© Copyright 2005 Hewlett-Packard Development Company, L.P.

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.

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.

Microsoft, Windows, and Windows NT 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.

July 2005 (Second Edition)
Part Number 382327-002

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 11
  Guide overview ................................................................................................................. 11
  New in this version .......................................................................................................................... 11
  Removed in this version ........................................................................................................ 12
  Usage model .................................................................................................................... 12
  Network connection overview ........................................................................................................... 13
  Supported server operating system software ..................................................................................... 14
  Supported browsers and client operating systems .............................................................................. 15
    Linux browser configuration .................................................................................................. 16

Configuring iLO 17
  iLO configuration options ...................................................................................................... 17
  iLO RBSU .............................................................................................................................. 18
  Browser-based setup ............................................................................................................ 19
  Installing iLO device drivers ................................................................................................... 20
    Novell NetWare Server Driver Support .................................................................................. 21
    Red Hat Linux and SuSE Linux server driver support ........................................................... 22
  Enabling iLO Advanced functionality ............................................................................................... 23
    iLO Advanced evaluation license ........................................................................................... 24
    iLO Advanced license options................................................................................................ 24
    Activating iLO Advanced features using a browser .................................................................. 24
  ProLiant BL p-Class configuration ............................................................................................. 26
    ProLiant BL p-Class user requirements .................................................................................. 26
    Static IP bay configuration ..................................................................................................... 26
    HP BladeSystem setup ........................................................................................................... 31
  Integration with RILOE II accessory boards ................................................................................. 37

Using iLO 39
  Logging in to iLO for the first time ........................................................................................... 39
  Progressive delays for failed browser login attempts ............................................................. 40
  Help ..................................................................................................................................... 40
  System Status .................................................................................................................. 40
    Status Summary ................................................................................................................. 40
    iLO Status .......................................................................................................................... 40
    Server Status ..................................................................................................................... 41
    iLO Event Log .................................................................................................................... 42
Directory services for Active Directory.......................................................... 166
Active Directory Lights-Out management......................................................... 183
Directory services for eDirectory ................................................................. 184
User login using directory services............................................................... 196
Configuring directory settings...................................................................... 197
Directory tests ........................................................................................... 199

Directory-enabled remote management ....................................................... 201
  Introduction to directory-enabled remote management............................ 201
  Using bulk import tools.............................................................................. 202
  Using existing groups................................................................................ 203
  Using multiple roles.................................................................................. 204
  Creating roles to follow organizational structure...................................... 205
  Restricting roles...................................................................................... 205
    Role time restrictions.......................................................................... 206
    IP address range restrictions............................................................... 206
    IP address and subnet mask restrictions.............................................. 206
    DNS-based restrictions....................................................................... 207
    Role address restrictions................................................................... 207
  How directory login restrictions are enforced........................................... 208
  How user time restrictions are enforced................................................... 208
  User address restrictions....................................................................... 209
  Creating multiple restrictions and roles.................................................... 210

Certificate services ................................................................................ 213
  Introduction to certificate services......................................................... 213
  Installing certificate services................................................................. 213
  Verifying directory services.................................................................. 214
  Configuring Automatic Certificate Request........................................... 214

Lights-Out directories migration utilities .................................................. 217
  Introduction to Lights-Out migration utilities.......................................... 217
  Compatibility......................................................................................... 218
  Pre-migration checklist......................................................................... 218
  HP Lights-Out directory package............................................................ 219
  HPQLOMIG operation............................................................................ 220
    Finding management processors....................................................... 220
    Upgrading firmware on management processors................................ 222
    Selecting a directory access method................................................ 225
    Naming management processors...................................................... 226
    Configuring directories when HP Extended schema is selected........... 227
    Configuring directories when schema-free integration is selected........ 229
    Setting up management processors for directories............................ 231
  HPQLOMGC Operation.......................................................................... 232
Launching HPQLOMGC using application launch ..............................................................233

Insight Manager 7 integration .................................................................................................237
Integrating iLO with Insight Manager 7 ....................................................................................237
Functional overview ..................................................................................................................238
Identification and association .....................................................................................................238
Status .........................................................................................................................................239
Queries ......................................................................................................................................239
Links .........................................................................................................................................239
Configuring identification of iLO ................................................................................................240
Receiving SNMP alerts in Insight Manager 7 ..........................................................................240
Port matching ...............................................................................................................................242
Reviewing iLO advanced license information in Insight Manager 7 ..........................................242
ProLiant BL p-Class rack visualization .......................................................................................244

Systems Insight Manager integration ..........................................................................................245
Integrating iLO with Systems Insight Manager ..........................................................................245
Systems Insight Manager functional overview ...........................................................................246
Systems Insight Manager identification and association ...........................................................247
Systems Insight Manager status ..................................................................................................247
Systems Insight Manager links ...................................................................................................248
Systems Insight Manager systems lists .......................................................................................248
Configuring Systems Insight Manager identification of iLO .......................................................248
Receiving SNMP alerts in Systems Insight Manager .................................................................249
Systems Insight Manager port matching ....................................................................................250
Reviewing iLO Advanced Pack license information in Systems Insight Manager .........................251
Systems Insight Manager ProLiant BL p-Class rack visualization ............................................251

Troubleshooting iLO ..................................................................................................................253
Minimum requirements ..............................................................................................................253
iLO POST LED indicators ........................................................................................................254
Event log entries .......................................................................................................................256
Hardware and software link-related issues ..................................................................................260
Hardware ....................................................................................................................................260
Software .....................................................................................................................................260
Login issues ................................................................................................................................261
Login name and password not accepted .....................................................................................261
Directory user premature logout ...............................................................................................262
iLO Management Port not accessible by name .........................................................................262
iLO RBSU unavailable after iLO and server reset ......................................................................263
Inability to access the login page ...............................................................................................263
Inability to access iLO using Telnet ...........................................................................................263
Inability to access virtual media or graphical remote console ....................................................263
Inability to connect to iLO after changing network settings .................................................. 264
Inability to connect to the iLO Diagnostic Port ................................................................. 264
Inability to connect to the iLO processor through the NIC ............................................... 265
Inability to log in to iLO after installing the iLO certificate ............................................... 265
Firewall issues .................................................................................................................. 266
Two-factor authentication login failure ............................................................................. 267
Proxy server issues ......................................................................................................... 268
Troubleshooting alert and trap problems ......................................................................... 268
- Inability to receive Insight Manager 7 or Systems Insight Manager alarms (SNMP traps)
  from iLO .................................................................................................................... 269
- iLO Security Override switch ...................................................................................... 269
- Authentication code error message .............................................................................. 270
Troubleshooting directory problems ................................................................................ 270
- I can not log in using domain/name format but I can using the full distinguished name
  ................................................................................................................................ 270
- ActiveX controls are enabled and I see a prompt but the domain/name login format
does not work ................................................................................................................. 270
- User contexts do not appear to work .............................................................................. 271
Troubleshooting mouse problems .................................................................................... 271
- Local USB mouse and Linux ........................................................................................ 271
- Mouse issue using SuSE Linux ..................................................................................... 272
- Remote Console mouse control issue .......................................................................... 272
- Emulating a PS/2 keyboard in a headless server environment ....................................... 273
Troubleshooting Remote Console problems ..................................................................... 273
- Linux Remote Console ............................................................................................... 274
- Remote Console applet has a red X when running Linux client browser ......................... 274
- Inability to navigate the single cursor of the Remote Console to corners of the Remote
  Console window ............................................................................................................ 274
- Remote Console no longer opens on the existing browser session ................................. 275
- Remote console text window not updating properly ...................................................... 276
- Remote Console turns gray or black .............................................................................. 276
Troubleshooting SSH and Telnet problems ..................................................................... 276
- Initial PuTTY input slow ............................................................................................... 276
- PuTTY client unresponsive with Shared Network Port .................................................. 277
- SSH text support from a Remote Console session ....................................................... 277
Troubleshooting terminal services problems .................................................................... 277
- Terminal Services button is not working ...................................................................... 277
- Terminal Services proxy stops responding ................................................................... 278
Troubleshooting video and monitor problems ................................................................. 278
- General guidelines ....................................................................................................... 278
- Telnet displays incorrectly in DOS® ............................................................................ 278
- Video applications not displaying in the Remote Console .............................................. 279
Troubleshooting Virtual Media problems ......................................................................... 279
- Virtual drive listing ....................................................................................................... 279
- Virtual Media applet has a red X and will not display ..................................................... 279
- Virtual Floppy media applet is unresponsive ................................................................. 279
Operational overview

In this section

Guide overview ................................................................................................................. 11
New in this version ............................................................................................................ 11
Removed in this version ............................................................................................................... 12
Usage model ................................................................................................................................. 12
Network connection overview .................................................................................................... 13
Supported server operating system software ................................................................................ 14
Supported browsers and client operating systems ........................................................................ 15

Guide overview

The HP iLO management processor provides multiple ways to configure, update, operate, and manage servers remotely. The HP Integrated Lights-Out 1.80 User Guide describes each feature and how to use the feature with the web-based interface and ROM-Based Setup Utility. The HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide and addendum describe in detail the syntax and tools available to use iLO through a command line or scripted interface.

New in this version

New features in iLO 1.80 include:

- Schema-free directories ("Setup for Schema-free directory integration" on page 154)
- Two-factor authentication ("Two-Factor Authentication Settings" on page 101)
- Power regulator reporting ("Power Regulator for ProLiant" on page 62)
- SSH key authorization ("SSH Key Administration" on page 100)
- Virtual USB key drive ("iLO Virtual Floppy/USBKey" on page 69)
- Shared network port virtual LAN ("Shared Network Port VLAN" on page 131)
- Remote Console Acquire ("Acquiring the Remote Console" on page 58)

### Removed in this version

iLO 1.80 no longer supports:

- Netscape browser on Linux clients
- Shipping of Softpaq of binary image (The binary image has been replaced by online flash components.)

### 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.

Another way to access iLO functionality is through the scripting interface. The 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 also supports operations such as power on control.

Additionally, iLO functionality that can be accessed from the SMASH CLP is a low bandwidth interface that provides similar functionality as the Web interface. The CLP is designed for users who prefer a non-graphical interface over a telnet or SSH connection.

**NOTE:** iLO supports a preliminary draft version of the new SMASH CLP under development by the DMTF.

HP recognizes that customer usage models vary. iLO supports various interfaces for configuration and operation. This guide details the following interfaces:
• iLO RBSU (on page 18)
• A browser-based web interface

Refer to the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide* for the details on using the following interfaces:

• CPQLOCFG is a Microsoft® Windows® utility that sends RIBCL scripts to iLO over the network.
• CPQLODOS is a DOS deployment utility (part of the HP SmartStart Scripting Toolkit) that runs on the host during SmartStart or RDP deployment.
• Perl 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 require the HP iLO Management Interface Driver.
• The SMASH CLP is accessible through the following access methods: telnet, SSH, virtual serial port, or physical serial port.

Graphical Remote Console (on page 47), Virtual Media (on page 65), the Terminal Services Pass-Through option (on page 119), and Directory Services (on page 151) are advanced functions that must be enabled by licensing the optional iLO Advanced Pack.

**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 corporate 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, HP Insight Manager 7, and HP 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 iLO.

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

- Microsoft®
  - Windows NT® 4.0 Server
  - Windows NT® 4.0, Enterprise Edition
  - Windows® 2000 Server
  - Windows® 2000 Advanced Server
  - Windows® Server 2003
  - Windows® Server 2003, Enterprise Edition (EM64T)
  - Windows® Small Business Server 2003
- Red Hat
  - Red Hat Enterprise Linux 3
  - Red Hat Enterprise Linux 4
  - Red Hat Enterprise Linux 2.1 AS
- SUSE
  - SUSE LINUX Enterprise Server 8
  - SUSE LINUX Enterprise Server 9 (x86 and AMD64/EM64T)
- Novell
  - NetWare 6.5
  - NetWare 5.1

Supported browsers and client operating systems

- Microsoft® Internet Explorer 6 with Service Pack 1 or later
  - This browser is supported on Microsoft® Windows® 2000 Professional, Microsoft® Windows® XP Professional, and Microsoft® Windows® 2003.
If you are using single-cursor mode in Remote Console or virtual media, Java™ JVM is required. HP supports Java™ 1.4.2 and Java™ 1.3.1. To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvm).

- Firefox 1.0.2
  - This browser is supported on RedHat Enterprise Linux 3 Workstation and Novell Linux Desktop 9.
  - If you are using Remote Console or virtual media, Java™ 1.4.2 is required. To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvm).

- Mozilla 1.7.3
  - This browser is supported on RedHat Enterprise Linux 3 Workstation and Novell Linux Desktop 9.
  - If you are using Remote Console or virtual media, Java™ 1.4.2 is required. To download the recommended JVM for your system configuration, refer to the HP website (http://www.hp.com/servers/manage/jvm).

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

**Linux browser configuration**

The font configuration of the desktop and browser can affect the placement of tab menus within the iLO user interface. A fixed font of 12 points is required for proper placement.

To change the font size in Mozilla, open the Preferences menu and set minimum font size to 12 on the Appearance, Fonts screen.
Configuring iLO

In this section

iLO configuration options ......................................................................................................................... 17
Installing iLO device drivers ....................................................................................................................... 20
Enabling iLO Advanced functionality ....................................................................................................... 23
ProLiant BL p-Class configuration ............................................................................................................ 26
Integration with RILOE II accessory boards ............................................................................................ 37

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 14) drivers be installed.

iLO offers several configuration options:

- iLO RBSU (on page 18)
- Browser-based setup (on page 19)
- Remote scripted setup using CPQLOCFG
- Local scripted deployment using CPQLODOS
- Local on-line scripted setup using HPONCFG
iLO RBSU

HP recommends iLO RBSU to initially set up iLO and 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 on the network.

iLO RBSU is designed to assist you with setting up iLO on a network. iLO RBSU 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.
Installing iLO device drivers

The SmartStart Firmware 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 the Terminal Services Pass-Through service to communicate with iLO.


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.

