HP Industry Standard Servers

June 2003

Best Practice TC030606BP

Best Practices for Integrated Lights-Out

Table of contents

Abstract.. 2
Introduction.. 2
Planning.. 2
Management network.. 3
Out-of-band management.. 4
iLO configuration.. 4
Enhancing security.. 5
Networks with proxy servers.. 8
Remote Console performance.. 10
Integration with Insight Manager 7.. 12
Managing multiple iLO devices.. 13
Deploying headless servers.. 17
Unattended server deployment.. 17
Deploying servers using Rapid Deployment Pack.. 18
Virtual Media/USB support.. 19
Using RILOE-II in an iLO server.. 19
Linux tips.. 19
For more information.. 19
Feedback.. 19
Appendix A: Barcode scanning.. 21

Abstract

This document identifies specific practices for using the Integrated Lights-Out (iLO) management processor to reduce complexity and simplify management of the datacenter and remote sites. HP recommends that customers implement these practices if appropriate for their unique IT infrastructure. These practices may not be applicable in all situations, depending on the unique environment of the customer.

Introduction

The iLO device is an autonomous management processor that resides on the system board of a host server. It contains its own processor, memory, and network interface that allow it to operate independently from the host server. Using iLO, IT administrators can manage a ProLiant server remotely through its entire life cycle: initial deployment, operation, and redeployment. Unlike other management solutions, iLO devices are entirely independent of the state of the operating system (OS) or server hardware. They provide seamless control of remote servers in full graphics mode (when using the iLO Advanced feature set). The Virtual Media feature of iLO allows IT administrators to perform remote ROM upgrades and server deployments. All these capabilities combine to provide administrators the ability to respond quickly to downtime events, diagnose OS or server problems remotely, increase uptime, and reduce the loss of business revenue.

This paper discusses best practices in system planning, deployment, and operation of iLO management processors. It is assumed that the reader is familiar with the general features of iLO. More information about iLO is available from the website at**:** http://www.hp.com/servers/ilo

Planning

Before deploying and configuring an iLO device, it is helpful to assess the IT environment. Table 1 outlines areas to consider when planning the use of lights-out technology.

Table 1. Assessing the IT Environment

Environment Factor	Assessment Criteria	Potential for Improvement
Asset management	Where are servers located (in datacenters or at remote sites)? Where would it be helpful to use iLO? How many servers exist in the computing environment?	Deploying iLO can eliminate the need for keyboards, video monitors, and mice, which reduces cabling complexity and increases server density in the datacenter.
Systems management	How are remote sites and data center servers currently managed? Can the servers be managed remotely through lights-out technology?	The iLO device provides seamless access to the server, which eliminates the need for an administrator to be present in front of the server.
Security	Is the network as secure as possible? Does the datacenter use virtual private networks or include firewalls? Can all servers use directory services and authentication?	The iLO device provides multiple levels of security, including directory authentication, Secure Sockets Layer (SSL) encryption, event generation for failed login attempts, lockout of configuration utilities, enforced delay after unsuccessful login attempts, and configurable internet protocol (IP) port assignments.

When planning future server purchases, a customer can determine whether a server includes iLO by referring to this webpage: http://h18013.www1.hp.com/products/servers/management/riloe2/supported-servers.html.

Customers that have a large installed based of iLO devices and frequently add more may want to purchase a Master License Agreement (MLA) from HP. An MLA allows the customer to purchase a single activation key for multiple licenses of the ProLiant Essentials Value Packs, such as the iLO Advanced Pack. After the MLA is in place with HP, the customer purchases the desired number of license-only part numbers whenever they need additional licenses for iLO Advanced. This simplifies the software licensing process and reduces the amount of physical documentation that is shipped to the customer. Additional information is available from the website at: http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/licensing.html.

Management network

Before deploying iLO devices, an administrator should consider the setup and design of the network on which the iLO devices will reside.

The iLO devices allow browser access to the host ProLiant servers through a seamless, hardware-based, OS-independent Remote Console. For security reasons, HP recommends that customers establish a private management network that is separate from their data network and that only administrators be granted access to that management network.

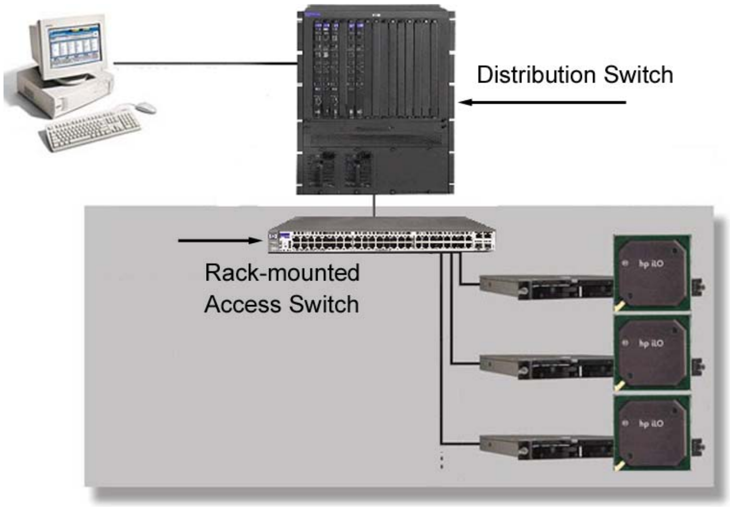
Network cabling in dense rack environments

When deploying multiple iLO-enabled servers in very dense rack environments, it is beneficial to consolidate all of the iLO network connections to a rack-mounted hub or access switch (Figure 1). The administrator may then uplink all Lights-Out Management network traffic via a single output from the hub/switch into a distribution switch in the enterprise network infrastructure.

