel is desired on a wheel mouse connected to the server, run YaST2 Control Center and select Intelli/Wheel mouse (Aux-port).

Remote Console Mouse Control Issue

While using Remote Console on a server running Microsoft® Windows® Server 2003, mouse movement can be slow, and it might be difficult to navigate to each of the four corners of the screen. When trying to reach a far corner of the screen, the mouse can disappear completely.

> **NOTE:** This mouse behavior is more pronounced when the Remote Console session is running in a browser applet window that is smaller than the size of the server screen, and scrolling is required to see the full contents of the screen, which are not displayed.

To resolve this issue:

1. Select **Start>Settings>Control Panel>Mouse Properties** from the Windows® Server 2003 desktop applet.
2. Disable the Enhance pointer precision parameter.

If mouse movement is still sluggish:

1. Select **Start>Settings>Control Panel>Display>Settings>Advanced>Troubleshooting>** from the Windows® Server 2003 desktop applet.
2. Set the slider control to full hardware acceleration.

For more information, refer to the "Optimizing Performance for Graphical Remote Console (on page 54)" section.

Emulating a PS/2 Keyboard in a Headless Server Environment

iLO will emulate a PS/2 keyboard in a headless server environment. When iLO detects that the server is going through POST, iLO scans for a PS/2 keyboard. If no local PS/2 keyboard is detected, iLO will be the PS/2 keyboard for the server.

Troubleshooting Remote Console Problems

The following sections discuss troubleshooting Remote Console issues. In general:

- Pop-up blockers prevent Remote Console and Virtual Serial Port from starting.
- Pop-up blocking applications that are set to prevent the automatic opening of new windows prevent Remote Console and Virtual Serial Port from running. Disable any pop-up blocking programs before starting Remote Console or Virtual Serial Port.

Linux Remote Console

When using a Linux client machine with a JVM other than 1.4.2, you might experience some issues with Remote Console. For example, if you resize the Remote Console window, the entire window can turn gray. These issues are caused by the JVM. To correct this problem, use JVM 1.4.2. JVM 1.4.2 and 1.4.2_02 are different, and problems have been observed in 1.4.2_02 that do not occur in 1.4.2. JVM 1.4.2 is supported on the following operating system and browser combinations:

- Red Hat 7.3 Professional

  - Mozilla 1.6
  - Mozilla 1.7 RC3
  - Netscape 7.1
- Red Hat 8 Professional
  - Mozilla 1.6
  - Mozilla 1.7 RC3
  - Netscape 7.1
- SuSE 9 Professional
  - Mozilla 1.7 RC3
  - Netscape 7.1
- United Linux 1.0 Professional
  - Mozilla 1.7 RC3
  - Netscape 7.1

Inability to Navigate the Single Cursor of the Remote Console to Corners of the Remote Console Window

In some cases, you may be unable to navigate the mouse cursor to the corners of the Remote Console window. If so, right-click and drag the mouse cursor outside the Remote Console window and back inside.

If the mouse still fails to operate correctly, or if this situation occurs frequently, verify that your mouse settings match those recommended in the "Optimizing Performance for Graphical Remote Console (on page 54)" section.

Remote Console No Longer Opens on the Existing Browser Session

With the addition of the Terminal Services Pass-Through function, the behavior of the Remote Console applet is slightly different from previous versions of iLO firmware. If a Remote Console session is already open, and the Remote Console link is clicked again, the Remote Console session will not restart. It may appear to the user as if the Remote Console session has frozen.

For example, if the following steps are executed:

1. From Client-1, login to iLO and open a remote console session.
2. From Client-2, login to iLO and try to open a Remote Console session. The message `Remote console is already opened by another session` is displayed. This is expected because only one Remote Console session is supported at a time.
3. Return to Client-1 and close the Remote Console session.
4. From Client-2, click the Remote Console link with the old Remote Console applet still open. The remote console session will not refresh and the old message discussed in step 2 is still displayed.

Although this behavior is different than in previous versions of iLO firmware, this is expected behavior in this version of the iLO firmware. To avoid problems of this nature, always close an open remote console session prior to trying to reopen it.