Configuring Linux font size

To change the font size:

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

Installing or updating iLO Linux and SUSE drivers

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

- rpm -e cmanic
- rpm -e hprssm
- rpm -e hpasm

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

rpm -ivh hpasm-d.vv.v-pp.Linux_version.i386.rpm
Configuring iLO

```
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 47)
- Power regulation ("Power Regulator for ProLiant" on page 62)
- Virtual media (on page 65) (including Virtual Floppy and Virtual CD)
- Directory-based authentication and authorization ("Directory-enabled remote management" on page 201)
- Terminal Services Pass-Through option (on page 119)

Advanced functionality is enabled by licensing the optional iLO Advanced Pack. The iLO Advanced Pack contains an activation key that you must enter in iLO to enable advanced functionality. The advanced features can be evaluated using an evaluation key. For more information, refer to the “iLO Advanced evaluation license (on page 24)” section.
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.

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.

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.

5. Click **OK**.

The advanced features of iLO are now enabled.
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
- "Browser-based setup (on page 19)" which initially configures the system through the iLO Diagnostic Port
- Step-by-step installation wizard through HP BladeSystem Setup

On select p-Class blades in enclosures with updated management backplanes that support 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.

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.

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 to the iLO in each blade server 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.
Configuring iLO 27

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

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).

Enabling iLO IP address assignment

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

HP BladeSystem setup

The HP BladeSystem setup wizard provides step-by-step instructions to simplify single blade setup without requiring DHCP or PXE. The HP BladeSystem Setup page launches after you authenticate to iLO from the front port.

The server blade must be properly cabled for iLO connectivity. Connect to the server blade through the server blade I/O port, while the blade is 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 through iLO through its standard Web browser interface.

Although any blade can be used for access, if static IP bay configuration will be used to configure iLO network settings, then the first blade in the enclosure should be used for access.

The first page of the wizard automatically launches if:

- This blade is new from the factory, and you have logged into iLO from the front port.
- You did not fully complete the wizard by selecting Finish on the final page, and you did not select Do not show setup wizard again and clicked Cancel on the beginning page.
• You have cleared the iLO NVRAM or set iLO back to factory default settings.

Click **Cancel** to close the automated setup wizard. Click **Next** to set up your blade server. The setup wizard will guide you through:

1. iLO configuration
2. Server RAID verification
3. Virtual media connection
4. Software installation

**iLO configuration screen**

This screen enables you to:

• Change the administrator password. HP recommends changing the default password.

• Change network configuration settings. The default settings are:
  
  – Enable DHCP—Yes
– Enable Static IP Bay Configuration—No

• If connected to the blade in enclosure slot 1, you can enable Static IP Bay configuration to preconfigure the static address for other iLO processors in the enclosure.

In the default configuration, the iLO being updated gets its IP address through DHCP. Other iLO processors in the enclosure must be configured separately. If these settings are not changed, clicking Next displays the next page in the setup wizard. If either of these settings are changed, iLO reboots to invoke the updated settings.

The other configuration combinations are:

• Enable DHCP—Yes and Enable Static IP Bay Configuration—Yes
   This configuration causes the iLO being configured to get its IP address through DHCP. Clicking Next displays the Static IP Bay Configuration page, enabling you to specify the IP addresses for other iLOs in the enclosure. After you click Next, you are prompted to verify that you want to use DHCP for this iLO IP address.

• Enable DHCP—No and Enable Static IP Bay Configuration—Yes
   This configuration causes the iLO being configured to set its IP address according to the settings specified through the Static IP Bay Configuration. Clicking Next displays the Static IP Bay Configuration page.

• Enable DHCP—No and Enable Static IP Bay Configuration—No
   This configuration causes the iLO being configured to set its IP address according to the settings specified through the Network Settings page. Clicking Next displays the Network Settings page.

To save any network changes, you must have the configure iLO privilege.
Click **Next** to save changes and continue.

### Verify Server RAID Configuration screen

This step of the installation wizard enables you to verify and accept server RAID configuration settings.

- **Verify the detected RAID level** for the hard drives on the blade server displayed on the web page.
- **Click Next** to keep current RAID settings.
- **Click Default Settings** to automatically configure the RAID level based on the number of installed drives. You are prompted to verify that you want to reset the RAID level because this could result in loss of data. Resetting the RAID level requires a server power-on or reboot. iLO displays a page indicating that this action is occurring. The page is refreshed automatically every 10 seconds. After the server reboots, the next page in the installation wizard displays again. If an error occurs during the RAID reset process, the RAID Configuration page will redisplay with an indication of the error. An error is most likely to occur if the server is in POST. If this is the case, exit any RBSU program you are running, allow POST to complete, and try the operation again.
- The RAID level can be changed manually through RBSU.

If the operating system is already installed, changing the RAID level results in a loss of data.

**Connect Virtual Media screen**

This step of the installation wizard enables you to verify and accept the drive you will use during the installation of the operating system. Under Settings, select the local drive and media type you intend to use during operating system installation. Click **Launch Virtual Media** to launch the Virtual Media applet.

- Ensure the operating system media is connected. In the Virtual Media applet, a green icon appears next to the media currently selected.
- Verify that the operating system media is in the appropriate local drive.
- Accept security certificates as they appear.
After making your selection, click **Next** to save your settings and continue. The Virtual Media applet appears. After the applet is available, you can change the selected drive, or choose other options not available on the installation wizard page.

**Install Software screen**

This step of the installation wizard enables you to launch the Remote Console and install the operating system. To start the operating system installation process:

- Click **Launch Software Installation** to launch the Remote Console. iLO automatically initiates a server power-on or reboot to start the operating system installation through the previously selected virtual media.
- Accept security certificates as they appear.
Click **Finish** to complete the setup process.

**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 18). Select **Settings>Enabled** for the Enable Lights-Out functionality setting.
Using iLO

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.

The default values are:

- **User name**—Administrator
- **Password**—A random, eight-character, alphanumeric string
- **DNS Name**—*iLOXXXXXXXXXXXX*, where the Xs represent the serial number of the server

**NOTE:** User names and passwords are case sensitive.
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 146)."

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

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. The Event Log also contains a record of 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.

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.

To clear the <LOM_short_name>:

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.

**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 44)
- NVRAM environment variables listing (on page 45)
- Virtual NMI button (on page 45)
- iLO self-test results (on page 46)

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.

<table>
<thead>
<tr>
<th>Code</th>
<th>Start of phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>FE04</td>
<td>EISA Initialization</td>
</tr>
<tr>
<td>FE08</td>
<td>PCI Initialization</td>
</tr>
<tr>
<td>FE0C</td>
<td>Processor Initialization</td>
</tr>
<tr>
<td>FE10</td>
<td>Video Initialization</td>
</tr>
<tr>
<td>Code</td>
<td>Start of phase</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>FE14</td>
<td>Cache Initialization</td>
</tr>
<tr>
<td>FE18</td>
<td>USB Initialization</td>
</tr>
<tr>
<td>FE1C</td>
<td>Memory Test</td>
</tr>
<tr>
<td>FE20</td>
<td>Memory Initialization</td>
</tr>
<tr>
<td>FE24</td>
<td>USB Startup</td>
</tr>
<tr>
<td>FE28</td>
<td>Floppy Controller Test</td>
</tr>
<tr>
<td>FE2C</td>
<td>Option ROM Initialization</td>
</tr>
<tr>
<td>FE30</td>
<td>ATAPI Option ROM Initialization</td>
</tr>
<tr>
<td>FE34</td>
<td>BBS Initialization</td>
</tr>
<tr>
<td>FE38</td>
<td>Begin BOOT Process</td>
</tr>
<tr>
<td>FE3C</td>
<td>Attempting SCSI CD Boot</td>
</tr>
<tr>
<td>FE40</td>
<td>Attempting Floppy Boot</td>
</tr>
<tr>
<td>FE44</td>
<td>Attempting HD Boot</td>
</tr>
<tr>
<td>FE48</td>
<td>Attempting CD Boot</td>
</tr>
<tr>
<td>FE4C</td>
<td>Attempting PXE Boot</td>
</tr>
<tr>
<td>FE50</td>
<td>Passing control to boot sector code</td>
</tr>
<tr>
<td>FE54</td>
<td>No bootable devices</td>
</tr>
</tbody>
</table>

**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.
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 50)."

Remote Console Information option

The Remote Console Information option displays the Remote Console options available, as well as a link to download an updated Java™ Runtime Environment, which is necessary for using the Remote Console with the single-cursor option ("Single-cursor mode" on page 56).
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 appears indicating that it is in use by another user. If the Enable Remote Console Acquire setting on the Global Settings page is set to yes, an Acquire button is visible on the Remote Console page. Clicking **Acquire** will end the other user's Remote Console session and start a Remote Console session in your current window.

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 buttons that provide iLO with enhanced features. These options have the following functions:

- **Refresh**—Forces iLO to refresh the screen.
- **Terminal Svcs**—Launches the Microsoft® Terminal Services client installed on this system. This button deactivated out if Terminal Services is disabled or is not installed on the server.
- **Ctrl-Alt-Del**—Enters the key sequence Ctrl+Alt+Del in 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.
- **High Performance Mouse**—When selected, changes the mouse from PS2 emulation to USB HID, greatly improving mouse performance.
- **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.
- **Acquire**—Allows you to take control of a Remote Console session when in use by another user and starts a new Remote Console session in your current window. The Enable Remote Console Acquire setting on the Global Settings page must be set to Yes for this button to be visible.
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.
High performance mouse settings

When using the Remote Console, you have the option to enable the High Performance Mouse feature. High Performance Mouse greatly improves pointer performance and accuracy on Windows® Server 2003 and Windows® 2000 Service Pack 3 or later. The High Performance Mouse feature changes the mouse emulation from a conventional PS/2 mouse to a USB HID mouse. The HID mouse reports updates in an absolute coordinate system instead of a relative coordinate system (like a PS/2 mouse) and eliminates mouse synchronization problems.

The High Performance Mouse feature currently only works in Windows® operating systems. Because it uses USB, this feature can potentially interfere with virtual media. High Performance Mouse can not be enabled or disabled while virtual media is connected. The host server should be running Windows® 2000 Service Pack 3 or later or Windows® 2003.

NOTE: When using remote console during a SmartStart assisted operating system installation, disable High Performance Mouse support.

For best performance, configure the host server to use the hardware mouse cursor. Adjust the following settings in Control Panel:

1. Select Mouse>Pointers>Scheme>Windows® Default scheme. Click OK.
2. Deselect Mouse>Pointers>Enable pointer shadow. Click OK.
3. Set Display>Settings>Advanced>Troubleshoot>Hardware Acceleration>Full. Click OK.

Alternatively, the HP online configuration (HPONCFG) utility can automatically adjust these settings. You can also edit High Performance Mouse settings using the XML command MOD_GLOBAL_SETTINGS. For more information on using RIBCL, refer to the "MOD_GLOBAL_SETTINGS" section of the HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Addendum.
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 54)."

The following table lists keys available to combine in a Remote Console hot key sequence.
<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESC</td>
<td>F12</td>
</tr>
<tr>
<td>L_ALT</td>
<td>&quot; &quot; (Space)</td>
</tr>
<tr>
<td>R_ALT</td>
<td>!</td>
</tr>
<tr>
<td>L_SHIFT</td>
<td>#</td>
</tr>
<tr>
<td>R_SHIFT</td>
<td>$</td>
</tr>
<tr>
<td>INS</td>
<td>%</td>
</tr>
<tr>
<td>DEL</td>
<td>&amp;</td>
</tr>
<tr>
<td>HOME</td>
<td>~</td>
</tr>
<tr>
<td>END</td>
<td>(</td>
</tr>
<tr>
<td>PG UP</td>
<td>)</td>
</tr>
<tr>
<td>PG DN</td>
<td>*</td>
</tr>
<tr>
<td>ENTER</td>
<td>+</td>
</tr>
<tr>
<td>TAB</td>
<td>-</td>
</tr>
<tr>
<td>BREAK</td>
<td>.</td>
</tr>
<tr>
<td>F1</td>
<td>/</td>
</tr>
<tr>
<td>F2</td>
<td>0</td>
</tr>
<tr>
<td>F3</td>
<td>1</td>
</tr>
<tr>
<td>F4</td>
<td>2</td>
</tr>
<tr>
<td>F5</td>
<td>3</td>
</tr>
<tr>
<td>F6</td>
<td>4</td>
</tr>
<tr>
<td>F7</td>
<td>5</td>
</tr>
<tr>
<td>F8</td>
<td>6</td>
</tr>
<tr>
<td>F9</td>
<td>7</td>
</tr>
<tr>
<td>F10</td>
<td>8</td>
</tr>
<tr>
<td>F11</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

Single-cursor mode

Single-cursor mode 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_02 JVM 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 Java website (http://java.sun.com). 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 website (http://java.sun.com) or on the SmartStart CD.

Dual-cursor mode

All the features discussed in the "Remote Console (on page 47)" section are available when using dual-cursor mode. 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 tracks 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, configure the host operating system display as described in "Optimizing performance for graphical Remote Console (on page 50)."
The dual-cursor option is your only Remote Console for Microsoft® Windows clients 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 cross-hair cursor to align with the mouse cursor of the remote server.

2. Press and hold the Ctrl key, and move the local cross-hair 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.
Acquiring the Remote Console

When the Enable Remote Console Acquire setting on the Global Settings page is set to Yes, the Remote Console page displays the Acquire button. If you have opened the Remote Console page and are notified that another user is currently using Remote Console, clicking the Acquire button ends the other user's Remote Console session and starts a Remote Console session in your current window.

When you click Acquire, you are prompted to verify that you want to interrupt the other user's Remote Console session. The other user receives a notification that another user has acquired the Remote Console session after losing the connection. No prior warning is given. After you confirm you want to proceed with the acquire operation, you will be notified by an alert window that the operation could take 30 seconds or longer to complete. Do not click the Acquire button again during this time.
Only one acquire command is allowed every five minutes for all users. If another user has recently acquired the Remote Console, clicking the Acquire button can result in a page informing you that the five minute acquire disabled period is in effect. Close the window and re-launch Remote Console to try again. The Acquire button is disabled in the new page until the acquire disable period expires. When the Acquire button is enabled (this happens automatically; you do not have to refresh the page), you can attempt to acquire the Remote Console session again.

Only one acquire attempt may be made per Remote Console session window. If you have successfully acquired the Remote Console, and someone subsequently acquires it from you, you must open a new Remote Console window to attempt to acquire the Remote Console session again.

**Virtual devices**

Within the Virtual Devices tab are the following options:

- Virtual power (on page 60)
- Power regulator for ProLiant (on page 62)
- Virtual media (on page 65)
- Virtual indicators (on page 82)
- Virtual serial port (on page 83)
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.

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 action immediately removes 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.

• **Manual Override for BL p-Class**—This option appears 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.

• **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.
Power Regulator for ProLiant

The Power Regulator for ProLiant page is enabled by licensing the optional iLO Advanced Pack. If it is not licensed, the message *iLO feature not licensed* displays.

The Power Regulator for ProLiant page enables dynamically modifying the processors' frequency and voltage levels based on operating conditions to provide power savings with minimal effect on the performance. Processors that support this feature have predefined voltage and frequency states known as p-states. The software can dynamically switch the processor from one p-state to another. P-0 is the highest frequency/voltage combination supported by the processor. Modifying the processor p-state based on CPU utilization enables significant power savings with minimal performance degradation by reducing the voltage and frequency on the processor when the system is idle and vice versa. To allow the processor to dynamically set the power level based on usage, select **Enable HP Dynamic Power Savings Mode**. To set the processor to minimum power, select **Enable HP Static Low Power Mode**. To set the processor to maximum power, select **Disable**.

**NOTE:** The system processor determines if the Power Regulator option is supported. The Power Regulator option is only supported on the following servers:
- ProLiant ML350 G4
- ProLiant ML350 G4p
- ProLiant ML320 G3
- ProLiant DL360 G4
- ProLiant DL360 G4p
- ProLiant DL380 G4
- ProLiant DL380 G4p
- ProLiant DL20p G3
- ProLiant ML570 G3
- ProLiant DL580 G3

The system ROM firmware revision date must be dated at least 6/1/05. If your system processor does not support the Power Regulator (different processor p-states), the Power Regulator page displays the HP Power Regulator for ProLiant not supported by iLO message.

The Power Regulator for ProLiant settings can only be invoked through iLO on servers that have host ROM power regulator support. Some servers might support modifying the processor power level through the system RBSU. Consult your system’s user guide for more information.
• **Enable HP Dynamic Power Savings Mode** sets the processor to dynamically set the power level based on usage.

• **Enable HP Static Low Power Mode** sets the processor to minimum power.

• **Disabled** sets the processor to maximum power.

Click **Apply** to save the desired setting. A server reboot is required to invoke the new setting. If the server does not support the feature the message **HP Power Regulator for ProLiant not supported by iLO on this server** is displayed across the page.

Click **View Data** to navigate to the Power Regulator Data page to view the current p-state and a running average of the percentage of time each processor has spent in each p-state. The View Data page requires iLO Advanced. Refer to the Licensing page for information on acquiring an iLO Advanced Pack license.
P-state data for each logical processor in the host system is collected by iLO when the host system is powered on and is not in POST. The current P-state and a rolling average of p-state data collected over the last 12 hours is displayed. A multi-colored bar exhibits the percentage of time each logical processor has spent in each p-state. The data is reset when iLO reboots.

**Virtual media**

Virtual media is enabled by licensing the optional iLO Advanced Pack. If not licensed, the message *iLO feature not licensed* appears.

The iLO Virtual Media option provides you with a Virtual Floppy disk drive, USB key drive, and a Virtual DVD/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. 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 66).
If the Virtual Floppy/USBKey capability is enabled, the floppy and USB key 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, you can access the Virtual Floppy and USB key drive from the client operating system while it is connected. However, it is important that access to the Virtual Floppy or USB key drive from the client operating system not be attempted while it is connected as a virtual media device. Doing so could cause data loss on the floppy drive. Always disconnect virtual media before trying to access it from the client operating system.

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, USB key drive, or a 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.

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.

<table>
<thead>
<tr>
<th>Operating system install using Virtual USB floppy¹</th>
<th>Operating system run time using Virtual USB floppy²</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-DOS</td>
<td>No</td>
</tr>
<tr>
<td>NetWare 5.x or 6</td>
<td>No</td>
</tr>
<tr>
<td>NetWare 6.5</td>
<td>Yes</td>
</tr>
<tr>
<td>UnitedLinux 1.0</td>
<td>Yes³</td>
</tr>
</tbody>
</table>

¹Virtual Floppy or USB key drive can be installed.
²Virtual Floppy or USB key drive can be accessed at runtime.
³iLO Virtual CD-ROM is also supported.
<table>
<thead>
<tr>
<th>Operating system install using Virtual USB floppy</th>
<th>Operating system run time using Virtual USB floppy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux AS 2.1</td>
<td>Yes³</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows NT® 4.0</td>
<td>No</td>
</tr>
<tr>
<td>Windows® 2000 SP3 or later</td>
<td>Yes²</td>
</tr>
<tr>
<td>Windows® Server 2003</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating system install using Virtual USB CD</th>
<th>Operating system run time using Virtual USB CD²</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-DOS</td>
<td>No</td>
</tr>
<tr>
<td>NetWare 5.x or 6</td>
<td>No</td>
</tr>
<tr>
<td>NetWare 6.5</td>
<td>No</td>
</tr>
<tr>
<td>UnitedLinux 1.0</td>
<td>Yes</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux AS to 2.1</td>
<td>Yes</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3</td>
<td>Yes¹</td>
</tr>
<tr>
<td>Windows NT® 4.0</td>
<td>No</td>
</tr>
<tr>
<td>Windows® 2000 SP3 or later</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows® Server 2003</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating system install using Virtual USB Key</th>
<th>Operating system run time using Virtual USB Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-DOS</td>
<td>No</td>
</tr>
<tr>
<td>NetWare 5.x or 6</td>
<td>No</td>
</tr>
<tr>
<td>Operating system install using Virtual USB Key</td>
<td>Operating system run time using Virtual USB Key</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>NetWare 6.5</td>
<td>Yes</td>
</tr>
<tr>
<td>UnitedLinux 1.0</td>
<td>Yes³</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux AS 2.1</td>
<td>Yes³</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 3</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows NT® 4.0</td>
<td>No</td>
</tr>
<tr>
<td>Windows® 2000 SP3 or later</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows® Server 2003</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

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

**NOTE:** You must manually load the USB driver.

**NOTE:** Not available on a BL20p G1.

**NOTE:** Only with an integrated operating system CD.

**NOTE:** Only available on servers with ProLiant USB key drive support.

**Using iLO Virtual Media devices**

You can access virtual media on a host server from a client through a graphical interface using a Java™ applet and through a script interface using an XML engine.

To access iLO Virtual Media devices using the graphical interface, select **Virtual Media** on the Virtual Devices tab. An applet loads in support of the Virtual Floppy/USBKey or Virtual CD-ROM device.
iLO Virtual Floppy/USBKey

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

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

To use a physical floppy or USB key drive in your client PC:

1. Select **Local Media Drive**.
2. Select the drive letter of the desired local floppy or USB key drive on your client PC from the dropdown menu. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.
3. Click **Connect**.
The connected drive icon and LED will change state to reflect the current status of the Virtual Floppy Drive.

To use an image file:

1. Select **Local Image File** within the Virtual Floppy/USBKey section of the Virtual Media applet.

2. Enter the path or file name of the image in the text-box, or click **Browse** to locate the image file using the Choose Disk Image File dialog. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.

3. Click **Connect**.

The connected drive icon and LED will change state to reflect the current status of the Virtual Floppy or USB key drive. 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/USBKey, you can either select to disconnect the device from the host server or close the applet.

![Virtual Media](image.png)

**NOTE:** The Virtual Media applet must remain open in your browser as long as you continue to use a Virtual Media Device.
iLO Virtual Floppy/USBKey is available to the host server at run time if the operating system on the host server supports USB floppy or key drives. Refer to "Operating System USB Support (on page 66)" for information on which operating systems support USB mass storage at the time of the publication of this manual.

iLO Virtual Floppy/USBKey appears to your operating system just like any other drive. When using iLO for the first time, the host operating system might 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 Floppy/USBKey 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 drive 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 SP3 or later and Windows® Server 2003**
  Virtual Floppy and USB key drives display automatically after Microsoft® Windows® has recognized the mounting of the USB device. Use it as you would a locally attached device.

  To use Virtual Floppy during a Windows® installation to provide a driver diskette, disable the integrated diskette drive in the host RBSU which forces the Virtual Floppy to appear as drive A.

  To use Virtual USBKey during a Windows® installation to provide a driver diskette, change the boot order of the USB key drive in the system RBSU. HP recommends placing the USB key drive first in the boot order.

- **NetWare 6.5**
NetWare 6.5 supports the use of USB diskette and key drives. Refer to "Mounting USB Virtual Floppy/USBKey in NetWare 6.5 (on page 72)" for step-by-step instructions.

- Red Hat and SLES Linux
  
  Linux supports the use of USB diskette and key drives. Refer to the "Mounting USB Virtual Floppy/USBKey in Linux ("Mounting USB Virtual Media/USBKey in Linux" on page 72)" section for step-by-step instructions.

**Mounting USB Virtual Floppy/USBKey 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 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/USBKey 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.
   a. For a floppy drive or image, select a Local Media Drive or Local Image File and click **Connect**.
b. For a USB key drive or image, select a Local Image File and click **Connect**.

For a physical USB key drive, enter `/dev/sda` in the Local Image File text box.

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 drive.
   - To mount the diskette drive, use the following command:
     ```
     mount /dev/sda /mnt/floppy -t vfat
     ```
   - To mount the USB key drive, use the following command:
     ```
     mount /dev/sdal /mnt/keydrive
     ```

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

The floppy and key drive 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
   ```