Using an access switch for Lights-Out Management network traffic provides the following benefits:

- Simplifies cable management inside the rack
- Makes more efficient use of available bandwidth
- Reduces the number of network cables run to the rack for management traffic
- Reduces usage of more expensive enterprise network infrastructure ports

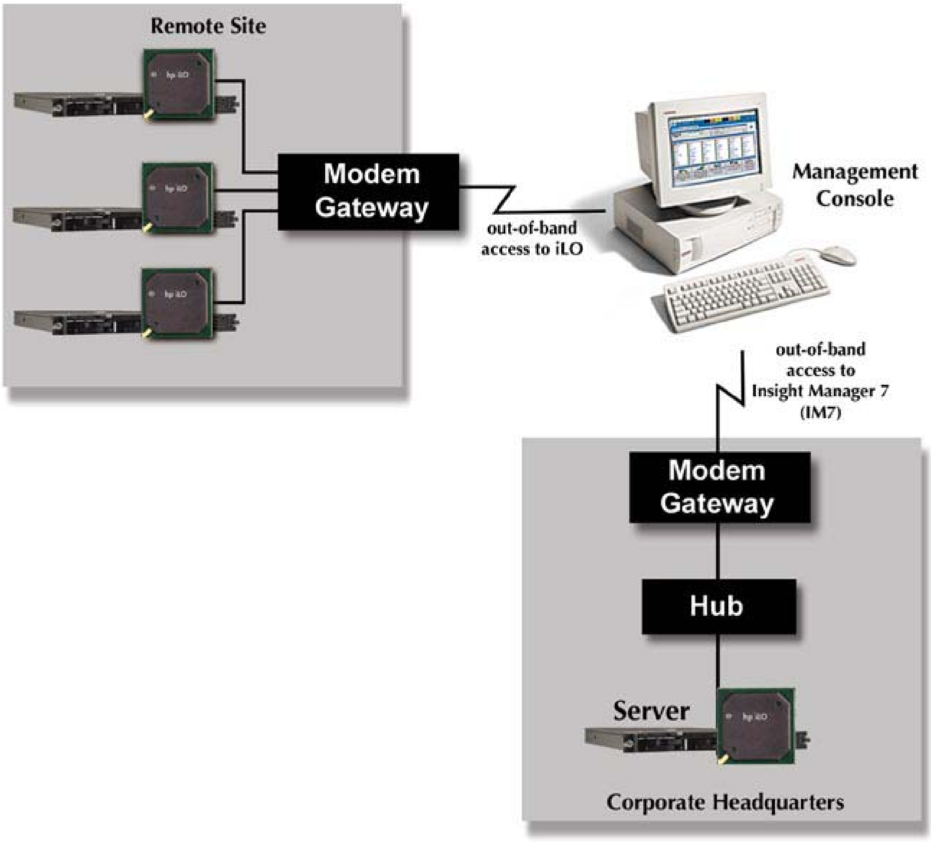
Figure 1. Consolidating multiple iLO devices into a single rack-mounted access switch



Out-of-band management

An iLO device can be used for remote management even if there is no Ethernet local area network (LAN) connection to the host server located at a remote site. IT administrators can use a modem gateway or a remote access server (RAS) login into the local LAN to enable out-of-band (dial-up) access to the host server. If there were multiple servers at the remote site, this solution would require only one telephone line to access all iLO devices installed at that site (Figure 2).

Figure 2. Example of out-of-band access configuration



iLO configuration

Each iLO device can be configured individually in one of three ways: through the ROM-Based Setup Utility (RBSU), through the web browser interface, or through a scripted setup.

Single iLO device

RBSU is the recommended method to set up a single iLO device initially. After the iLO device has been set up, it should be available on the network; and subsequent configuration and management can be done through the web browser or a script. RBSU is available every time the server is booted and may be run remotely using the iLO Remote Console. RBSU is not intended for continued administration. Other tools such as the web browser or scripting tools are better suited for that.

See the iLO User Guide for more information about each of the three configuration methods (http://www.hp.com/servers/ilo).

Multiple iLO devices

Manually deploying a large number of iLO-enabled servers is a time-consuming task. HP has developed samples of XML script files that can be used along with the Lights-Out Configuration Utility (`CPQLOCFG.EXE`) to allow administrators to configure and manage user accounts on multiple iLO devices simultaneously. Additionally, HP developed sample Perl scripts for use with a Perl interpreter that communicates with iLO directly.

Both `CPQLOCFG.EXE` and the sample scripts files are available from the website at http://www.hp.com/servers/ilo . The `CPQLOCFG.EXE` version 2.0 or greater must be used for iLO devices.