Remote Console Text Window not Updating Properly

When using the Remote Console to display text windows that scroll at a high rate of speed, the text window might not update properly. This error is caused by video updates occurring quicker than the iLO firmware can detect and display them. Typically, only the upper left corner of the text window updates while the rest of the text window remains static. After the scrolling is complete, click **Refresh** to properly update the text window.

One known example of this issue is during the Linux booting and posting process, in which some of the POST messages can be lost. A possible repercussion is that a keyboard response will be requested by the boot process and will be missed. To avoid this issue, the booting and posting process should be slowed down by editing the Linux startup script to allow more time for keyboard responses.

Remote Console Turns Grey or Black

The Remote Console screen will turn gray or black when the server is rebooted from the Terminal Services client. The screen will remain gray or black for 30 seconds to one minute. The client will close because the Terminal Services server is not available. The iLO remote console should take over, but the Remote Console screen will turn gray or black. When the screen returns, the Remote Console functions normally.

Troubleshooting SSH and Telnet Problems

The following sections discuss troubleshooting SSH and telnet issues.

Initial PuTTY Input Slow

During initial connection using a PuTTY client, input is accepted slowly for approximately 5 seconds. This can be addressed by changing the configuration options in the client under the Low-level TCP connection options, uncheck the **Disable Nagle's algorithm** option. Under telnet options, set telnet negotiation mode to **Passive.**

PuTTY Client Unresponsive with Shared Network Port

When using PuTTY client with the Shared Network Port, the PuTTY session may become unresponsive when a large amount a data is transferred or when using a Virtual Serial Port and Remote Console. To correct the issue, close the PuTTY client, and restart the session.

SSH Text Support from a Remote Conosle Session

The telnet and SSH access from text Remote Console supports the standard 80 x 25 configuration of the text screen. This mode is compatible for text Remote Console for the majority of available text mode interfaces in current operating systems. Extended text configuration beyond the 80 x 25 configuration is not displayed correctly when using telnet or SSH. HP recommends configuring the text application in 80 x 25 mode or use the iLO Remote Console applet provided by the web interface.

Troubleshooting Terminal Services Problems

The following sections discuss troubleshooting Remote Console issues.

Terminal Services Button Is Not Working

The Terminal Services option will not function if the Deny option is selected on the Java security warning popup. When the Deny option is selected, you are telling the browser that the Remote Console applet is not trustworthy. The Remote Console will not be allowed to execute any code requiring a higher level of trust. If the Deny option is select, the Remote Console is not allowed to launch the code required to activate the Terminal Services button. If you look in the Java Console, you will see a `"Security Exception - Access denied"` message.

Terminal Services Proxy Stops Responding

Any time iLO is reset (such as changing network settings or global settings), Terminal Services pass-through is unavailable for two minutes from the beginning of the reset. iLO requires 60 seconds to complete the reset and POST with a 60-second buffer before continuing. After two minutes, the status changes to Available and Terminal Services pass-through is available for use.

Troubleshooting Video and Monitor Problems

The following sections discuss items to be aware of when attempting to resolve video and monitor issues.

General Guidelines

- The client screen resolution must be greater than the screen resolution of the remote server.
- The iLO Remote Console only supports the ATI Rage XL video chip that is integrated in the system. The Remote Console functionality of iLO does not work if you install a plug-in video card. All other iLO functionality is available if you choose to use a plug-in video card.
- Only one user at a time is allowed to access the Remote Console. Check to see if another user is logged into iLO.

Telnet Displays Incorrectly in DOS®

When using the iLO Telnet session to display text screens involving a maximized DOS® window, the telnet session is unable to represent anything except the upper portion of the screen if the server screen is larger than 80x25.

To correct this adjust the DOS® windows properties to limit its size to 80x25, before maximizing the DOS window.

- On the title bar of the DOS® window, right-click the mouse and select **Properties** and select **Layout.**
- On the Layout tab, change the Screen Buffer Size height to 25.