To enable the various `mtools` commands to access the Virtual USBKey device, modify the existing `/etc/mtools.conf` file and add the following line:

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

To list the Virtual USBKey device partition table to find the desired partition, use the following command:

   ```
   fdisk -l /dev/sda
   ```
This modification enables the mtools suite to access the Virtual Floppy as v. For example:

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

### Changing diskettes

When using the iLO Virtual Floppy or USB key drive, and the physical diskette drive on the client machine is a USB diskette 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/USBKey, be sure the client machine contains a non-USB diskette 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 66)" 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 you 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 using 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**.

To use an image file:

1. Select **Local Image File** within the Virtual CD-ROM section of the Virtual Media applet.

2. Enter the path or file name of the image in the text-box or click **Browse** to locate the image file using the Choose Disk Image File dialog.

3. Click **Connect**.

The connected drive icon and LED will change state to reflect the current status of the Virtual CD-ROM. 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 66)" 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 SP3 or later 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 turns green, but the additional CD-ROM drive does 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 the "Mounting USB Virtual Media CD in NetWare 6.5 (on page 77)" section 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
    ```

  - **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, 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-ROM in Linux (on page 78)" 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 iLO disk image files

The iLO virtual media feature enables you to create diskette and CD-ROM image files within the same applet. Creation of DVD image files using the Virtual Media applet is not supported. The image files created from the applet are ISO-9660 file system images. The performance of iLO virtual media is faster when image files are used. The utility to create iLO Virtual Floppy and CD-ROM disk image files is integrated into the Virtual Media applet; however, images may also be created using industry standard tools such as DD.

NOTE: The iLO Create Image utility does not support USB devices in Linux or NetWare.

To create an image file:

1. Click **Create Disk Image**.
2. Select the local media drive from the dropdown menu.
3. Enter the path or file name in the text box or click **Browse** to select an existing image file or to change the directory in which the image file will be created.
4. Click **Create**. The virtual media applet begins the process of creating the image file. The process is complete when the progress bar reaches 100%. To cancel the creation of an image file, click **Cancel**.
The Disk>>Image option is used to create image files from physical diskettes or CD-ROMs. The Image>>Disk option is not valid for a Virtual CD-ROM image. The Disk>>Image button 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.

**Virtual Media multi-device support**

Virtual media multi-device support allows both the Virtual Media Floppy/USBKey drive and the CD-ROM device to be connected to the host simultaneously. The drive selected can be a physical drive, or an image file, or any combination of the two devices.

Virtual media multi-device mode and multiple USB devices are only supported on Microsoft® Windows® 2000 with Service Pack 3 and Windows® 2003. Virtual media multi-device mode is not supported on Linux. Some servers might require a system ROM update for this mode of operation.

**IMPORTANT:** When using the SmartStart CD-ROM, use single mode configuration. Do not use multi-device support.
To enable a multi-device connection, select the **Enable Virtual Media multi-device connection** checkbox. A multi-device connection only functions properly on server operating systems that support composite USB devices. For each session, an initial notice message box appears.

To use a multi-device connection:

1. From the Virtual Floppy/USBKey section, select **Local Floppy Drive** and select the drive letter of the desired physical floppy or USB key 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.

2. 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.
3. From the virtual CD-ROM section, select **Local CD-ROM Drive** and select the drive letter of the desired physical CD-ROM drive on your client system from the dropdown menu, or 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, or click **Browse** to locate image files.

4. 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 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.

**Virtual Serial Port and serial BREAK**

iLO Virtual Serial Port supports serial BREAK. The serial BREAK event can be transmitted to the host system through the Virtual Serial Port by pressing the **Esc Ctrl-B** key sequence. This key sequence allows the Virtual Serial Port applet, telnet, and SSH applications that operate over TCP/IP networks to transmit the serial BREAK event to the host when using Virtual Serial Port.

iLO serial BREAK supports the Linux operating system feature of Magic SysRq. The Linux kernel supports the Magic SysRq feature on a console on tty0 through the Alt-SysRq key combination. When the kernel supports a console on a serial connection, ttyS0 or other, the BREAK event is used to implement Magic SysRq.

When Magic SysRq is correctly configured:

- The console is defined on serial tty (ttyS0 or other) in LILO or GRUB
- The appropriate kernel is configured with /proc/sys/kernel/sysrq
- The appropriate agetty (or equivalent) is configured for serial tty (ttyS0 or other)

The Esc Ctrl-B sequence will generate a serial BREAK event, which causes the Magic SysRq event. An additional magic SysRq key after the Esc Ctrl-B sequence is used to select a specific command. Refer to your Linux documentation for details and security implications of enabling Magic SysRq.
Linux End-to-End support

The Virtual Serial Port, by default, uses the I/O address 0x0408 and INTERRUPT 4 for communication. The Virtual Serial Port is configured and enabled when iLO 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 I/O address is not a standard supported I/O address. The `setserial` command can be used to configure `agetty`, but the kernel requires rebuilding to support GRUB for booting redirection and kernel redirection. Full configurability to standard UART I/O 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 GRUB 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 appears.

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.

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**.
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.

To modify user certificate information, refer to the "Two-factor authentication user certificates (on page 143)" section.

### 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 time-out 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)
- Enable Lights-Out Functionality
- Pass-Through Configuration
- Enable iLO ROM-Based Setup Utility
- Require Login for iLO RBSU
- Show iLO during POST
• Remote Console Port Configuration
• Remote Console Data Encryption
• Enable Remote Console Acquire
• SSL Encryption Strength
• Current Cipher
• Web Server Non-SSL Port
• Web Server SSL Port
• Virtual Media Port
• Remote Console Port
• Terminal Services Port
• Secure Shell (SSH) Port
• Secure Shell (SSH) Status
• Serial Command Line Interface Status
• Serial Command Line Interface Speed (bits/second)
• Minimum Password Length
• Remote Keyboard Model

For more information refer to the HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide.

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 Settings privilege 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 changes, click Apply to complete the changes.

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

For more information refer to the HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide.
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**

- **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.


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 Windows® 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, the addresses used are the same as the IP address of the Insight Manager 7 or Systems Insight Manager server console.

**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.

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
- Enable p-Class Alert Fowarding (displayed on p-Class servers only)

For more information refer to the *HP Integrated Lights-Out 1.70 Scripting and Applications Guide*.

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.

![Image of SNMP/Insight Manager Settings](image-url)

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) 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.

**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 151)." For additional information on directory configuration parameters, refer to "Configuring Directory Settings (on page 197)."

**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.

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 284)" 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 284) 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 23)" 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 147)" in the "iLO security (on page 135)" section and the "IMPORT_CERTIFICATE" in the "Remote Insight command language" section of the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*. 
SSH Key Administration

This page displays the owner of each authorized SSH key. Any key can be selected and viewed in detail or deleted by clicking View Selected Key or Delete Selected Key. Up to four keys may be authorized. Multiple keys can belong to one user.