HP recommends that administrators use these sample files and a bar code reader to scan all the passwords and Domain Name System or Service (DNS) names from the network settings tag into a spreadsheet or database. (An administrator can manually enter the passwords and DNS names into a spreadsheet; however, it is much more time-consuming and error-prone than scanning.) Then, using the appropriate XML script, the administrator can configure the group of iLO devices, add the license keys for the iLO Advanced functionality, upgrade firmware on the iLO devices, add a new user, or change user privileges. For example, if a customer established an MLA for the iLO Advanced Pack, the administrator could use an XML script to add the license keys for all applicable ProLiant servers.

Administrators can expand or change the sample XML scripts to perform other functions such as to power up or down servers or determine who has access rights to iLO. The iLO User Guide includes the supported XML commands for additional script development.

The administrator must have `CPQLOCFG.EXE` or a Perl interpreter, DHCP server and appropriate XML scripts; and HP recommends using a bar code scanner to reduce deployment time. Appendix A includes additional information about how to use the sample Perl and XML script files.

Naming conventions

When deploying many iLO devices, it is helpful to name them according to a consistent convention, for example: ServerName_iLO. This convention clearly identifies which server is hosting the iLO device and makes it easier to set up proxy settings for wildcard usage.

Enhancing security

Because they are completely autonomous and can be used to control the server, iLO devices should be treated is if they were servers. For example, the administrator should include the iLO devices in the security and network audits and should review the access logs daily.

Change the default login password

Each iLO device comes with a network settings tag that shows the default password for that device. The default password is a randomly generated, eight-character, alphanumeric string. It should be changed immediately to a more relevant password. The iLO management passwords should be changed with the same frequency and according to the same guidelines as the server's administrative passwords.

In the event that login passwords are lost or forgotten, there is a way to temporarily override the security of iLO. In servers with an iLO device, there is an iLO Security Override Switch on the system board. This switch temporarily disables authentication security, allowing a user to log in without using a password. It does not give a user read access to existing passwords or erase any existing account information, but it does allow that user to change existing passwords, add user accounts, or delete user accounts.

To change the state of the iLO Security Override Switch, an administrator must have physical access to the inside of the server. Depending on the server, the iLO Security Override Switch may be a single jumper or a specific switch position on a dipswitch panel. Refer to the server documentation to locate the iLO Security Override Switch.

Implement directory access

An administrator can implement directory services to improve security. Directory services (available in iLO firmware version 1.40) allow an administrator to authenticate a user and authorize user privileges by means of the same login process employed throughout the rest of the network. By using the same login process (password), security is enhanced because an end-user no longer needs to remember (or write down in a non-secure area) a separate password for iLO access. Similarly, because the directory provides a way to control multiple iLO devices simultaneously, an administrator can perform maintenance functions such as changing passwords, disabling accounts, or adding accounts, just once rather than multiple times. This reduces the risk of an administrator making an error as he or she performs the same function repeatedly.

Directories provide role-based access to iLO. An administrator can define specific roles and privileges to restrict iLO access for certain users. Restrictions can be as tightly controlled as allowing certain users, from specifically identified workstations, during certain times of the day. When setting up the user roles, it is important for the administrator to consider carefully how the roles interact with each other and with the devices. Characterizing the roles carefully can reduce the possibility of accidentally giving user privileges to an unauthorized user.

Using directory access can also provide greater protection against malicious attacks on the network. If a hacker were to try to log in to iLO using a local account, after several unsuccessful tries, the iLO would lock the hacker out of the login process. However, there is nothing to prevent this same hacker from trying other iLO devices on the network. With directory services, a hacker would have only a single access point to multiple iLO devices, thus reducing the chance that a hacker would be able to login to any iLO device.

Because the directory accounts provide these security benefits, an administrator using directories may want to disable local accounts or remove them entirely. For more information about directory services, see the section titled “Directory services” later in this paper.

Restrict access to the Remote Console port

The Remote Console port (port 23) allows an authorized user to establish a Remote Console session with the host server. To provide tighter security, a user with supervisor rights can restrict access to the Remote Console port and can turn on Remote Console encryption. Three options are available for access to the Remote Console port:

- The Remote Console port is always disabled. A user trying to access the Remote Console will always be denied access when this setting is in place. This provides the highest security, but it may not allow adequate management capabilities.
- The Remote Console port is set to "auto-enable," which is the default setting for the Remote Console port. This setting disables the port except when iLO senses the Remote Console applet starting. In that case, iLO automatically enables the Remote Console port and automatically disables it when the Remote Console session has ended. The auto-enable setting allows only Remote Console sessions to connect to port 23.
- The Remote Console is enabled. An authorized user can access the Remote Console port at any time. This allows a Telnet connection or a Remote Console applet connection to be made to the Remote Console port.

For maximum security when the Remote Console is enabled, HP recommends that the administrator turn on the Remote Console encryption.

For maximum security for customers who do not require the Remote Console feature, HP recommends disabling the Remote Console port.

NOTE: Because Telnet sessions connect to port 23, an administrator that has disabled the Remote Console port or set the Remote Console port to auto-enable will not have Telnet support. Telnet support is available only when the Remote Console port is enabled and Remote Console encryption is disabled.

To configure the availability of the Remote Console port, complete the following steps:

1. Log on to the iLO management device using an account that has supervisor status
2. In the Administration section, click **Global Settings.**
3. In the **Remote Console Port Configuration** section, click the appropriate option.