Video Applications not Displaying in the Remote Console

Some video applications, such as Microsoft® Media Player, will not display, or will display incorrectly, in the Remote Console. This problem is most often seen with applications that use video overlay registers. Typically, applications that stream video use the video overlay registers. iLO is not intended for use with this type of application.

Troubleshooting Virtual Media Problems

The following sections discuss troubleshooting Virtual Media issues.

Virtual Drive Listing

When using Terminal Services pass-through on a server running Windows® 2000, a Virtual CD-ROM session does not appear on the server. This issue does not exist if the server is running Windows® 2003. The same behavior occurs when connecting to Terminal Services directly. This is not a problem with the iLO Terminal Services pass-through feature.

Virtual Media Applet has a Red X and Will Not Display

The Virtual Media applet may produce a red X if an unsupported browser or JVM is used, or if Enable All Cookies is not enabled. To correct this, ensure you are using a supported browser and JVM on your client by reviewing the support matrix found in the "Supported Browsers (on page 18)" section. Also be sure Enable All Cookies is selected on the browser Preferences or Options menu. Some browsers do not enable this cookies by default.

Virtual Floppy Media Applet is Unresponsive

iLO Virtual Floppy media applet can become unresponsive if the physical floppy diskette contains media errors.

To prevent the virtual floppy media applet from becoming unresponsive, run CHKDSK.EXE (or a similar utility) to check the physical floppy diskette media for errors. If the physical media contains errors, reload the floppy diskette image onto a new physical floppy diskette.

Troubleshooting Miscellaneous Problems

The following sections discuss troubleshooting miscellaneous hardware or software issues.

Cookie Sharing Between Browser Instances and iLO

iLO uses browser session cookies in part to distinguish separate logins—each browser window displays as a separate user login—while actually sharing the same active session with the iLO. These multiple logins can confuse the browser. This confusion can appear as an iLO issue is a manifestation of typical browser behavior.

Several processes can cause a browser to open additional windows. Browser windows opened from within an open browser represent different aspects of the same program in memory. Consequently, each browser window shares properties with the parent, including cookies.

Shared Instances

When iLO opens another browser window, for example, Remote Console, Virtual Media, or Help, this window shares the same connection to iLO and the session cookie.

The iLO Web server makes URL decisions based on each request received. For example, if a request does not have access rights, it is redirected to the login page, regardless of the original request. Web server based redirection, selecting **File>New>Window** or pressing the **Ctrl+N** keys, opens a duplicate instance of the original browser.

Cookie Order Behavior

During login, the login page builds a browser session cookie that links the window to the appropriate session in the firmware. The firmware tracks browser logins as separate sessions listed in the Active Sessions section of the iLO Status page.

For example, when User1 logs in, the Web server builds the initial frames view, with current user: User1 in the top pane, menu items in the left pane, and page data in the lower-right pane. As User1 clicks from link to link, only the menu items and page data are updated.

While User1 is logged in, if another user, User2, opens another browser window on the same client and logs in, the second login overwrites the cookie generated in the original User1 session. Assuming that User2 is a different user account, a different current frame is built, and a new session is granted. The second session is displayed in the Active Sessions section of the iLO Status page as current user: User2.

The second login has effectively orphaned the first session (User1) by wiping out the cookie generated during User1's login. This behavior is the same as closing User1's browser without clicking the Log Out link. User1's orphaned session is reclaimed when the session timeout expires.

Because the current user frame is not refreshed unless the browser is forced to refresh the entire page, User1 can continue navigating using his or her browser window. However, the browser is now operating using User2's session cookie settings, even though it is not readily apparent.

If User1 continues to navigate in this mode (User1 and User2 sharing the same process because User2 logged in and reset the session cookie), the following can occur:

- User1's session behaves consistently with the privileges assigned to User2.
- User1's activity keeps User2's session alive, but User1's session can time out unexpectedly.
- Logging out of either window causes both window sessions to terminate. The next activity in the other window can redirect the user to the login page as if a session timeout or premature timeout occurred.
- Clicking Log Out from the second session (User2) results in a `Logging out:  unknown page to display before redirecting the user to the login page.`
- If User2 logs out then logs back in as User3, User1 assumes User3's session.
- If User1 is at login, and User2 is logged in, User1 can alter the URL to redirect to the index page. It appears as if User1 has accessed iLO without logging in.