To authorize a new key:

1. Click Browse and locate the key file.
   
   The public key file path must be submitted to iLO. The key file should contain the user name after the end of the key. iLO will associate each key with a local user account. If the local account does not exist or if it is deleted, the key will be invalid (the key will not be listed here if the local account does not exist.) Alternatively, you can authorize SSH keys for an HP SIM server by running the mxagentconfig tool from the HP SIM server, specifying the address and user credentials for iLO. Refer to HP SIM documentation for more details.

2. Click Authorize Key.
Two-Factor Authentication Settings

This page displays the configuration of two-factor authentication settings and the trusted CA certificate information. It also provides a method of changing the configuration and importing or deleting a trusted CA certificate.
The Enforce Two-Factor Authentication setting controls whether two-factor authentication will be used for user authentication during login. Selecting Yes for this setting will require two-factor authentication. The No value will disable this feature and allow login with user name and password only. iLO will not allow this setting to be changed to Yes if a trusted CA certificate has not been configured. Changing this setting causes iLO to reset for the change to take effect. To provide the necessary security, the following configuration changes will also be made when two-factor authentication is enabled:

- Remote Console Data Encryption: Yes (Disables telnet access)
- Enable Secure Shell (SSH) Access: No
- Serial Command Line Interface Status: Disabled

If telnet, SSH, or Serial CLI access is required, re-enable these settings after two-factor authentication is enabled. However, because these access methods do not provide a means of two-factor authentication, only a single factor is required to access iLO with telnet, SSH or Serial CLI.

When two-factor authentication is enabled, access with the CPQLOCFG utility is disabled, because CPQLOCFG does not supply all authentication requirements. However, the HPONCFG utility is functional, because administrator privileges on the host system are required to execute this utility.

The Check for Certificate Revocation setting controls whether iLO uses the certificate CRL distribution points attribute to download the latest CRL and check for revocation of the client certificate. If the client certificate is contained in the CRL or if the CRL cannot be downloaded for any reason, access is denied. The CRL distribution point must be available and accessible to iLO when Check Certificate Revocation is set to Yes.

The Certificate Owner Field setting specifies which attribute of the client certificate to use when authenticating with the directory. If SAN is specified, iLO will extract the User Principle Name from the Subject Alternative Name attribute and the use User Principle Name when authenticating with the directory, for example, username@domain.extension. If Subject is specified, iLO will derive the user's distinguished name from the subject name attribute. For example, if the subject name is /DC=com/DC=domain/OU=organization/CN=user, iLO will derive:

```
CN=user,OU=organization,DC=domain,DC=com.
```
The Certificate Owner Field setting is only used if directory authentication is enabled. Configuration of this setting depends on the version of directory support being used, the directory configuration, and the certificate issuing policy of your organization.

A trusted CA certificate is required for two-factor authentication to function. iLO will not allow the Enforce Two-Factor Authentication setting to be set to Yes if a trusted CA certificate has not been configured. Also, a client certificate must be mapped to a local user account if local user accounts are being used. If the iLO is using directory authentication, client certificate mapping to local user accounts is optional.

To change two-factor authentication settings for iLO:

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

**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.

**Rack View**

The Rack View page presents an overview of all the enclosures and their contained blade servers, network components, and power supplies. A component, when present, is indicated by the ability to select the component from the Rack View. Blank or empty bays are not selectable. Component-specific information, such as blade name, IP address, and product type is displayed as you move the mouse cursor over each component. Clicking the component will display additional information and configuration options in the adjacent screen.

The following fields are available on the Rack View screen:
- Rack name
- Logged-in iLO Location
  This section annotates the blade into which the current user is logged in. The
  user is able to configure blade settings for this blade only.
- Selected Bay Location
  This section annotates the currently selected bay. You can view information
  for many different types of components, including blades, power supplies,
  network components, and enclosures.
- Enclosure Details
  Information about a particular enclosure is viewed by selecting Details
  located on the enumerated enclosure headers.

A Refresh button is available to obtain current Rack View information. Click
Refresh to force the entire graphical representation of the rack to be redrawn.
This will take a few moments.

If the rack view information cannot be properly obtained, an error message will
display in place of the rendered components. The Refresh button can be used to
make another attempt to obtain the proper rack view data. Rack View
functionality requires version 2.10 or later of the Server Blade and Power
Management Module firmware to display correctly.
Blade configuration and information

The blade configuration option provides information regarding the identity, location, and network address of the blade selected on the Rack View page. To view these settings, select a blade component and select Configure on the Rack View (on page 105) page. You can change some of the settings for the blade in which you are currently logged in. To save changes, click Apply.

The following fields are available:

- Identification Information
  - Bay Name
  - Bay Number
- Power On Control
- Power Source
- Enable Automatic Power On
- Enable Rack Alert Logging (IML)

Enclosure information

Enclosure information is specific to the selected enclosure. Information about a particular enclosure is viewed by selecting Details located on the enumerated enclosure headers. A limited amount of rack information is available, including:

- Rack Name
- Rack Serial Number

A basic set of information is available for the enclosures that do not contain the blade into which you are logged in. This information includes:
• Enclosure Name
• Enclosure Serial Number
• Enclosure Type

An advanced set of details is available for the enclosure that contains the bay into which you are logged in. These details include:

• Enclosure Name
• Enclosure Serial Number
• Enclosure Type
• Firmware Revision
• Hardware Revision
• Enclosure Temperature
• Management Module Unit ID

Certain fields can be changed and updated using the Apply button.
Power enclosure information

The Power Enclosure Information page provides diagnostic information regarding the power management module and the power components contained in the power enclosure. This information provides an overview on the health and condition of the power enclosure and the power components.

The following fields are available:

- Rack Name
- Rack Serial Number
- Enclosure Name
• Enclosure Serial Number
• Enclosure type
• Firmware revision
• Hardware revision
• Load balance Wire
• Enclosure Temperature
• Enclosure Temperature Side A and B
• Management Module UID

Certain fields can be changed and updated using the Apply button.
Power component information

Selecting a power component on the Rack View (on page 105) page displays general location, status, power output, and temperature metrics for the selected power component in the power enclosure.

The Status Information section provides the following information:

- Bay Number
- AC Input
- Power
- Firmware Revision

The Usage Statistics section displays the following fields:
• Current
• Maximum Current
• Power
• Maximum Power

The Temperature Information section contains temperature settings that represent current and threshold values for input and output temperatures. These fields include:

• Input
• Input Trip
• Input Fail
• Output
• Output Trip
• Output Fail
Network component information

Network component information displays the status of the patch panel or interconnect switch that has been selected.

The following information is available:

- Fuse A
- Fuse B
- Network Component Type

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.

ProLiant BL p-Class alert forwarding

iLO supports blade infrastructure SNMP traps on a pass-through basis. Reporting of blade infrastructure status by iLO does not require operating system support. The alerts (traps) originate from the Enclosure Manager and Power Supply Manager and are transmitted to iLO. iLO p-Class firmware forwards infrastructure alerts as SNMP traps to a correctly configured management console. These alerts allow the monitoring of p-Class alerts to take place in an SNMP management console.

p-Class alert forwarding is disabled by default and can be enabled from the SNMP/Insight Manage Settings web page.

The following alerts are identified and forwarded by iLO:

<table>
<thead>
<tr>
<th>Alert ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22005</td>
<td>Enclosure temperature failure</td>
</tr>
<tr>
<td>22006</td>
<td>Enclosure temperature degradation</td>
</tr>
<tr>
<td>22007</td>
<td>Enclosure temperature OK</td>
</tr>
<tr>
<td>22008</td>
<td>Enclosure fan failed</td>
</tr>
<tr>
<td>Alert ID</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>22009</td>
<td>Enclosure fan degraded</td>
</tr>
<tr>
<td>22010</td>
<td>Enclosure fan OK</td>
</tr>
<tr>
<td>22013</td>
<td>Rack power failure</td>
</tr>
<tr>
<td>22014</td>
<td>Rack power degraded</td>
</tr>
<tr>
<td>22015</td>
<td>Rack power supply OK</td>
</tr>
<tr>
<td>22023</td>
<td>Rack server failed; not enough power</td>
</tr>
</tbody>
</table>

**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 117)."

- 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 120)" 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 124)" section.

To configure the Terminal Services pass-through option, refer to "Terminal Services Client requirements (on page 119)" and "Terminal Services Pass Through installation ("Terminal Services Pass-Through installation" on page 121)."

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 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.

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 126)” 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 127)” 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.

<table>
<thead>
<tr>
<th>ProLiant server</th>
<th>Minimum iLO firmware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL320G3</td>
<td>1.64</td>
</tr>
<tr>
<td>DL360 G4</td>
<td>1.60</td>
</tr>
<tr>
<td>DL360 G4</td>
<td>1.64</td>
</tr>
<tr>
<td>DL380 G4</td>
<td>1.60</td>
</tr>
<tr>
<td>DL385 G1</td>
<td>1.64</td>
</tr>
</tbody>
</table>
Using iLO

<table>
<thead>
<tr>
<th>ProLiant server</th>
<th>Minimum iLO firmware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL580 G3</td>
<td>1.64</td>
</tr>
<tr>
<td>ML370 G4</td>
<td>1.60</td>
</tr>
<tr>
<td>ML570 G3</td>
<td>1.64</td>
</tr>
</tbody>
</table>

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.
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 130)" 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.

**Re-enabling the dedicated iLO management port**

The iLO RBSU or XML (described in the *HP Insight-Lights Out 1.70 Scripting and Command Line Reference Guide*) scripting must be used to re-enable the iLO dedicated NIC management port. 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.
**Shared Network Port VLAN**

The Shared Network Port VLAN feature is designed for customers who want to use the Shared Network Port but want to keep their management network traffic separate from their regular network traffic. For example, you can configure the management traffic for all of the iLO Shared Network Ports on a network to be on the same VLAN. Regular network traffic traveling through the Shared network Ports could be on the same LAN, different LANs, different VLAN, and so on.

To communicate with iLO through a client system, the client must be on the same VLAN as the iLO Shared Network Ports, and any network switches between the iLO Shared Network Port and the client must be IEEE 802.1q compliant. IEEE 802.1q managed switches might need to be configured to enable VLAN support.

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

- iLO RBSU
- iLO web interface
- XML scripting

The VLAN feature is only available on systems that support SNP NIC. All VLANs must be configured with a VLAN ID. The VLAN ID can be any number between 1 and 4094. Only users with the Configure iLO Settings privilege are allowed change enable or disable VLAN support and to configure VLAN IDs.

**Enabling and configuring VLAN using the iLO interface**

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

   **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.

2. Click **Network Settings**.

3. Click **Yes** in the Enable Virtual LAN option to enable the VLAN feature.
If the Shared Network Port is not selected, the choices for the Enable Virtual LAN radio button and the VLAN ID field are deactivated and cannot be configured.

4. Enter a number between 1 and 4094 in the Virtual LAN ID field.

   If the Virtual LAN feature is disabled, the Virtual LAN ID field is deactivated and cannot be configured.

5. Click **Apply**. iLO will reset with the current VLAN ID settings.

### Enabling and configuring VLAN using RBSU

1. Reboot the server and press the **F8** key. When prompted, enter iLO RBSU.

2. Navigate to **Network>NIC>TCP/IP**, and press the **Enter** key.

3. Use the space bar to select **Shared Network Port** in the Network Interface Adapter field.

4. Navigate to the Virtual LAN field, and use the space bar to select **Enabled**. A user definable VLAN ID field appears.

5. Navigate to the Virtual LAN ID field, and enter any number between 1 and 4094.
Enabling and configuring VLAN using XML

You can enable or disable VLAN support through XML scripting using RIBCL. For more information, refer the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*.

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](http://www.hp.com/servers/rdp)).
iLO security

In this section

Security features ................................................................. 135
General security guidelines ...................................................... 135
Encryption .............................................................................. 136
iLO Security Override Switch administration .................................. 136
Two-factor authentication......................................................... 138
User accounts......................................................................... 145
Password guidelines ................................................................ 146
Certificates............................................................................... 147
Securing RBSU ....................................................................... 148

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 146)
- Support for X.509 CA signed certificates (on page 147)
- Support for RBSU settings ("Global security settings" on page 146)
- 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.
Two-factor authentication

iLO is a powerful tool for managing HP ProLiant servers. To prevent misuse of this tool, access to iLO requires reliable user authentication. The 1.80 firmware release provides a stronger authentication scheme for iLO using two factors of authentication. Users will be asked to verify their identities by providing both of these factors. The two factors required are a password or PIN and private key for their digital certificate. Users will store their digital certificates and private keys wherever they choose, for example, smart card, USB token, or hard disk.

Setting up two-factor authentication for the first time

This section describes setting up Two-Factor Authentication for the first time using either local user accounts or directory user accounts. For more information on Two-Factor Authentication settings, refer to the "Two-Factor Authentication settings (on page 101)" section.

Setting up local user accounts:

1. Obtain the public certificate from the CA that issues user certificates or smart cards in your organization.
2. Export this certificate in base64 encoded format to a file on your desktop, for example, CACert.txt.
3. Obtain the public certificate of the user who needs access to iLO.
4. Export this certificate in base64 encoded format to a file on your desktop, for example, Usercert.txt.
5. Open the file CACert.txt in Notepad, select all of the text, and copy by pressing the Ctrl+C keys.
6. Login to iLO and browse to the Two-Factor Authentication Settings page.
7. Click Import Trusted CA Certificate. Another page displays.
8. Click the white text area so that your cursor is in the text area, and paste the clipboard by pressing the Ctrl+V keys.
9. Click Import Root CA Certificate. The Two-Factor Authentication Settings page displays again, with information displayed under Trusted CA Certificate Information.
10. From your desktop, open the Usercert.txt file in Notepad, select all of the text, and copy it to the clipboard by pressing the \texttt{Ctrl+C} keys.

11. Browse to the User Administration page on iLO, and select the user for which you have obtained a public certificate or create a new user.

12. Click View/Modify.

13. Click Add a certificate.

14. Click on the white text area so that your cursor is in the text area, paste the contents of the clipboard (\texttt{CTRL+V}).

15. Click Add user Certificate. The Modify User page displays again, with a 40 digit number in the Thumbprint field. This number can be compared to the thumbprint displayed for the certificate in Microsoft® Certificate Viewer.


17. Change Enforce Two-Factor Authentication to Yes.


19. Click Apply. iLO will reset. When iLO attempts to go to the login page again, your browser will display the Client Authentication window with a list of certificates that are available to this system.

   \textbf{NOTE:} If the user certificate is not registered on the client machine, you will not see it in the list. The user certificate must be registered on the client system before you can use it. If there are no client certificates on the client system you may not see the Client Authentication window and instead see a Page cannot be displayed error page. To resolve this, the client certificate must be registered on the client machine. For more information on exporting and registering client certificates, refer to the documentation for your smart card, or certificate authority.

20. Choose the certificate that was added to the user in iLO. Click OK.

21. If prompted to do so, insert your smart card, or enter your PIN or password.

After completing the authentication process, you will have access to iLO.