Protect SNMP traffic

Because SNMP uses passwords (known as community strings) that are sent across the network in clear text, it is important to enhance the network security when using SNMP traffic. Here are two suggestions:

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

Networks with proxy servers

If the client web browser software is configured to use a proxy server, the administrator may be prompted for a username and password before a Remote Console session begins. Each iLO device can be accessed by its short name (for example, remote21), fully qualified name (for example, remote21.domain.com), or Internet protocol (IP) address. The browser needs to be configured to bypass the proxy server for each method used to access the iLO device.

Browser configuration

To configure Microsoft® Internet Explorer 5.5 (SP2) or above:

1. Click on Tools, Internet Options, and then Connections.
2. Click on **LAN Settings** (or the appropriate dial-up or VPN connection and click **Settings**). Make sure that the Bypass proxy server for local addresses box is checked. This will ensure that short names will not use a proxy server.
3. Click on **Advanced**. The Proxy Setting window will appear.
4. Under **Exceptions**, enter the IP address and/or the fully qualified name of the iLO device.

Wildcards can be used to indicate all addresses within a certain domain, (for example, *.domain.com or 199.199.199.*). When an attempt to access a website is made, Internet Explorer crosschecks that address with a list to determine if a proxy server should be used. If a proxy server is not required to access external Internet sites, uncheck the "**Use a proxy server**" box. The **Advanced** settings can then be skipped.

To configure Netscape Navigator 6.2 or above:

1. Click on **Edit** and then on **Preferences**.
2. Click on the **+** next to **Advanced** and then on **Proxies**.
3. Click on the radio button next to **Manual proxy configuration**.
4. Click on **View**.
5. In the **Exceptions** list, add the names, domain names, or IP addresses of the iLO device. Netscape Navigator does not support the use of wildcards.
6. If a proxy server is not required to access external Internet sites, click on the radio button next to Direct connection to the internet. The Exceptions list can then be skipped.

To configure Mozilla1.0 or 1.1, follow the same steps used for Netscape Navigator. To use a Mozilla browser with the Linux OS , set the browser to use 12-point font to improve screen legibility.

Configuring IP port assignments

Administrators can manually configure the Hypertext Transfer Protocol (HTTP), Remote Console, and Virtual Media ports used by the iLO device. Normally, a web browser automatically attempts to connect with port 80 when given an IP address. Using the port configuration capability, the administrator can redirect the HTTP, Remote Console, and Virtual Media ports to administrator-defined ports, so that others cannot access the HTTP, Remote Console, and Virtual Media ports without specific knowledge of the port numbers. Once the HTTP port is re-directed, a user would need to specify that port along with the IP address to access the login screen. This feature may be particularly useful for customers who wish to access iLO through a firewall and use Insight Manager 7 as the data collection vehicle for port changes.

Unlike most of the other ports, the Lightweight-Directory Assisted Protocol (LDAP) port is a client port, which means that nothing will ever connect to port 636 of the iLO device. Instead, the iLO device will be connecting to port 636 of a directory server (see the section titled "Directory services" for more information on directories). Therefore, routers that use port filtering will need to be set up to forward the directory traffic coming from iLO. LDAP traffic from a directory server uses random port numbers to enter the iLO device.

Trouble-shooting Tip: For an iLO device to work properly when going across routers using port blocking and/or firewalls, ports 23, 80, 443, and 17988 must be open. Port 23 is for the Telnet ports where the remote and graphical Remote Console is used, port 80 is for HTTP communications, port 443 is required for the SSL connection, and 17988 is for Virtual Media. The inability to access the iLO management ports is often confused with incorrect proxy settings. When in doubt, disable proxy in Internet Explorer or Netscape. Table 2 identifies default port locations and information about resetting ports to allow access.

Table 2. Default port locations for iLO

Port Number	Protocol	Can be Changed	Supports	Enabled
23	Telnet	Yes	Remote Console	Yes
80	Remote Insight port	Yes	HTTP interface to lights-out management board	Yes
161	SNMP get/set	No	Insight Manager 7 polls	No
162	SNMP trap	No	Insight Manager 7 agent events	No
443	Remote Insight encrypted port	Yes	SSL access to lights-out management board	Yes
636	Lightweight Directory Assisted Protocol (LDAP)	Yes	Secure connection to the directory server	Yes, if directory support is enabled
17988	Virtual Media	Yes	Virtual Media	Yes

Remote Console performance

The graphical Remote Console operates better when the host server and client browser settings have been optimized for certain OS conditions. Ideally, the screen resolution of the host server OS should be the same, or lower, than that of the client browser. For example, if the client browser uses a resolution of 1024x768, then the host server screen resolution should be no greater than 1024x768. The higher the resolution of the host server, the slower the overall performance.

Host server settings: Windows

HP recommends these settings for a host server using Windows NT® 4.0, Windows® 2000, or Windows Server 2003.

Server Display Properties

- Plain Background (no wallpaper pattern)
- Smaller display resolutions (800x600 or 1024x768 pixels)
- 256 color mode or 24 bits per pixel color setting

Server Mouse Properties

- Select **None** for mouse pointer **Scheme**.
- Uncheck **Enable pointer shadow**.
- Select **Motion** or **Pointer Options** and set the pointer **Speed** slider to the middle position.
- Disable pointer **Acceleration** to None (on Windows NT or Windows 2000).
- Uncheck **Advanced Pointer Precision** (on Windows Server 2003).