These behaviors continue as long as the duplicate windows are open. All activities are attributed to the same user, using the last session cookie set.

Displaying the Current Session Cookie

After logging in, you can force the browser to display the current session cookie by entering `javascript:alert(document.cookie)` in the URL navigation bar. The first field visible is the session ID. If the session ID is the same among the different browser windows, then these windows are sharing the same iLO session.

You can force the browser to refresh and reveal your true identity by pressing the F5 key, selecting **View**>**Refresh,** or using the refresh button.

Preventing Cookie-Related User Issues

To prevent cookie-based behavioral problems:

- Start a new browser for each login by double-clicking the browser icon or shortcut.
- Click the **Log Out** link to close the iLO session before closing the browser window.

Inability to Get SNMP Information from Insight Manager 7 or Systems Insight Manager

The agents running on the managed server supply SNMP information to <insight_namanger> or Systems Insight Manager. For agents to pass information through iLO, iLO device drivers must be installed. Refer to the "Installing iLO Device Drivers (on page 24)" section for installation instructions.

If you have installed the drivers and agents for iLO, verify that iLO and the management PC are on the same subnet. You can verify this quickly by pinging iLO from the management PC. Consult your network administrator for proper routes to access the network interface of iLO.

Incorrect Time or Date of the Entries in the Event Log

You can update the time and date on iLO by running the RBSU. This utility automatically sets the time and date on the processor using the server time and date. The time and date are also updated by Insight Management agents on supported network operating systems.

Inability to Upgrade iLO Firmware

If you attempt to upgrade the iLO firmware and it does not respond, does not accept the firmware upgrade, or is terminated before a successful upgrade, the following options are available:

- iLO network flash recovery
- ROMPaq

iLO Network Flash Recovery

The iLO network flash recovery payload enables you to recover from a failed firmware upgrade. The flash recovery payload uses FTP, which can only be used when the flash recovery payload is active, to transfer the firmware image to iLO. The flash recovery payload should only be used if:

- Previous firmware upgrade attempts have failed.
- You are unable to connect to the Web browser.
- No other firmware upgrade option is available. Servers with a floppy drive can use the ROMPaq option. ProLiant BL p-Class servers must use the flash recovery payload.

If the iLO firmware image is damaged, missing, or otherwise corrupted, then the iLO flash recovery process is used to re-flash iLO. The flash recovery process is for the sole purpose of getting the system re-flashed. No other processes can be run until the recovery process is complete.

Diagnostic Steps

Before attempting a flash recovery of the firmware, use the following diagnostic steps to verify that flash recovery is needed:

1. Attempt to connect to iLO through the Web browser. If you are unable to connect, then there is a communication problem.
2. Attempt to ping iLO. If you are successful, then the network is working.
3. Attempt to open an FTP session to the IP address or DNS name of iLO. If you are successful, then the flash recovery payload is active and it is necessary to upgrade the firmware using the flash recovery process.
4. If you cannot open an FTP session, then the system is not in recovery mode. Attempt to reset iLO using the steps in the "Resetting iLO (on page 395)" section.

Flash Recovery Process

If you have verified that the flash recovery process is necessary through the diagnostic steps:

1. Open an FTP session to the IP address or DNS name of iLO.
2. Log in to iLO using the fixed username `flash` and the password of `recovery.` The username and password are case-sensitive.
3. At the FTP prompt, enter the `put` command and the file name of the firmware image.

The following is an example of the entries used for the flash recovery process:

```
ftp 192.168.177.142
   login: flash
   password: recovery
   put \iLO160.bin
```

- If the file is found, then the `put` command transfers the file to iLO, the image is validated, and the flashing process begins.
- If the file is not found, then some versions of the `put` command do not report an error message.
- If the directory path includes spaces, enclose the path and filename in quotes.