**Setting up directory user accounts:**

1. Obtain the public certificate from the CA that issues user certificates or smart cards in your organization.
2. Export this certificate in bas64 encoded format to a file on your desktop, for example, CAcert.txt.

3. Open the CAcert.txt file in Notepad, select all of the text, and copy it to the clipboard by pressing the Ctrl+C keys.

4. Login to iLO and browse to the Two-Factor Authentication Settings page.

5. Click Import Trusted CA Certificate. Another page displays.

6. Click the white text area so that your cursor is in the text area, and paste the clipboard by pressing the Ctrl+V keys.

7. Click Import Root CA Certificate. The Two-Factor Authentication Settings page displays again, with information displayed under Trusted CA Certificate Information.

8. Change Enforce Two-Factor authentication to Yes.


10. Change Certificate Owner Field to SAN. For more information, refer to the "Two-Factor Authentication Settings (on page 101)" section.

11. Click Apply. iLO resets. When iLO attempts to go to the login page again, your browser displays the Client Authentication window with a list of certificates that are available to this system.

12. Select the certificate added to the user in iLO. Click Ok.

13. If prompted to do so, insert your smart card, or enter your PIN or password. The login page should be displayed with the e-mail address for the user in the Directory User field. You cannot change this field.

14. Enter the password for the directory user. Click Login.

After completing the authentication process, you will have access to iLO. Refer to the "Directory Settings" section for more information on configuring directory users and privileges.
Two-factor authentication login

When you connect to an iLO configured to require two-factor authentication, the Client Authentication window prompts you to select the certificate you want to use. The Client Authentication window displays all of the certificates available to authenticate a client. Select the certificate mapped to a local user in iLO, or that is the user's certificate issued for authenticating to the domain.

After you have selected a certificate, if the certificate is protected with a password or if the certificate is stored on a smart card, a second window appears prompting you to enter the PIN or password associated with the chosen certificate.
The certificate is examined by iLO to ensure it was issued by the trusted CA by checking the signature against the CA certificate configured in iLO. iLO will determine if the certificate has been revoked and if it maps to a user in the iLO local user database. If all of these tests pass, then the normal iLO user interface appears.

If the user credential authentication fails, the Login Failed page displays. If login fails, you will be instructed to close the browser, open a new browser window, and try connecting again. If directory authentication is enabled, and local user authentication fails, iLO displays a login screen with the directory user name field populated with either the User Principal Name from the certificate or the Distinguished name (derived from the subject of the certificate). iLO requests the password for this user account. After providing the password, the user is authenticated.

For this release iLO does not address passing two-factor authentication through the Remote Console. Instead relies on smart card device support within RDP to provide access to systems that require smart card authentication for the remote operating system. iLO provides access to RDP with the Terminal Services pass-through function. Smart card authentication is only required for a remote server if an operating system is up and running. Support for smart cards in RDP requires that the operating system of the remote server be a version of Microsoft® Windows® Server 2003. Refer to the "Terminal Services Pass-Through option (on page 119)" section for additional information.
Two-factor authentication user certificates

To have a user authenticated through the two-factor authentication locally on iLO, a certificate must be associated with the user’s local user name. On the Administration>Modify User page, if a certificate has been mapped to the user a thumbprint (an SHA1 hash of the certificate) is displayed, as well as a button allowing the removal of the certificate. If a certificate has not been mapped to the user, "Thumbprint: A certificate has NOT been mapped to this user" is displayed, along with a button that will start the certificate import process.

To set up a user for two-factor authentication and add a user certificate:

1. Log on to iLO using an account that has the Configure iLO Settings privilege. Click Administration.
2. Select a user.
3. Click View/Modify.
4. Under the User Certificate Information section, click Add a certificate.
5. On the Map User Certificate page, paste the user certificate into the text-box and click Import Certificate.

For more information on user administration, refer to the "User administration (on page 86)" section.

Using two-factor authentication with directory authentication

In some cases, configuring two-factor authentication with directory authentication is complicated. iLO can use HP Extended schema or Default Directory schema to integrate with directory services. To ensure security when two-factor authentication is enforced, iLO uses an attribute from the client certificate as the directory user's login name. Which client certificate attribute iLO uses is determined by the Certificate Owner configuration setting on the Two-Factor Authentication Settings page. If Certificate Owner is set to SAN, iLO obtains the directory user's login name from the UPN attribute of the SAN. If the Certificate Owner setting is set to Subject, iLO obtains the directory user's distinguished name from the subject of the certificate.
Which one of these settings to choose depends on which directory integration method is used, how the directory architecture is designed, and what information is contained in user certificates that are issued. The following examples assume you have the appropriate permissions.

**Authentication using Default Directory Schema, part 1:** The distinguished name for a user in the directory is CN=John Doe,OU=IT,DC=MyCompany,DC=com, and the following are the attributes of John Doe's certificate:

- Subject: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

Authenticating to iLO with username:john.doe@MyCompany.com and password, will work if two-factor authentication is not enforced. After two-factor authentication is enforced, if SAN is selected on the Two-Factor Authentication Settings page, the login page automatically populates the Directory User field with john.doe@MyCompany.com. The password can be entered, but the user will not be authenticated. The user is not authenticated because john.doe@MyCompany.com, which was obtained from the certificate, is not the distinguished name for the user in the directory. In this case, you must select **Subject** on the Two-Factor Authentication Settings page. Then the Directory User field on the login page will be populated with CN=John Doe,OU=IT,DC=MyCompany,DC=com, which is the user's actual distinguished name. If the correct password is entered, the user is authenticated.

**Authentication using Default Directory Schema, part 2:** The distinguished name for a user in the directory is CN=john.doe@MyCompany.com,OU=IT,DC=MyCompany,DC=com, and the following are the attributes of John Doe's certificate:

- Subject: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- Search context on the Directory Settings page is set to: OU=IT,DC=MyCompany,DC=com
In this example, if SAN is selected on the Two-Factor Authentication Settings page, the Directory User field on the login page is populated with john.doe@MyCompany.com. After the correct password is entered, the user is authenticated. The user is authenticated even though john.doe@MyCompany.com is not the distinguished name for the user. The user is authenticated because iLO attempts to authenticate using the search context fields (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configured on the Directory Settings page. Because this is the correct distinguished name for the user, iLO successfully finds the user in the directory.

**NOTE:** Selecting Subject on the Two-Factor Authentication Settings page causes authentication to fail, because the subject of the certificate is not the distinguished name for the user in the directory.

When using the HP Extended schema method, HP recommends selecting the SAN option on the Two-factor Authentication Settings page.

**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 the 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.

You can create a certificate request or import an existing certificate using RIBCL XML commands. These commands enable you to script and automate certificate deployment on iLO servers instead of manually deploying certificates through the Web interface. For more information, refer to "CERTIFICATE_SIGNING_REQUEST" and "IMPORT_CERTIFICATE" in the "Remote Insight Command Language" section.

CERTIFICATE_SIGNING_REQUEST and IMPORT_CERTIFICATE cannot be used with the standard CPQLOCFG utility. However, you can use the PERL version of CPQLOCFG in combination with these commands.

## 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

Overview of directory integration ................................................................. 151
Benefits of directory integration ................................................................. 151
How directory integration works ............................................................... 152
Advantages and disadvantages of schema-free and HP Extended schema ....... 153
Setup for Schema-free directory integration .............................................. 154
Setting up HP schema directory integration ........................................... 157
Configuring directory settings .................................................................. 197
Directory tests ......................................................................................... 199

Overview of directory integration

iLO can be configured to use a directory to authenticate and authorize its users. There are two configuration options available: using a directory that has been extended with HP Schema or using the directory’s default schema (schema-free.)

There are white papers available for more information on directory integration on the HP website (http://www.hp.com/servers/lights-out).

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 (when using HP Extended schema)—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, which 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—When configured for HP Extended schema, you can create a single role for a single user on a single iLO, 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.

How directory integration works

Schema-free

At the login page, enter a login name and a password. If ActiveX is enabled in the browser, the login name is converted to the directories DN format and stored in a security cookie in the browser. The browser then loads the home page for iLO.
iLO reads the security cookie and extracts the DN for each page displayed. iLO reads the directory object pointed to by the DN. iLO then determines what groups the object is a member of and compares this information with a list kept in iLO. If there is a match, then the privileges associated with this group in iLO determine whether you have access to the page requested.

When using a schema-free directory configuration, after you attempt to log in to iLO, iLO attempts to read your object in the directory to determine what groups you are a member of. iLO compares the list of groups to group names iLO is configured to recognize. If iLO finds a match, iLO determines what privileges you have based on the privileges configured for that group in iLO.

If you are a member of any group that iLO recognizes, you have login rights to iLO, regardless of what rights are associated with the group. User rights are a combination of all rights for the groups you are a member of that iLO recognizes.

If at login the ActiveX control does not run, then the complete login name or the login name prepended with a user context is used for the directory lookup process. For this to work, the login name must either be in full DN format or in a format that the combination of the login name with a user context is made into a full DN.

**HP Extended schema**

Refer to the "Directory-enabled remote management (on page 201)" section.

### Advantages and disadvantages of schema-free and HP Extended schema

Before configuring iLO for directories, you must decide whether to use the directory's schema-free (default schema) or the HP Extended schema option.

The advantages of using the schema-free option are:

- There is no need to extend the directory's schema.
- When ActiveX controls are enabled on the browser, login using NetBIOS and e-mail formats is supported.

The advantages of using the HP Extended schema option are:
• There is much more flexibility in controlling access. For example, access can be limited to a time of day or from a certain range of IP addresses.
• Groups are maintained in the directory, not on each iLO.
• RILOE and RILOE II only work with HP Extended schema. (Schema-free will be added to RILOE II at later date.)
• iLO, RILOE, and RILOE II will only work with eDirectory with HP Extended schema.

Setup for Schema-free directory integration

Before setting up the Schema-free option, your system must meet all the prerequisites outlined in the "Active Directory Preparation (on page 154)" section.

You can set up iLO for directories in three ways:
• Manually using a browser ("Schema-free browser-based setup" on page 155).
• Using a script ("Schema-free scripted set up" on page 155).
• Using HPLOMIG ("Schema-free HPLOMIG-based setup" on page 156).

Active Directory preparation

The schema-free option is supported on the following operating systems:
• Microsoft® Active Directory
• Microsoft® Windows® Server 2003 Active Directory

SSL must be enabled at the directory. To enable SSL, install a certificate for the domain in Active Directory. iLO only communicates with the directory over a secure SSL connection. For more information, refer to the Microsoft® Knowledge Base, article number 247078: Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers on the Microsoft® website (http://support.microsoft.com/).
To validate the setup, you should have the directory distinguished name for at least one user and the distinguished name of a security group the user is a member of.

**Schema-free browser-based setup**

Schema-free can be setup using the iLO browser-based interface.

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

2. Click Directory Settings.

3. Select Use Directory Default Schema in the Authentication Settings section. For more information, refer to the "Schema-free setup options (on page 156)" section.

4. Click Apply Settings.

5. Click Test Settings.

**Schema-free scripted set up**

Schema-free can be set up using RIBCL XML scripting.


2. Write a script that configures iLO for schema-free directories support and run it. The following script can be used as a template.

```xml
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">
<DIR_INFO MODE = "write">
  <MOD_DIR_CONFIG>
    <DIR_ENABLE_GRP_ACCT value = "yes"/>
    <DIR_GRPACCT1_NAME value ="CN=Administrators,CN=Builtin,DC=HP,DC=com "/>
    <DIR_GRPACCT1_PRIV value = "1"/>
  </MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```
Schema-free HPLOMIG-based setup

HPLOMIG is the easiest way to set up a large number of LOM processors for directories. To use HPLOMIG, download the HPQLOMIG utility and additional documentation from the HP website (http://www.hp.com/servers/lights-out). HP recommends using HPLOMIG when configuring many LOM processors for directories. For more information on using HPLOMIG, refer to the "HPLOMIG Operation ("HPQLOMIG operation" on page 220)" section.

Schema-free setup options

Setup options are the same regardless of which method (browser, HPQLOMIG, or script) you use to configure the directory.

After enabling directories and selecting the Schema-free option, you have the following options.

Minimum Login Flexibility

- Enter the directory server’s DNS name or IP address and LDAP port. Typically, the LDAP port for an SSL connection is 636.

- Enter the distinguished name for at least one group. This group can be a security group (for example: "CN=Administrators,CN=Builtin,DC=HP,DC=com") or any other group as long as the intended iLO users are members of the group.

  With a minimum configuration, you can log into iLO using your full distinguished name and password. You must be a member of a group that iLO recognizes.

Better Login Flexibility

- In addition to the minimum settings, enter at least one directory user context.
At login time, the login name and user context are combined to make the user's distinguished name. For instance, if the user logs in as "JOHN.SMITH" and a user context is set up as "CN=USERS,DC=HP,DC=COM", then the distinguished name that iLO will try will be "CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM."

**Maximum Login Flexibility**

- Configure iLO as described.
- Configure iLO with a DNS name, not an IP address for the directory server's network address. The DNS name must be resolvable to an IP address from both iLO and the client system.
- Enable ActiveX controls in your browser. The iLO login script will attempt to call a Windows® control to convert the login name to a distinguished name.

Configuring iLO with maximum login flexibility enables you to login using your full distinguished name and password, your name as it appears in the directory, NetBIOS format (domain/login_name), or the e-mail format (login_name@domain).

**NOTE:** Your system security settings or installed software might prevent the login script from calling the Windows® ActiveX control. If this happens, your browser displays a warning message in the status bar, message box, or might stop responding. To help identify what software or setting is causing the problem, create another profile and log in to the system.

In some cases, it might not be possible to get the maximum login flexibility option to work. For instance, if the client and iLO are in different DNS domains, one of the two might not be able to resolve the directory server name to an IP address.

### Setting up HP schema directory integration

When using the HP schema directory integration, iLO supports both Active Directory and eDirectory. However, these directory services require the schema being extended.
Features supported by HP schema 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.

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 to 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.

Setting up directory services

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

1. **Plan**

   Review the following sections:
   - "Directory services (on page 151)"
   - "Directory services schema (on page 293)"
   - "Directory-enabled remote management (on page 201)"

2. **Install**


   b. Run the schema installer (on page 161) once to extend the schema.
c. Run the management snap-in installer (on page 165), 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 97) 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 175) 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 201)." Examples are available in the "Directory services for Active Directory (on page 166)" and "Directory services for eDirectory (on page 184)" sections.

5. Handle exceptions
   – Lights-Out migration utilities are easier to use with a single Lights-Out role. If you plan to create 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 202)" 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:

<table>
<thead>
<tr>
<th>LOM product</th>
<th>Minimum supported firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>RILOE</td>
<td>2.41</td>
</tr>
<tr>
<td>RILOE II</td>
<td>All versions</td>
</tr>
<tr>
<td>iLO</td>
<td>1.10</td>
</tr>
</tbody>
</table>
After the schema has been extended, you can complete the directory services setup by using HP Lights-Out Directories Migration Utilities (on page 217). 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 293)."

Directory services support

Using HP schema directory integration, iLO supports the following directory services:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

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®. Spawning 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 running on one of the following operating systems:

- NetWare 5.X
- NetWare 6.X
- Red Hat Enterprise Linux AS 2.1

**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.

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.
Results

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

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.

• 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/).
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:

- 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\Services\Parameters\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.
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).
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 175)."

   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**.

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, \textit{rib-email-server} in folder testdomain.local/RLOES. Click \textbf{OK} to close the dialog, then click \textbf{Apply} to save the list.
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.

![Image of remoteAdmins Properties dialog box]

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=RILCES,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.
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.

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

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.

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.

**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*

**Snap-in installation and initialization for eDirectory**

Refer to "Snap-in installation and initialization ("Snap-in installation and initialization for Active Directory" on page 169)" 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.

![Properties of remoteAdmins](image)

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 LOM 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 LOM 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 LOM 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.