Host server settings: Linux

HP recommends these settings on a host server using RedHat Linux or SuSE Linux Server:

Server Display Properties

- Screen resolution of 1024x768 pixels or lower
- 256 color mode

Server Mouse Properties

- Set Pointer Acceleration to 1X.
- For KDE, access the Control Center, select **Peripherals/Mouse**, and then select the **Advanced** tab.

Host server settings: Novell NetWare

HP recommends these settings on a host server using Novell NetWare:

Server Display Properties

- Screen resolution of 800x600 pixels or lower
- 256 color mode

Client and browser settings

The speed of the Remote Console is dependent on the processing power of the client machine. For best Remote Console speed, HP recommends using a 700-MHz or faster processor with minimum of 128 MB of memory. To improve execution of the Remote Console Java applet, HP recommends using a single processor client. It is also important to ensure that the client Remote Console applet can display the entire host server screen.

HP recommends that users implement these settings on the client to optimize performance:

Display Properties

- Select a display resolution greater than the resolution of the host server.
- Select an option greater than 256 colors.

Mouse Properties

- Set the pointer **Speed** slider to the middle setting.
- Set the **Mouse Pointer Acceleration** to **low,** or disable the mouse acceleration.

HP recommends Microsoft Internet Explorer, version 5.5 or later and Java 1.3.1 Java Virtual Machine (JVM). Additional browsers may or may not work correctly, depending on the OS and specific implementations.

Dual-cursor mode

HP recommends using the Remote Console dual-cursor mode for text-based operating systems. Administrators may also prefer the dual-cursor mode because it allows them to see where the cursor exits the Remote Console applet window.

The dual-cursor mode uses two mouse cursors that represent the host server’s mouse cursor (seen as the standard cursor) and the local client’s mouse cursor (seen as a crosshair in the Remote Console window). The dual-cursor mode is supported with Java 1.1 JVM and later.

If the two cursors drift apart, they can be synchronized and brought back together. Use any of the following techniques to synchronize the remote and local cursors:

- Right-click-drag and move the local crosshair cursor to align with the remote server's mouse cursor.
- Holding the **Ctrl** key, move the local crosshair cursor to align with the remote server's mouse cursor.
- Set the speed of the mouse cursor to the middle setting. Set the mouse cursor Acceleration to **low**, or disable acceleration entirely.

Single-cursor mode

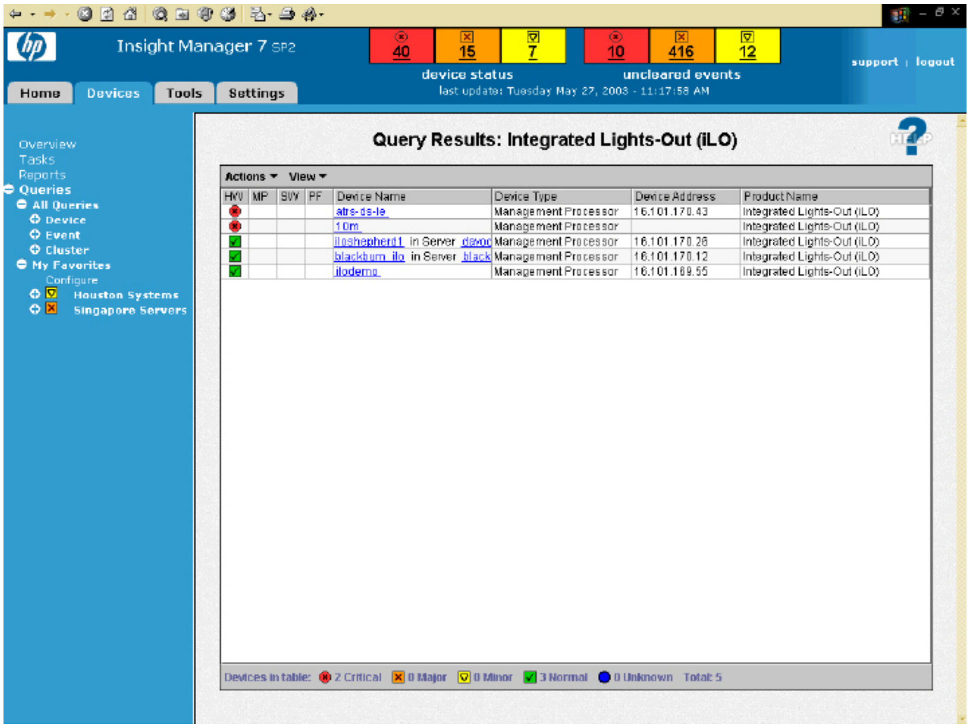
The single-cursor mode eliminates the need to synchronize two cursors, which makes navigation easier in the Remote Console window. To enable the single mouse cursor, the administrator must install the Sun Java Plug-in Version 1.3.1 or greater. The Java Virtual Machine applet must be downloaded and installed on the client machine. It is available at http://www.hp.com/servers/manage/jvm.

NOTE: The URL will redirect you from the Lights-Out management website to the java.sun website for the latest version available. However, HP recommends using the version specified in the Remote Console Help (available from the iLO browser interface).