After the firmware image is transferred, the recovery payload calculates the check sum, validates the digital signature, and reports if the image is valid. The flash reprogramming begins if the image is valid, and flashing progress is then reported to the client.

NOTE: This process will take a few seconds while the recovery payload decrypts the stored hash and computes a hash for the image to compare against. If the image is valid, the FTP server begins programming the image into the flash part and providing status updates.

When completed, the flash recovery payload module disconnects and reboots the iLO processor. If the flash recovery process is unsuccessful, attempt the process again while you view the progress for any errors. It might be necessary to use a different firmware image for the process.

ROMPaq

Using ROMPaq to upgrade the iLO firmware involves two procedures: The first can be performed on any server, and the second must be performed on the iLO host server.

Complete this procedure on any server:

1. Download the latest iLO firmware SoftPaq. Select the SoftPaq image for diskettes and save it to the hard drive. The SoftPaq can be downloaded from the HP website (http://www.hp.com/servers/lights-out).
2. Execute the SoftPaq to create diskettes.

Complete this procedure only on the iLO host server:

1. Boot the system from the ROMPaq diskette.
2. Press the **Enter** key at the ROMPaq welcome screen. A screen displays the devices in your server that can be upgraded.
3. Use the cursors to select **iLO Management** and press the **Enter** key. A screen displays the firmware images that ROMPaq can install.
4. Use the cursors to highlight the appropriate image and press the **Enter** key.
5. Press the **Enter** key again. ROMPaq reads the firmware image. If you are prompted to enter additional diskettes put in the appropriate diskette and press the **Enter** key.
6. Press the **Enter** key again to begin reprogramming the ROM. Do not power cycle, reboot, or turn off the system while this process is taking place.
7. After you receive a message that the flash programming has completed successfully, press the **Enter** key.

8. Press the **Enter** key to reprogram another device, or press the **Esc** key to return to the `A:\` prompt.

It might be necessary to set the Security Override Switch to perform the ROMPaq upgrade. The ROMPaq program informs you if the Security Override Switch must be set.

If none of the above solves the issue:

1. Remove the power from the server and the system battery.
2. Wait a few minutes.
3. Replace the battery, and power to the server.

This may return iLO to the default state.

iLO Does Not Respond to SSL Requests

iLO does not respond to SSL requests when a Java™ warning appears. If a user is logging into an iLO browser connection and does not complete the login process by responding to the Java certificate warning, iLO does not respond to future browser requests. The user must continue the login process to free the iLO Web server.

Testing SSL

The following test checks for the correct security dialog prompt. A non-working server will proceed to a `Page cannot be displayed` message. If this test fails, your domain controller is not accepting SSL connections, and probably has not been issued a certificate.

1. Open a browser and navigate to <https://<*domain controller*>:636.

   You can substitute <*domain*> in place of <*domain controller*> which goes to the DNS and checks which domain controller is handling requests for the domain. Test multiple domain controllers to verify all of them have been issued a certificate.

2. If SSL is operating correctly on the domain controller (a certificate is issued), you are prompted with a security message asking if you want to proceed with accessing the site, or view the server's certificate. Clicking **Yes** does not display a web page. This is normal. This process is automatic, but might require rebooting. To avoid rebooting:
   a. Open the MMC and add the certificates snap-in. When prompted, select **Computer Account** for the type of certificates you want to view. Click **OK** to return to the certificates snap in.
   b. Select **Personal>Certificates** folder. Right-click the folder and select **Request New Certificate.**
   c. Verify Type is domain controller and click **Next** until a certificate is used.

You can also use Microsoft® LDP tool to verify SSL connections. For more information on the LDP tool, go to the Microsoft® website (http://www.microsoft.com/support).

An old certificate can cause problems with SSL can on the domain controller pointing when it points to a previously trusted CA with the same name, which is rare but might happen if a certificate service is added and removed and then added again on the domain controller. To remove old certificates and issue a new one follow the instructions in Step 2.