```plaintext
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.

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

### 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.
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.

The available rights are:

- **Login**—This option controls whether users can 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.

**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\username 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.

Configuring directory settings

The Directory Settings screen contains the following settings options:

- Disable Directory Authentication
- Use Directory Default Schema
• Use HP Extended Schema
• Enable Local User Accounts
• Directory Server Address
• Directory Server LDAP Port
• LOM Object Distinguished Name
• LOM Object Password

   🔄 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

Click **Apply Settings** to save any changes. For more information refer to the *HP Integrated Lights-Out 1.70 Scripting and Applications Guide*.

To test the communication between the directory server and iLO, click **Test Settings**. Refer to the "Directory Tests (on page 199)" section for additional information.
Directory tests

To validate current directory settings for iLO, click **Test Settings** on the Directory Settings page. The Directory Tests page appears.

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 and 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 account would be intended to access the iLO being tested. It can be the same account as the directory administrator. However, the tests cannot 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.
Directory-enabled remote management

In this section

Introduction to directory-enabled remote management .............................................................. 201
Using bulk import tools .............................................................................................................. 202
Using existing groups ................................................................................................................. 203
Using multiple roles ........................................................................................................... ........ 204
Creating roles to follow organizational structure ....................................................................... 205
Restricting roles.............................................................................................................. ............ 205
How directory login restrictions are enforced ............................................................................ 208
How user time restrictions are enforced ..................................................................................... 208
User address restrictions...................................................................................................... ....... 209
Creating multiple restrictions and roles ...................................................................................... 210

Introduction to directory-enabled remote management

This section is for administrators who are familiar with directory services and the iLO product and want to use the HP schema directory integration option for iLO. You must be familiar with the “Directory services (on page 151)” section and comfortable with setting up and understanding the examples.

Directory-enabled remote management enables you to:

- Create Lights-Out Management Objects

  You 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 151)” section for additional information on creating LOM device objects for Active Directory ("Directory services for Active Directory" on page 166) and eDirectory ("Directory services for eDirectory” on page 184). In general, you 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 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 197)" for details on the specific directory settings. In general, you can 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 217)" 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 217)" 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" and the "Remote Insight command language" sections in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*.

- **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 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 293)" 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 178)" or "eDirectory Role Restrictions (on page 192)" 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 Client
Workstation
Directory Server LOM

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 time restrictions are enforced by the directory server

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.
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.
Certificate services

In this section
Introduction to certificate services ................................................................. 213
Installing certificate services ............................................................................ 213
Verifying directory services ............................................................................. 214
Configuring Automatic Certificate Request ..................................................... 214

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**.

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.
Lights-Out directories migration utilities

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 directories. 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 Directory 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 or schema-free directories.
- Name the management processors to identify them in the directory.
- Create objects in the directory corresponding to each management processor and associate 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.

<table>
<thead>
<tr>
<th>Management processor</th>
<th>Minimum firmware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RILOE</td>
<td>2.41</td>
</tr>
</tbody>
</table>
2. Install Microsoft® .NET Framework.


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 218)" 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 you click 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 canceled.

To start the process of discovering your management processors:

1. Click **Start** and select **Programs>Hewlett-Packard, Lights-Out Migration Utility** to start the migration process.
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 and password and click **Find**. The Find button changes to Verify when the search is complete.

You can also input a list of management processors by clicking **Import**. The file is a simple text file with one management processor listed per line. The fields are delimited with semicolons. The fields are as follows:

- Network Address
- Management Processor Type
- Firmware Version
- DNS Name
- User Name
- Password
- Directory Configuration

For example, one line could have:

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
```

If for security reasons the user name and password cannot be in the file, then leave these fields blank, but keep the semicolons.

**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 entering the path or clicking **Browse**.

![WARNING ICON] **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 HP website ([http://www.hp.com/servers/lights-out](http://www.hp.com/servers/lights-out)).

<table>
<thead>
<tr>
<th>Management processor</th>
<th>Minimum firmware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RILOE</td>
<td>2.50</td>
</tr>
<tr>
<td>RILOE II</td>
<td>1.10</td>
</tr>
</tbody>
</table>
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 appears 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 are 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 continues to run in the background and completes the firmware upgrade on all selected devices.
Selecting a directory access method

After the Firmware Upgrade page, the Select Directory Access Method page displays. You can select which management processors to configure (with respect to schema usage) and how it will be configured. The Select Directory Access Method page helps to prevent an accidental overwrite of iLOs already configured for HP schema or those that have directories turned off.

This page determines if the HP Extended schema, schema-free (default schema), or no directories support configuration pages follow.

To configure the management processor for:
• Directory Services, refer to the "Configuring directories when HP Extended schema is selected (on page 227)" section.

• Schema-free (default schema) directories support, refer to the "Setup for Schema-free directory integration (on page 154)" section.

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
• The DNS name
• An index
• Manually
• 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 Use Network Address, Use DNS Names, or Create Name Using Index. You can also name each management processor directory object by clicking twice in the name field with a delay between clicks.

2. Enter text to prepend or append all names (optional).

3. Click Generate Names. The names display in the Name column as they are generated. At this point, names are not written to the directory or the management processors. The names are stored until the next page.

4. To change the names (optional), click Clear All Names and rename the management processors.
5. After the names are correct, click Next.

![Configure Directory Screen]

### Configuring directories when HP Extended schema is selected

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**—The network address of the directory server and can either be a valid DNS name or IP address.

• **Port**—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 distinguished name. 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 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 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**. The tool will connect to the directory, creates the management processor objects, and adds them to the selected roles.
5. After the device objects have been associated with a role, click **Next**.

### Configuring directories when schema-free integration is selected

The fields in the Configure Management Processors screen are:

- **Network Address**—The network address of the directory server, which can be a valid DNS name or IP address.

- **Login Name** and **Password**—These fields are used to log in with an account that has domain administrator access to the directory.
• **Security Group Distinguished Name**—The distinguished name of the group in the directory that contains a set of iLO users with a common set of privileges. If the directory name, login name, and password are correct, you can click the **Browse** button to navigate to and select the group.

• **Privileges**—The iLO privileges associated with the selected group. The login privilege is implied if the user is a member of the group.

Configure Management Processors settings are stored until the next page in the wizard.

![hp Lights-Out Directories Migration Utility](image)

**Configure Management Processors**

Configure management processors to use the directory's default schema.

```
Directory Server
Network Address: 16.100.225.234
Login Name: Administrator
Password: ********
```

```
Group 1 | Group 2 | Group 3 | Group 4 | Group 5 | Group 6
---|---|---|---|---|---

Security Group Distinguished Name

**CN=Administrators,CN=BuiltIn,CN=ILOTEST2,DC=HP**

**Privileges**

- [x] Administer User Accounts
- [x] Virtual Media
- [x] Remote Console Access
- [x] Configure iLO Settings
- [x] Virtual Power and Reset

Connecting to directory.
Object reference not set to an instance of an object.

Apply

< Back | Next > | Done
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.

User contexts enable the user to use short or user object names to log in, rather than the full distinguished name. For example, having a user context such as CN=Users,DC=RLOETEST2,DC=HP enables user "John Smith" to log in using John Smith, rather than CN=John Smith,CN=Users, DC=RLOETEST2,DC=HP. The @ format is also supported. For example, @RLOETEST2.HP in a context field enables 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. For Directories Support and Local Accounts option, select Enabled or Disabled.
   Remote access is disabled if both Directory Support and Local Accounts are disabled. To reestablish access, reboot the server and use RBSU F8 to restore access.
3. Click Configure. The migration utility connects to all of the selected management processors and updates their configuration as you have specified.
4. When the process completes, 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.

### 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 functionality.
IMPORTANT: Installing directory support for any management processor requires downloading the HP Smart Component. Refer to the "Pre-migration checklist (on page 218)" 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 222), 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 toVerbose 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.
Insight Manager 7 integration

In this section

Integrating iLO with Insight Manager 7 ................................................................. 237
Functional overview .....................................................................................................238
Identification and association .....................................................................................238
Configuring identification of iLO ..................................................................................240
Receiving SNMP alerts in Insight Manager 7 ..............................................................240
Port matching ................................................................................................................242
Reviewing iLO advanced license information in Insight Manager 7 ..............................242
ProLiant BL p-Class rack visualization ........................................................................244

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.

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 \textit{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:

- **Enabled**—Associations are present, and all data is present on the summary page.
- **Disabled**—No data is returned to Insight Manager 7 or Systems Insight Manager.

**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 95)" 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 20)" 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:

- \textit{Port} is the number of the additional HTTP port to be added into discovery.
- \textit{Description} is the description of the Web server to be displayed in the list of links on the device page.
- \textit{Reserved 1} is reserved and should be set to a space.
- \textit{Reserved 2} is reserved and should be set to true.
- \textit{Reserved 3} is reserved and should be set to false.
- \textit{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:

\[ 80=iLO, \text{true}, \text{false}, \text{compaq.ID.MgmtProc.MgmtProcessorParser} \]

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 Enabled for Insight Manager 7 to draw the visualization.
Systems Insight Manager integration

In this section

Integrating iLO with Systems Insight Manager ................................................................. 245
Systems Insight Manager functional overview ................................................................. 246
Configuring Systems Insight Manager identification of iLO ............................................. 248
Receiving SNMP alerts in Systems Insight Manager ......................................................... 249
Systems Insight Manager port matching ........................................................................... 250
Reviewing iLO Advanced Pack license information in Systems Insight Manager ............... 251
Systems Insight Manager ProLiant BL p-Class rack visualization .................................... 251

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 Installation and User Guide*, provided with Systems Insight Manager.
Systems 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.

Systems 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*.

**Systems 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.

**Systems 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 Systems 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 240)."
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 95)” 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 20)” for additional details about installing and configuring agents.

Systems 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.identification.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.

Systems Insight Manager ProLiant BL p-Class rack visualization

HP Systems Insight Manager provides comprehensive management of ProLiant BL p-Class server blades. HP Systems 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 Systems 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.
Troubleshooting iLO

In this section

Minimum requirements ..............................................................................................................253
iLO POST LED indicators .......................................................................................................254
Event log entries ....................................................................................................................256
Hardware and software link-related issues...........................................................................260
Login issues ...........................................................................................................................261
Troubleshooting alert and trap problems .............................................................................268
Troubleshooting directory problems ....................................................................................270
Troubleshooting mouse problems .......................................................................................271
Troubleshooting Remote Console problems .........................................................................273
Troubleshooting SSH and Telnet problems ..........................................................................276
Troubleshooting terminal services problems .......................................................................277
Troubleshooting video and monitor problems ......................................................................278
Troubleshooting Virtual Media problems ............................................................................279
Troubleshooting miscellaneous problems .............................................................................280

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
  - Mozilla 1.60 or Firefox 1.0.2 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/jvm).

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 or 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.

A sequential flashing pattern on LEDs, 1, 2, 3, 4, 5, 6, 7, and 8, repeating indefinitely, indicates iLO has experienced a failed flash (firmware upgrade) and is in the flash recovery mode. Refer to the "iLO network flash recovery (on page 284)" section for more information.

The LED indicators have the following assignments:

<table>
<thead>
<tr>
<th>LED indicators</th>
<th>POST code (activity completed)</th>
<th>Description</th>
<th>Failure indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>00</td>
<td>Set up chip selects.</td>
<td></td>
</tr>
<tr>
<td>1 or 2</td>
<td>02—Normal operation</td>
<td>Determine platform.</td>
<td></td>
</tr>
<tr>
<td>2 and 1</td>
<td>03</td>
<td>Set RUNMAP bit.</td>
<td></td>
</tr>
<tr>
<td>LED indicators</td>
<td>POST code (activity completed)</td>
<td>Description</td>
<td>Failure indicates</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>3</td>
<td>04</td>
<td>Initialize SDRAM controller.</td>
<td></td>
</tr>
<tr>
<td>3 and 2</td>
<td>06</td>
<td>Activate the I cache.</td>
<td></td>
</tr>
<tr>
<td>3, 2, and 1</td>
<td>07</td>
<td>Initialize (only) the D cache.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>08</td>
<td>Copy secondary loader to RAM.</td>
<td>Could not copy secondary loader.</td>
</tr>
<tr>
<td>4 and 1</td>
<td>09</td>
<td>Verify secondary loader.</td>
<td>Did not execute secondary loader.</td>
</tr>
<tr>
<td>4 and 2</td>
<td>0a</td>
<td>Begin secondary loader.</td>
<td>SDRAM memory test failed.</td>
</tr>
<tr>
<td>4, 2, and 1</td>
<td>0b</td>
<td>Copy ROM to RAM.</td>
<td>Could not copy boot block.</td>
</tr>
<tr>
<td>4 and 3</td>
<td>0c</td>
<td>Verify ROM image in RAM.</td>
<td>Boot block failed to execute.</td>
</tr>
<tr>
<td>4, 3, and 1</td>
<td>0d</td>
<td>Boot Block Main started.</td>
<td>Boot block could not find a valid image.</td>
</tr>
<tr>
<td>None</td>
<td></td>
<td>Start C Run time initialization.</td>
<td></td>
</tr>
<tr>
<td>4, 3, and 2</td>
<td>0e</td>
<td>Main() has received control.</td>
<td>Main self-test failed.</td>
</tr>
<tr>
<td>Varies</td>
<td>Varies</td>
<td>Each subsystem may self-test.</td>
<td></td>
</tr>
<tr>
<td>4, 3, 2, and 1</td>
<td>0f</td>
<td>Start ThreadX.</td>
<td>RTOS startup failed.</td>
</tr>
<tr>
<td>None</td>
<td>00</td>
<td>Main_init() completed.</td>
<td>Subsystem startup failed.</td>
</tr>
<tr>
<td>HB and 7</td>
<td></td>
<td>Flashes as the iLO processor executes firmware code. It does not change the value of the lower six LEDs.</td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>FEH Code</th>
<th>Consistency Check</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>9902</td>
<td>TXAPICHK</td>
<td>An RTOS function was called with an inappropriate value or from an inappropriate caller.</td>
</tr>
<tr>
<td>9903</td>
<td>TXCONTEXT</td>
<td>The saved context of one or more threads has been corrupted.</td>
</tr>
<tr>
<td>9905</td>
<td>TRAP</td>
<td>A stack probe failed, the return address is invalid, or an illegal trap instruction has been detected.</td>
</tr>
<tr>
<td>9966</td>
<td>NMIWR</td>
<td>An unexpected write to low memory has occurred.</td>
</tr>
<tr>
<td>99C1</td>
<td>CHKNULL</td>
<td>The reset vector has been modified.</td>
</tr>
</tbody>
</table>