Integration with Insight Manager 7

The Insight Management Suite and management agents are tightly integrated with iLO, allowing administrators to view subsystem and status information from a web browser. Furthermore, an administrator can use the query mechanism of Insight Manager 7 to discover each iLO device and store it on a device list. The device list provides direct hyperlink access to each iLO device (see Figure 3), giving the administrator the benefit of having a single location for accessing all Lights-Out management devices (including Remote Insight Lights-Out Edition II, or RILOE II).

Figure 3. Device list in Insight Manager 7



last update: Tuesday May 27, 2003 - 11:17:58 AM

Query Results: Integrated Lights-Out (iLO)

HW	MP	SW	PF	Device Name	Device Type	Device Address	Product Name
●				atrs-ds-le	Management Processor	16.101.170.43	Integrated Lights-Out (iLO)
●				10m	Management Processor		Integrated Lights-Out (iLO)
✓				iloshepherd1 in Server davoc	Management Processor	16.101.170.26	Integrated Lights-Out (iLO)
✓				blackburn_ilo in Server black	Management Processor	16.101.170.12	Integrated Lights-Out (iLO)
✓				ilodemo	Management Processor	16.101.169.55	Integrated Lights-Out (iLO)

Devices in table: ● 2 Critical ☒ 0 Major ▽ 0 Minor ✓ 3 Normal ● 0 Unknown Total: 5

The administrator can configure the iLO device for proactive management by allowing SNMP trap delivery to Insight Manager 7. Up to three TCP/IP addresses can be configured to receive SNMP alerts. Typically, the administrator configures one address to be the same as the TCP/IP address of the Insight Manager 7 server console, while the others can be backup monitoring consoles.

If the administrator has changed the ports that the iLO device uses, some modifications must be made to Insight Manager 7 to be able to discover these new ports. To customize the port scans used by Insight Manager 7, follow these steps:

1. Open Windows Explorer on the server running Insight Manager 7.
2. Navigate to the installed directory for Insight Manager 7 (typically, this is located at c:\Program Files\Compaq\ Insight Manager 7\).
3. Navigate to the \config\additionalWsDisc.props file and open the file with Notepad or another text editor.
4. Follow the directions in the .props file to change the ports discovered by Insight Manager 7.

Managing multiple iLO devices

Administrators can manage iLO devices as a group rather than one at a time. For example, an administrator can change the user access rights and privileges, add or delete users, update passwords, or update firmware for an entire group of iLO devices. Groups of iLO devices can be managed using Insight Manager 7, using CPQLOCFG.EXE and script (batch) files, using CPQLODOS, or using directory services.

Insight Manager 7

Managing multiple iLO devices can be done through Insight Manager 7 by using the following components:

- Remote Insight board Command Language (RIBCL) – an XML-based scripting language
- Lights-Out Configuration Utility (CPQLOCFG.EXE). This utility must reside on the same server as Insight Manager 7. The iLO device must be upgraded to firmware version 1.10 (or higher) before using this utility. CPQLOCFG.EXE version 2.0 is used for group configuration of iLO. Previous versions of CPQLOCFG support only RILOE.
- Query Definition in Insight Manager 7
- Application Launch in Insight Manager 7

These components allow an administrator to perform group management of lights-out boards. An administrator can also use RIBCL to write scripts that remotely perform a multitude of operations on many servers. For example, an administrator might write a script to remotely upgrade the system BIOS for every server in a rack. The script might instruct the iLO device in each server to do the following: power down the server, download the new BIOS, and then power up the server. With XML-based remote scripting capabilities, every function or task an administrator can do using Lights-Out technology and a web browser can also be done in a secure environment through an XML script running at a remote site.

The administrator would perform the following steps to perform a task on a group of iLO devices:

1. Write a RIBCL script file to perform the desired management tasks (such as add a user, delete a user, or change a user profile). Sample scripts are provided in Appendix B of the iLO User Guide.
2. Perform a device query on iLO devices in Insight Manager 7 and save the query list.
3. Set up an Application Launch Task to start CPQLOCFG.EXE on all iLO devices listed in the Insight Manager 7 Management Processor query. The Application Launch can be executed on demand or can be scheduled to run automatically at a specific date and time.
5. Specify the script file, query list, and log file destination as parameters to the launch task. Through Insight Manager 7, CPQLOCFG sends a RIBCL file to a group of iLO devices to manage their user accounts.
6. The iLO devices then perform the action designated by the RIBCL file and send a response to the log file.

When Insight Manager 7 performs a query, it is important to consider that various levels of information may be returned, depending on how each iLO device was configured. There are four levels of iLO identification:

- **High** – associations are present and all data are present on the summary page.
- **Medium** – associations are present but the summary page contains less detail. This is the default setting for iLO.
- **Low** – associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.
- **None** – no data is returned to Insight Manager 7.

The most secure level is "None"; however, it eliminates all data returned from an Insight Manager 7 query. The default iLO setting is "Medium." To allow Insight Manager 7 to discover Lights-Out devices and to associate these devices with the host server, the iLO device must be configured to return "High" or "Medium" amounts of data. The administrator can configure this setting on the SNMP/Insight Manager Settings page and preview the data to be returned at the various configuration settings.