Resetting iLO

In rare instances, it might be necessary to reset iLO; for example, if iLO is not responding to the browser. To reset iLO, you must power down the server and disconnect the power supplies completely.

iLO may reset itself in certain instances. For example, an internal iLO watchdog timer resets if the firmware detects an iLO problem. If a firmware upgrade is completed or a network setting is changed, iLO also resets.

The HP Management Agents 5.40 and later have the ability to reset iLO. To reset iLO, select the **Reset** iLO option on the HP Management Agent Web page under the iLO section.

You can also manually force the iLO management processor to reset by clicking **Apply** on the Network Settings page. You do not need to change any parameters before clicking Apply.

Server Name Still Present after ERASE Utility is Executed

The Server Name field is communicated to iLO through the Insight Manager Agents. To change the Server Name field after a redeployment of a server, load the Insight Manager Agents to update the Server Name field with the new server name.

To remove the Server Name field after a redeployment of a server, use the Reset to Factory Defaults feature of the iLO RBSU utility to clear the Server Name field.

This procedure clears all iLO configuration information, not just the Server Name information.

Troubleshooting a Remote Host

Troubleshooting a remote host server might require restarting the remote system. You can restart the remote host server by using the options listed in the Virtual Devices tab.

Technical Support

In This Section

HP Contact Information

For the name of the nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- In other locations, refer to the HP website (http://www.hp.com).

For HP technical support:

- In North America, call the HP Technical Support Phone Center at 1-800-633-3600. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to the HP website (http://www.hp.com).

Before You Contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware

- Third-party hardware or software
- Operating system type and revision level

Acronyms and Abbreviations

ACPI

Advanced Configuration and Power Interface

ARP

Address Resolution Protocol

ASCII

American Standard Code for Information Interchange

ASM

Advanced Server Management

ASR

Automatic Server Recovery

CA

certificate authority

CGI

Common Gateway Interface

CLI

Command Line Interface

CR

Certificate Request

DAV

Distributed Authoring and Versioning

DDNS

Dynamic Domain Name System

DHCP

Dynamic Host Configuration Protocol

DLL

dynamic link library

DNS

domain name system

DSA

Digital Signature Algorithm

EMS

Emergency Management Services

EULA

end user license agreement

FEH

fatal exception handler

FSMO

Flexible Single-Master Operation

GUI

graphical user interface

HB

heartbeat

HPONCFG

HP Lights-Out Online Configuration utility

HPQLOMGC

HP Lights-Out Migration Command Line

HPQLOMIG

HP Lights-Out Migration

ICMP

Internet Control Message Protocol

iLO

Integrated Lights-Out

IML

Integrated Management Log

IP

Internet Protocol

JVM

Java Virtual Machine

LAN

local-area network

LDAP

Lightweight Directory Access Protocol

LED

light-emitting diode

LOM

Lights-Out Management

LSB

least significant bit

MAC

medium access control

MLA

Master License Agreement

MMC

Microsoft® Management Console

MP

Multilink Point-to-Point Protocol

MTU

maximum transmission unit

NIC

network interface controller

NMI

non-maskable interrupt

NVRAM

non-volatile memory

PERL

Practical Extraction and Report Language

PKCS

Public-Key Cryptography Standards

POST

Power-On Self-Test

PSP

ProLiant Support Pack

RAS

remote access service

RBSU

ROM-Based Setup Utility

RDP

Remote Desktop Protocol

RIB

Remote Insight Board

RIBCL

Remote Insight Board Command Language

RILOE

Remote Insight Lights-Out Edition

RILOE II

Remote Insight Lights-Out Edition II

RSA

Rivest, Shamir, and Adelman public encryption key

RSM

Remote Server Management

SLES

SuSE Linux Enterprise Server

SNMP

Simple Network Management Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

TCP

Transmission Control Protocol

UART

universal asynchronous receiver-transmitter

UID

unit identification

USB

universal serial bus

VM

Virtual Machine

VPN

virtual private networking

WINS

Windows® Internet Naming Service

XML

extensible markup language

Index