### Event log entries

<table>
<thead>
<tr>
<th>Event log display</th>
<th>Event log explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server power failed</td>
<td>Displays when the server power fails.</td>
</tr>
<tr>
<td>Browser login: IP address</td>
<td>Displays the IP address for the browser that logged in.</td>
</tr>
<tr>
<td>Server power restored</td>
<td>Displays when the server power is restored.</td>
</tr>
<tr>
<td>Browser logout: IP address</td>
<td>Displays the IP address for the browser that logged out.</td>
</tr>
<tr>
<td>Server reset</td>
<td>Displays when the server is reset.</td>
</tr>
<tr>
<td>Failed Browser login – IP Address: IP address</td>
<td>Displays when a browser login fails.</td>
</tr>
<tr>
<td>iLO Self Test Error: #</td>
<td>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.</td>
</tr>
<tr>
<td>iLO reset</td>
<td>Displays when iLO is reset.</td>
</tr>
<tr>
<td>On-board clock set; was #:#:##:#:#:#</td>
<td>Displays when the onboard clock is set.</td>
</tr>
<tr>
<td><strong>Event log display</strong></td>
<td><strong>Event log explanation</strong></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Server logged critical error(s)</td>
<td>Displays when the server logs critical errors.</td>
</tr>
<tr>
<td>Event log cleared by: User</td>
<td>Displays when a user clears the event log.</td>
</tr>
<tr>
<td>iLO reset to factory defaults</td>
<td>Displays when iLO is reset to the default settings.</td>
</tr>
<tr>
<td>iLO ROM upgrade to #</td>
<td>Displays when the ROM has been upgraded.</td>
</tr>
<tr>
<td>iLO reset for ROM upgrade</td>
<td>Displays when iLO is reset for the ROM upgrade.</td>
</tr>
<tr>
<td>iLO reset by user diagnostics</td>
<td>Displays when iLO is reset by user diagnostics.</td>
</tr>
<tr>
<td>Power restored to iLO</td>
<td>Displays when the power is restored to iLO.</td>
</tr>
<tr>
<td>iLO reset by watchdog</td>
<td>Displays when an error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.</td>
</tr>
<tr>
<td>iLO reset by host</td>
<td>Displays when the server resets iLO.</td>
</tr>
<tr>
<td>Recoverable iLO error, code #</td>
<td>Displays when a non-critical error has occurred in iLO and iLO has reset itself. If this problem persists, call customer support.</td>
</tr>
<tr>
<td>SNMP trap delivery failure: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Test SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Power outage SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Server reset SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Illegal login SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Diagnostic error SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Host generated SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>Network resource shortage SNMP trap alert failed for: IP address</td>
<td>Displays when the SNMP trap does not connect to the specified IP address.</td>
</tr>
<tr>
<td>iLO network link up</td>
<td>Displays when the network is connected to iLO.</td>
</tr>
<tr>
<td>iLO network link down</td>
<td>Displays when the network is not connected to iLO.</td>
</tr>
</tbody>
</table>
### Event log display

<table>
<thead>
<tr>
<th>Event log display</th>
<th>Event log explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>iLO Firmware upgrade started by: <strong>User</strong></td>
<td>Displays when a user starts a firmware upgrade.</td>
</tr>
<tr>
<td>Host server reset by: <strong>User</strong></td>
<td>Displays when a user resets the host server.</td>
</tr>
<tr>
<td>Host server powered OFF by: <strong>User</strong></td>
<td>Displays when a user powers off a host server.</td>
</tr>
<tr>
<td>Host server powered ON by: <strong>User</strong></td>
<td>Displays when a user powers on a host server.</td>
</tr>
<tr>
<td>Virtual Floppy in use by: <strong>User</strong></td>
<td>Displays when a user begins using a Virtual Floppy.</td>
</tr>
<tr>
<td>Remote Console login: <strong>User</strong></td>
<td>Displays when a user logs on a Remote Console session.</td>
</tr>
<tr>
<td>Remote Console Closed</td>
<td>Displays when a Remote Console session is closed.</td>
</tr>
<tr>
<td>Failed Console login - IP Address: <strong>IP address</strong></td>
<td>Displays a failed console login and IP address.</td>
</tr>
<tr>
<td>Added User: <strong>User</strong></td>
<td>Displays when a local user is added.</td>
</tr>
<tr>
<td>User Deleted by: <strong>User</strong></td>
<td>Displays when a local user is deleted.</td>
</tr>
<tr>
<td>Modified User: <strong>User</strong></td>
<td>Displays when a local user is modified.</td>
</tr>
<tr>
<td>Browser login: <strong>User</strong></td>
<td>Displays when a valid user logs on to iLO using an Internet browser.</td>
</tr>
<tr>
<td>Browser logout: <strong>User</strong></td>
<td>Displays when a valid user logs off iLO using an Internet browser.</td>
</tr>
<tr>
<td>Failed Browser login – IP Address: <strong>IP address</strong></td>
<td>Displays when a browser login attempt fails.</td>
</tr>
<tr>
<td>Remote Console login: <strong>User</strong></td>
<td>Displays when an authorized user logs on using the Remote Console port.</td>
</tr>
<tr>
<td>Remote Console Closed</td>
<td>Displays when an authorized Remote Console user is logged out or when the Remote Console port is closed following a failed login attempt.</td>
</tr>
<tr>
<td>Failed Console login – IP Address: <strong>IP address</strong></td>
<td>Displays when an unauthorized user has failed three login attempts using the Remote Console port.</td>
</tr>
<tr>
<td>Added User: <strong>User</strong></td>
<td>Displays when a new entry is made to the authorized user list.</td>
</tr>
<tr>
<td>User Deleted by: <strong>User</strong></td>
<td>Displays when an entry is removed from the authorized user list. The User section displays the user who requested the removal.</td>
</tr>
<tr>
<td>Event Log Cleared: <strong>User</strong></td>
<td>Displays when the user clears the Event Log.</td>
</tr>
<tr>
<td>Event log display</td>
<td>Event log explanation</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Power Cycle (Reset): <em>User</em></td>
<td>Displays when the power has been reset.</td>
</tr>
<tr>
<td>Virtual Power Event: <em>User</em></td>
<td>Displays when the Virtual Power Button is used.</td>
</tr>
<tr>
<td>Security Override Switch Setting is On</td>
<td>Displays when the system is booted with the Security Override Switch set to On.</td>
</tr>
<tr>
<td>Security Override Switch Setting Changed to Off</td>
<td>Displays when the system is booted with the Security Override Switch changed from On to Off.</td>
</tr>
<tr>
<td>On-board clock set; was previously [NOT SET]&quot;</td>
<td>Displays when the on-board clock is set. Will display the previous time or &quot;NOT SET&quot; if there was not a time setting previously.</td>
</tr>
<tr>
<td>Logs full SNMP trap alert failed for: <em>IP address</em></td>
<td>Displays when the logs are full and the SNMP trap alert failed for a specified IP address.</td>
</tr>
<tr>
<td>Security disabled SNMP trap alert failed for: <em>IP address</em></td>
<td>Displays when the security has been disabled and the SNMP trap alert failed for a specified IP address.</td>
</tr>
<tr>
<td>Security enabled SNMP trap alert failed for: <em>IP address</em></td>
<td>Displays when the security has been enabled and the SNMP trap alert failed for a specified IP address.</td>
</tr>
<tr>
<td>Virtual Floppy connected by <em>User</em></td>
<td>Displays when an authorized user connects the Virtual Floppy.</td>
</tr>
<tr>
<td>Virtual Floppy disconnected by <em>User</em></td>
<td>Displays when an authorized user disconnects the Virtual Floppy.</td>
</tr>
<tr>
<td>License added by: <em>User</em></td>
<td>Displays when an authorized user adds a license.</td>
</tr>
<tr>
<td>License removed by: <em>User</em></td>
<td>Displays when an authorized user removes a license.</td>
</tr>
<tr>
<td>License activation error by: <em>User</em></td>
<td>Displays when there is an error activating the license.</td>
</tr>
<tr>
<td>iLO RBSU user login: <em>User</em></td>
<td>Displays when an authorized user logs in to iLO RBSU.</td>
</tr>
<tr>
<td>Power on request received by: <em>Type</em></td>
<td>A power request was received as one of the following types:</td>
</tr>
<tr>
<td></td>
<td>Power Button</td>
</tr>
<tr>
<td></td>
<td>Wake On LAN</td>
</tr>
<tr>
<td></td>
<td>Automatic Power On</td>
</tr>
<tr>
<td>Event log display</td>
<td>Event log explanation</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual NMI selected by: User</td>
<td>Displays when an authorized user selects the Virtual NMI button.</td>
</tr>
<tr>
<td>Virtual Serial Port session started by: User</td>
<td>Displays when a Virtual Serial Port session is started.</td>
</tr>
<tr>
<td>Virtual Serial Port session stopped by: User</td>
<td>Displays when a Virtual Serial Port session is ended.</td>
</tr>
<tr>
<td>Virtual Serial Port session login failure from: User</td>
<td>Displays when there is a login failure for a Virtual Serial Port session.</td>
</tr>
</tbody>
</table>

## 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” 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.
Troubleshooting iLO 265

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 in to iLO after installing the iLO certificate

If the iLO self-signed certificate is installed permanently into some browsers and the iLO is reset, you might not be able to log back in to iLO because iLO generates a new self-signed certificate every time it is reset. When a certificate is installed in 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, do not install the iLO self-signed certificate in 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 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.
Two-factor authentication login failure

When authentication fails, a similar page appears.

Logging in to iLO using the two-factor smart card authentication will fail if:

- The certificate selected in the Client Authentication page is not issued by the trusted Certificate Authority
- The certificate was issued by the trusted CA but not mapped to a local user account
- Directory authentication is enabled (a different page appears)
In this case, the username field is populated with the user principle name obtained from the certificate or with the distinguished name of the directory user, which is derived from the certificate subject. This setting is configured using the Certificate Owner field on the Two-Factor Authentication Settings page on iLO. The user name field cannot be modified. iLO will not allow an attempt to authenticate with any other directory user besides the user for which the certificate was issued.

To correct these issues, be sure a certificate is issued by the CA and mapped to the user. For more information, refer to the "Two-factor authentication settings (on page 101)" section.

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

<table>
<thead>
<tr>
<th>Alert</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Trap</td>
<td>This trap is generated by a user through the Web configuration page.</td>
</tr>
<tr>
<td>Server Power Outage</td>
<td>Server has lost power.</td>
</tr>
<tr>
<td>Server Reset</td>
<td>Server has been reset.</td>
</tr>
<tr>
<td>Failed Login Attempt</td>
<td>Remote user login attempt failed.</td>
</tr>
<tr>
<td>General Error</td>
<td>This is an error condition that is not predefined by the hard-coded MIB.</td>
</tr>
<tr>
<td>Logs</td>
<td>Circular log has been overrun.</td>
</tr>
<tr>
<td>Security Override Switch Changed: On/Off</td>
<td>The state of the Security Override Switch has changed (On/Off).</td>
</tr>
<tr>
<td>Rack Server Power On Failed</td>
<td>The server was unable to power on because the BL p-Class rack indicated that insufficient power was available to power on the server.</td>
</tr>
<tr>
<td>Rack Server Power On Manual Override</td>
<td>The server was manually forced by the customer to power on despite the BL p-Class reporting insufficient power.</td>
</tr>
</tbody>
</table>
Alert | Explanation
---|---
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 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 directory problems

The following sections discuss troubleshooting directory issues.

I can not log in using domain/name format but I can using the full distinguished name

To login using the domain/name format, ActiveX controls must be enabled. To verify that your browser is letting the login script call ActiveX controls open Internet Explorer and set ActiveX controls to Prompt. You should see a similar to the following figure.

![ActiveX prompt](image)

ActiveX controls are enabled and I see a prompt but the domain/name login format does not work

1. Log in with a local account and determine the directory server name.
2. Verify the directory server name is a name and not an IP address.
3. Verify you can ping the directory server name from your client.
4. Run directory setup tests. Verify the ping was received successfully. For more information on testing directory settings, refer the the "Directory tests (on page 199)" section.

User contexts do not appear to work

Check with your network administrator. The full distinguished name of your user object must be in the directory. Your login name is what appears after the first CN=. The remainder of the distinguished name should appear in one of the user context fields. User contexts are not case-sensitive. However, anything else, including spaces are part of the user context.