CPQLOCFG.exe and script files

HP has developed sample script files that can be used along with `CPQLOCFG.EXE` to allow administrators to configure and manage user accounts on multiple iLO devices simultaneously. These are described in the previous section "iLO configuration" and in Appendix A.

CPQLODOS

CPQLODOS is a command-line, host-side configuration utility that is typically used only for the initial configuration of iLO devices. The utility generates a hardware configuration script file that can be used to duplicate the iLO configuration from a source server onto a target server. The iLO DOS Utility is required only for customers who want to use the SmartStart Scripting Toolkit on servers that include an iLO device. For example, an administrator at a central location may want to use the SmartStart Scripting Toolkit to bring a set of iLO devices to a baseline configuration of username and password. Then, when the iLO devices are deployed at remote sites, the local IT administrator can use other methods such as CPQLOCFG to perform detailed configuration over the network.

The CPQLODOS utility is not intended for continued administration; also, it is not supported on Linux operating systems or when using the Novell NetWare Client. Additional information about this tool is available from the iLO User Guide.

Directory services

Administrators that have upgraded to iLO firmware version 1.40 (to be available in 3Q '03) and greater can use directory services to authenticate user access and authorize user privileges for groups of iLO management processors. This is beneficial for customers that are already using directories in their network environment and want to integrate their iLO devices into that management scheme.

The HP directory-enabled remote management products currently support Microsoft Active Directory running on Windows 2000 and Windows Server 2003, in addition to Novell eDirectory running on Windows 2000, NetWare 6.0, or Red Hat Linux 7.2/7.3. Detailed information about how to set up directory services is available in the iLO User Guide version 1.40. More information is also available in the paper titled *Directory-enabled Lights-Out Management*, document number TC030601WP.

Required software

To enable directory services, customers must have iLO firmware version 1.40 or greater, the iLO Advanced feature set, and the HP Smart Component installation software. The installation software is available for download from the HP website at http://www.hp.com/servers/ilo and includes the following:

- Schema Installer, which extends the existing directory schema.
- Management Snap-in Installer, which provides snap-ins to manage iLO objects in an existing directory-enabled IT environment.
- Migration Utilities (*`HPQLOMIG.EXE` and `HPQLOMGC.EXE`*), which automate the process of upgrading the firmware. The utilities also configure the iLO management processors (objects), turn on directory authentication, and create the iLO objects in the directory.

Migration utilities

The HP Lights-Out Migration utility, `HPQLOMIG.EXE`, includes a graphical user interface (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.

The HP Lights-Out Migration Command utility, `HPQLOMGC.EXE`, offers a comm Set the speed of the mouse cursor to the middle setting. Set the mouse cursor Acceleration to **low**, or disable acceleration entirely. and-line approach to migration, rather than a GUI-based approach. This utility works in conjunction with the Application Launch feature of Insight Manager 7. The command-line approach may be preferred for customers that need to configure only a few iLO devices to use directory services.

For more information about these migration tools, see the *HP Directory Migration Utility User Guide* available on the HP web site at http://www.hp.com/servers/ilo.

Extending schema

The schema is a set of rules that define the directory (in terms of tree structure), object types, object attributes, and relationships. However, the base (or initial) schema does not define all of the objects that can be stored within the directory: For example, the base schema does not recognize an iLO management processor as an object and is not aware of its attributes or relationships. Therefore, the schema must be extended to define the iLO management processor in terms of object classes and attributes within the schema.

HP recommends that the administrator carefully review the schema found in the *HP Directory Services Schema Information Booklet*, part number 325823-001, before deploying any iLO management processors within the directory. This schema works on all directories that are compliant with LDAP version 3. The *HP Directory Services Schema Information Booklet* contains class, category, and attribute definitions relating to remote management.

Setting up the directory server

The directory service may be configured to have a single DNS name that points to multiple TCP/IP addresses. If the directory service is configured for this multi-hosting, HP recommends configuring iLO to access the directory server using the DNS name rather than an IP address. This allows iLO to search for a directory server at every address returned in the lookup of the DNS name, guaranteeing that the administrator can always access a directory server. For this reason, using a DNS name that resolves to a single IP address does not provide any benefit.

If the administrator configures the directory server addresses using IP addresses or a single address DNS name, HP recommends never using the host server of an iLO device as the directory server for that iLO device. If the server is down, the directory service is down. For example, if the administrator uses iLO to power off the server, the connection to the directory will be lost. The administrator will be unable to log in using the directory account and will have to use a local account to power on the server remotely.

When using Microsoft Active Directory, the administrator *must* make changes to the directory server before extending the schema. The schema extensions cannot be removed after they are installed. Therefore, it is very important that the administrator understands the changes that will be made before extending the schema. The schema extension tool will require the IP address or DNS name of the server that is the schema master role owner. The administrator must use the Active Directory Schema Tool to configure that server to allow schema updates.

Local versus directory accounts

It is important to remember that local iLO user accounts still exist, even after iLO is configured to use directory services. HP recommends using the local accounts only if the directory service has not been configured or is unavailable, or if the administrator cannot authenticate to the directory service. To increase security, an administrator using directory accounts may want to disable local accounts or remove them entirely.

Customers using a ProLiant p-Class blade server must use a local account when accessing the blade server through the diagnostic cable. Connecting the diagnostic cable to the front of the blade disconnects iLO from the standard network connection, therefore making directory accounts unavailable.