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"
  ```
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:

2. Set the slider control to full hardware acceleration.

For more information, refer to the "Optimizing performance for graphical Remote Console (on page 50)" 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 3.0 WS
  - Mozilla 1.7
  - Firefox 1.02
- Novell Linux Desktop
  - Mozilla 1.7
  - Firefox 1.02

Remote Console applet has a red X when running Linux client browser

Mozilla browsers must be configured to accept cookies.

1. Open the Preferences menu, and select Privacy & Security>Cookies.
2. On the Level of Privacy screen, select Allow cookies based on privacy settings and click View.
3. On the Cookies screen, select Allow cookies based on privacy settings.

The level of privacy must be set to Medium or Low.

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 50)" 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 gray 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 of 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 Console 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 terminal services 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.
Troubleshooting iLO 279

Troubleshooting iLO 279

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 might produce a red X if an unsupported browser or JVM is used, or if Enable All Cookies is not enabled. To correct this issue, ensure you are using a supported browser and JVM on your client by reviewing the support matrix found in the "Supported browsers and client operating systems (on page 15)" section. Also be sure Enable All Cookies is selected on the browser Preferences or Options menu. Some browsers do not enable 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.

How do I access legacy BL p-Class pages?

The previous BL p-Class pages are still accessible by browsing directly to the
following URLs. These URLs are only accessible from within an iLO session. To
access the BL p-Class pages, refer to:

• Rack topology: https://<iLO network address>/dtopo.htm
Troubleshooting iLO

- Server blade management: https://<iLO network address>/dservmm.htm
- Power management module: https://<iLO network address>/dpwrmm.htm
- Redundant power management module: https://<iLO network address>/dpwrsmm.htm

**ProLiant Power Regulator option deactivated**

The system processor determines if the Power Regulator option is supported. The Power Regulator option is only supported on the following servers:

- ProLiant ML350 G4
- ProLiant ML350 G4p
- ProLiant ML320 G3
- ProLiant DL360 G4
- ProLiant DL360 G4p
- ProLiant DL380 G4
- ProLiant DL380 G4p
- ProLiant BL20p G3
- ProLiant ML570 G3
- ProLiant DL580 G3

The system ROM firmware revision date must be dated at least 6/1/05. If your system processor does not support the Power Regulator (different processor p-states), the Power Regulator page displays the **HP Power Regulator for ProLiant not supported by iLO** message.
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 Manager 7 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 20)" 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.
Troubleshooting iLO

- 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 290)" 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](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.

**Enclosure bay static IP changes do not take effect**

For a blade to automatically use enclosure bay static IP, the following must be true:

1. The enclosure bay static IP record must contain a valid IP range.
2. The enclosure bay static IP record must have the respective bay identified as a bay to participate in enclosure bay static IP.
The enclosure bay static IP record will not have a valid IP range for new enclosures. Plugging your servers into this enclosure before setting up the enclosure bay static IP record forces all blades to use the default setting of DHCP. If this happens and you want to use enclosure bay static IP, you must first set up the enclosure bay static IP record on the first blade. After you have set up the enclosure bay static IP record, log in to each of the other blades and modify the network settings to use enclosure bay static IP. You can use either the interface or an XML script. The easiest way to set up each blade is use the front crash cart to log into each blade and make the network modifications.

To use enclosure bay static IP to manage iLO networking:

1. Plug one blade into the first slot of the enclosure leaving the rest of the enclosure empty.
2. Log in to this blade through the front crash cart. The default IP address is 192.168.1.1.
3. Set up the enclosure bay static IP using the blade setup wizard or by canceling the wizard and browsing to the enclosure bay static IP set up tab.
4. Save the settings.

After the settings are saved, other blades can be inserted into the enclosure.

Do not insert other blades into the enclosure until the enclosure bay static IP record has been saved. After the other blades are inserted, iLO initializes its network to the address specified in the enclosure bay static IP record, assuming one of the following:

- The new blade is from the factory and has not had auxiliary power applied to it.
- The new blade was previously using enclosure bay static IP and is being moved to this new enclosure where enclosure bay static IP has been configured.

If either of these statements is false, the iLO network cannot use the customer-expected IP address identified in the enclosure bay static IP record.
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 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.

**Rack view does not display components**

If you continue to receive the *Unable to collect rack data* error message, your firmware in the Management enclosure might need to be updated to version 2.10 or later.

The rack view will not display any rack components if:

1. Two or more blades are trying to view or refresh the Rack View page at the same time. Wait a few moments and try again. Only one blade can load the Rack View page at the same time.
2. Server Management Modules and Power Management Modules must have firmware version 2.10 or later. The latest firmware is available on the HP website (http://h18000.www1.hp.com/support/files/server/us/download/21000.html).

3. The Server Management Modules and Power Management Modules are incorrectly cabled together. Refer to the P-Class Enclosure documentation for cabling instructions.

**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.
Directory services schema

In this section
HP Management Core LDAP OID classes and attributes .......................................................... 293
Lights-Out Management specific LDAP OID classes and attributes ........................................ 298

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 293)
- Core attributes (on page 293)

Core classes

<table>
<thead>
<tr>
<th>Class name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqTarget</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.1</td>
</tr>
<tr>
<td>hpqRole</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.2</td>
</tr>
<tr>
<td>hpqPolicy</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.3</td>
</tr>
</tbody>
</table>

Core attributes

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqPolicyDN</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.1</td>
</tr>
<tr>
<td>hpqRoleMembership</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.2</td>
</tr>
<tr>
<td>hpqTargetMembership</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.3</td>
</tr>
</tbody>
</table>
Core class definitions

The following defines the HP Management core classes.

**hpqTarget**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqTargetIPRestrictionDefault</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.4</td>
</tr>
<tr>
<td>hpqTargetIPRestrictions</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.5</td>
</tr>
<tr>
<td>hpqRoleTimeRestriction</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.6</td>
</tr>
</tbody>
</table>

**hpqRole**

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1</td>
<td></td>
</tr>
<tr>
<td>hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This class defines Target objects, providing the basis for HP products using directory-enabled management</td>
</tr>
<tr>
<td>Class type</td>
<td>Structural</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>user</td>
</tr>
<tr>
<td>Attributes</td>
<td>hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1</td>
</tr>
<tr>
<td></td>
<td>hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
<tr>
<td>OID</td>
<td>1.3.6.1.4.1.232.1001.1.1.2</td>
</tr>
<tr>
<td>Description</td>
<td>This class defines Role objects, providing the basis for HP products using directory-enabled management.</td>
</tr>
<tr>
<td>Class type</td>
<td>Structural</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>group</td>
</tr>
</tbody>
</table>
Attributes

<table>
<thead>
<tr>
<th>Attributes</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqRoleIPRestrictions</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.5</td>
</tr>
<tr>
<td>hpqRoleIPRestrictionDefault</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.4</td>
</tr>
<tr>
<td>hpqRoleTimeRestriction</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.6</td>
</tr>
<tr>
<td>hpqTargetMembership</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.3</td>
</tr>
</tbody>
</table>

Remarks

None

hqpPolicy

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

hqpPolicyDN—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.

hqpPolicyDN

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

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a list of hpqTarget objects to which this object belongs.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

hpqTargetMembership

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a list of hpqTarget objects that belong to this object.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

hpqRoleIPRestrictionDefault

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A Boolean representing access by unspecified clients which partially specifies rights restrictions under an IP network address constraint</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean—1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>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.</td>
</tr>
</tbody>
</table>
**hpqRoleIPRestrictions**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Provides a list of IP addresses, DNS names, domain, address ranges, and subnets which partially specify right restrictions under an IP network address constraint.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Octet String—1.3.6.1.4.1.1466.115.121.1.40</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>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.</td>
</tr>
</tbody>
</table>

- 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 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 0x6E 0x6F 0x62 0x73 0x61 0x6C 0x6F 0x63 0x68 0x6F 0x64 0x65 0x61 0x6C 0x69 0x76 0x65>`.

**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

<table>
<thead>
<tr>
<th>Class name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqLOMv100</td>
<td>1.3.6.1.4.1.232.1001.1.8.1.1</td>
</tr>
</tbody>
</table>

#### Lights-Out Management attributes

<table>
<thead>
<tr>
<th>Class name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqLOMRightLogin</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.1</td>
</tr>
</tbody>
</table>
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
| 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 |

---

### Directory services schema

<table>
<thead>
<tr>
<th>Class name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqLOMRightRemoteConsole</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.2</td>
</tr>
<tr>
<td>hpqLOMRightVirtualMedia</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.3</td>
</tr>
<tr>
<td>hpqLOMRightServerReset</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.4</td>
</tr>
<tr>
<td>hpqLOMRightLocalUserAdmin</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.5</td>
</tr>
<tr>
<td>hpqLOMRightConfigureSettings</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.6</td>
</tr>
</tbody>
</table>
## Lights-Out Management attribute definitions

The following defines the Lights-Out Management core class attributes.

### hpqLOMRightLogin

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Login Right for HP Lights-Out Management products</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean—1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>Meaningful only on ROLE objects, if TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>

### hpqLOMRightRemoteConsole

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Remote Console Right for Lights-Out Management Products. Meaningful only on ROLE objects.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean—1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>

### hpqLOMRightVirtualMedia

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Virtual Media Right for HP Lights-Out Management products</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean—1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>
### 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. |
Technical support

In this section
HP contact information......................................................................................................... 303
Before you contact HP ........................................................................................................ 303

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 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  – If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com).
• 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
CLP
command line protocol

CR
Certificate Request

CRL
certificate revocation list

DAV
Distributed Authoring and Versioning

DDNS
Dynamic Domain Name System

DHCP
Dynamic Host Configuration Protocol

DLL
dynamic link library

DMTF
Distributed Management Task Force

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

ISIP
Enclosure Bay Static IP

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

SMASH
System Management Architecture for Server Hardware

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
VLAN
virtual local-area network

VM
Virtual Machine

VPN
virtual private networking

WINS
Windows® Internet Naming Service

XML
extensible markup language
Index

A
accessing software, browser 15, 19, 24
acquire, remote console 58
Active Directory 166
ActiveX 152, 270
administration 86, 99, 245
alert and trap problems 268
alert messages 116
alerts 95, 240
ASR (Automatic Server Recovery) 305
authorized reseller 303
automatic certificate request 214
Automatic Server Recovery (ASR) 305

B
BL p-Class blade server 26, 104, 115, 282, 287, 290
blade configuration 31, 108
blade information 108
boot options 18
Browser-Based Setup 19
browsers, supported 15
bulk import tools 202

certificate services, overview 147, 213
certificates 99, 147, 265
certificates, installing 213, 265
CGI, software components 59
composite device support 59, 80
configuration options 17, 18, 19, 26, 32, 54, 93
configuration parameters 26, 28, 30
configuring the LOM processor 32
connection overview 13
contacting HP 303
cursor modes 56

D
data protection methods 240
definitions 117
device drivers, installing 20, 21, 22
DHCP (Dynamic Host Configuration Protocol) 306
directory authentication, two-factor
authentication 143
directory integration, benefits 151
directory integration, operation 151
directory integration, overview 151
Directory Services for eDirectory 184
Directory Services Objects 177, 178, 191, 192
Directory Services, integration 151, 157
directory services, verifying 199
Directory-Enabled remote management 201
disk image files 79
diskette, changing 74
display settings 290
domain/name login 270
dual-cursor 56

e
eDirectory 184
enabling 23, 24, 151
closure information 109
error messages 270
event log 43
event log entries 256

F
features 11, 14, 135, 151, 158
Firefox 15
firmware, updating 284

G
global settings 86, 89
Graphical Remote Console 47
groups 203
H

hardware troubleshooting 260
help resources 303
high performance mouse 51
host server troubleshooting 291
hot-plug keyboard 117, 118
HP Extended schema 151, 153, 157, 227
HP ProLiant Essentials Rapid Deployment Pack 134
HP schema directory integration 158
HP Technical Support 303
HPQLOMGC 232
HPQLOMIG 156, 220, 231

I

iLO Advanced Functionality 23, 24, 242
iLO RBSU (Integrated Lights-Out ROM-Based Setup Utility) 18
image files, disk 79
IML (Integrated Management Log) 43
initial access 39
Insight Manager 7 237, 238, 240
Insight Manager 7 integration 237, 238
Insight Manager, iLO identification 240
installation overview 158, 166
installing software 22
integration with RILOE II 37
IP addresses, setting up 31

L

Linux, End-to-End 86
login, failure 261, 267
login, two-factor authentication 141

M

management processors 225
Microsoft procedures 20, 47, 59
Microsoft software 151, 166
Microsoft support 14
minimum requirements 15, 253
mounting virtual media 72, 77, 78
mouse 271, 272, 273
mouse problems 271
mouse settings 271, 273
mouse settings, high performance 51
Mozilla settings 15
multi-device support 80

N

NetWare server support 14, 21, 47, 59
network component information 115
network settings 86
NIC (network interface controller) 309
Novell NetWare 21

O

operating systems supported 253
operational overview 11, 12, 13, 22, 151, 213, 238
optimizing performance 50, 52, 53
options installation 23, 24
overview, directory integration 151, 153

P

phone numbers 303
port matching 250
port settings 129, 132
power button 59
power management 111, 113
power regulator 62
powering on/off 60
preinstallation, guidelines 154, 161, 166
preinstallation, overview 20, 21, 22
preparation procedures 167

R

rack resources 106, 109, 111, 113, 115
rack settings 104
Rack View 106, 290
RAID configuration 34
RBSU (ROM-Based Setup Utility) 18, 133
RBSU Erase Option 291
<table>
<thead>
<tr>
<th>Index</th>
<th>315</th>
</tr>
</thead>
</table>

- **rear panel connectors**: 104
- **remote console**: 47, 48, 49, 50, 52, 53, 54, 56, 125, 273
- Remote Console Information option: 48
- remote console, acquire: 58
- remote console, enhanced features: 49
- Remote Console, troubleshooting: 273, 274, 275, 276
- remote host: 43, 54, 104, 120, 240, 249, 291
- required information: 303
- required software: 14, 15, 65, 161
- resetting to defaults: 290
- Restore Factory Presets: 290
- restoring: 284, 290
- ROM-Based Setup Utility (RBSU): 18, 133, 148, 263

**S**
- schema documentation: 160, 293, 298
- schema installer: 161, 162, 165
- schema-free integration: 154
- schema-free options: 156
- schema-free, setup: 155, 156, 229, 231
- scripted setup: 22
- scripts: 59
- security enhancements: 146
- security features: 135, 136
- security settings: 135, 146, 148
- serial BREAK: 85
- serial port: 83, 85
- server status: 41
- server warnings and cautions: 240, 249
- settings: 52, 53, 100, 102, 151, 156, 197, 199
- setup, browser-based: 17, 19, 24, 39, 132, 155
- setup, schema-free: 155, 156
- setup, scripted: 17, 134, 155
- shared network port, features: 128
- shared network port, requirements: 127
- shared network port, restrictions: 128
- single-cursor: 56
- SLES procedures: 15, 47, 59, 271, 273
- Snap-In installer: 165, 169, 176, 177, 178, 185
- SNMP alerts: 95, 116, 240, 249
- SNMP settings: 86, 94
- software installation: 36
- software supported: 14
- software troubleshooting: 260
- SSH (Secure Shell), requirements: 127
- SSL connection: 147
- support: 303
- supported hardware: 62, 127
- supported operating systems: 14, 15
- supported software: 14, 15
- System Erase Utility: 291
- system status: 40, 42, 43, 44, 45, 46
- Systems Insight Manager: 246, 247, 248, 249, 250

**T**
- technical support: 303
- telephone numbers: 303
- telnet, using: 278
- Terminal Services: 120, 121, 122, 123, 124, 125, 277
- Terminal Services, troubleshooting: 277, 278
- timeout, Virtual Media: 82
- two-factor authentication: 138
- two-factor authentication, directory authentication: 143
- two-factor authentication, first time use: 138
- two-factor authentication, login: 141, 268
- two-factor authentication, setup: 138
- two-factor authentication, user certificates: 143

**U**
- UnitedLinux procedures: 47, 59, 271, 273
- updating drivers: 20, 22
- updating the firmware: 98
- usage model: 12, 118
- user access: 40, 145, 196, 209
- user accounts: 145
- user certificates, two-factor authentication: 143
- user contexts: 271
user profile 145
user roles 178, 180, 181, 192, 193, 204, 206,
       207, 208, 209, 210
user settings 145
using virtual media 59, 60, 65, 68, 72, 77, 78,
       82, 84, 279
utilities 220, 232

V
video problems 278
virtual CD-ROM 77, 78, 279
virtual devices 66
virtual floppy 65, 72, 279
virtual indicators 82
Virtual Media 35, 65, 66, 68, 72, 77, 78, 82,
       279
virtual media image files 59
virtual power 60, 62, 65
Virtual Power button 65
Virtual Serial port 83, 84, 86
VLAN information 132
VLAN, browser-based configuration 132
VLAN, configuration 132, 133, 134
VLAN, RBSU configuration 133
VLAN, scripted configuration 134
VLAN, shared network port 132

W
website, HP 303
Windows server support 14, 20