The administrator should set up a review process for local accounts on iLO devices that are primarily accessed by directory users. This will help ensure that all local accounts are identified.

In the unlikely event that the directory services are unavailable, it may be useful to have an emergency local user account with a tightly controlled password to manage the iLO devices.

Roles

Using role-based access allows the administrator to control which users have access to which iLO objects, and what rights and privileges are available to them in that role. For example, the administrator might set up a role called "local admin" and a role called "regional admin." If someone is defined as having the role of "local admin," then that person can access only the rights specified for that role (such as login access and Remote Console) and only at specified times (such as from 8:00 a.m. to 5:00 p.m.) and locations (such as from a specific IP address).

It is important to remember that users can be grouped into one or more roles. Because roles can model very complex relationships and users can have multiple roles, it may be best to set up a role with the minimal rights associated with that role, then put any users that apply into that role. One way to simplify role management is to associate existing user groups with roles, and then manage the membership of the groups instead of the membership of the roles.

A Lights-Out device object in the directory service may have multiple role objects associated with it. Be aware that a user's total privileges to a device are an accumulation of privileges from all roles associated with the device.

Finally, any role object that is related to the iLO device should be placed in a partition housed on the directory server that iLO is referencing. The iLO device will be reading all of the role objects that manage it; and if iLO has to contact a different server to read the role object, it may result in long latencies or the possibility that iLO cannot read the role object and therefore denies access to a legitimate user.

Deploying headless servers

The use of iLO devices seamlessly enables headless server operation. The term headless refers to running a server without legacy input/output devices such as a keyboard, mouse, or monitor (KVM). Headless servers must be accessed through alternative means, such as network or serial ports. By using iLO rather than local KVM devices, the administrator increases the amount of computing space, reduces cabling, reduces complexity, and increases the security of the computing environment.

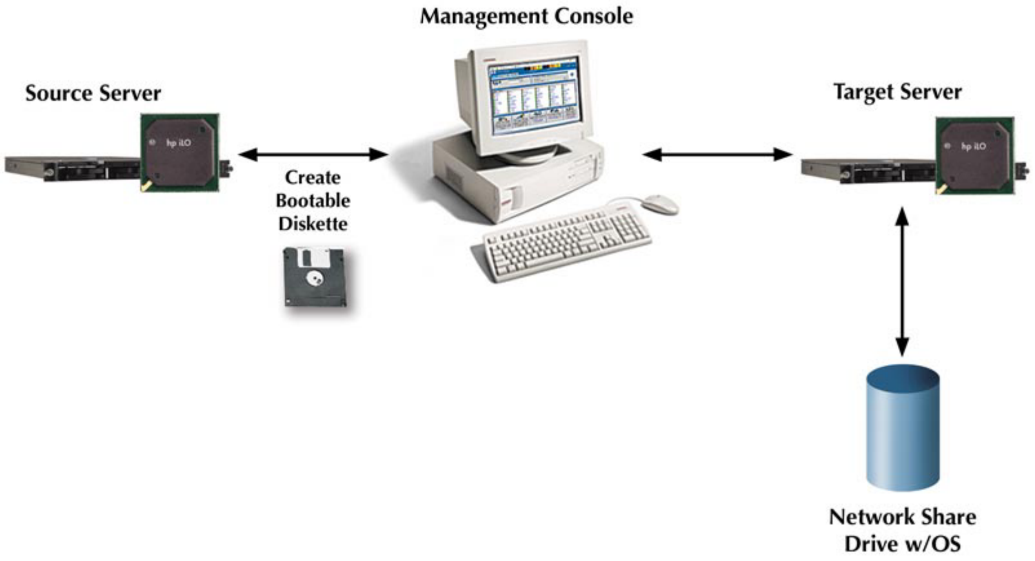
In a headless server environment, iLO will emulate a PS/2 keyboard. When iLO detects that the server is going through POST, iLO scans for a PS/2 keyboard. If no local PS/2 keyboard is detected, iLO will be the PS/2 keyboard for the server.

A consequence of only scanning for a PS/2 keyboard at server POST is that iLO will not implement hot-plug PS/2 keyboard functionality. If a user plugs in a PS/2 keyboard after the server POST, the keyboard will not be detected. If a user unplugs the PS/2 keyboard after the server has gone through POST, but before the OS loads, the OS will be unable to accept keystrokes from the Remote Console. The server must be rebooted to force iLO to rescan for the PS/2 keyboard and use iLO for keyboard input.

Unattended server deployment

Using the capabilities of iLO with its Virtual Media, the SmartStart Scripting Toolkit, and a network share drive, administrators can deploy a server in a completely unattended fashion (Figure 4).

Figure 4. Server deployment with iLO, the Virtual Floppy, and the SmartStart Scripting Toolkit



For example, the administrator configures a source server. Then using the SmartStart Scripting Toolkit, the administrator builds a configuration (boot) diskette with script files. This diskette is inserted into a local management workstation, and the administrator logs into the iLO device in the target server. Using the Virtual Floppy functionality of iLO, the administrator can reboot the target server to the Virtual Floppy and run the script file. If the OS image is stored on a network share drive, the administrator can install the complete OS and applications from the share drive.

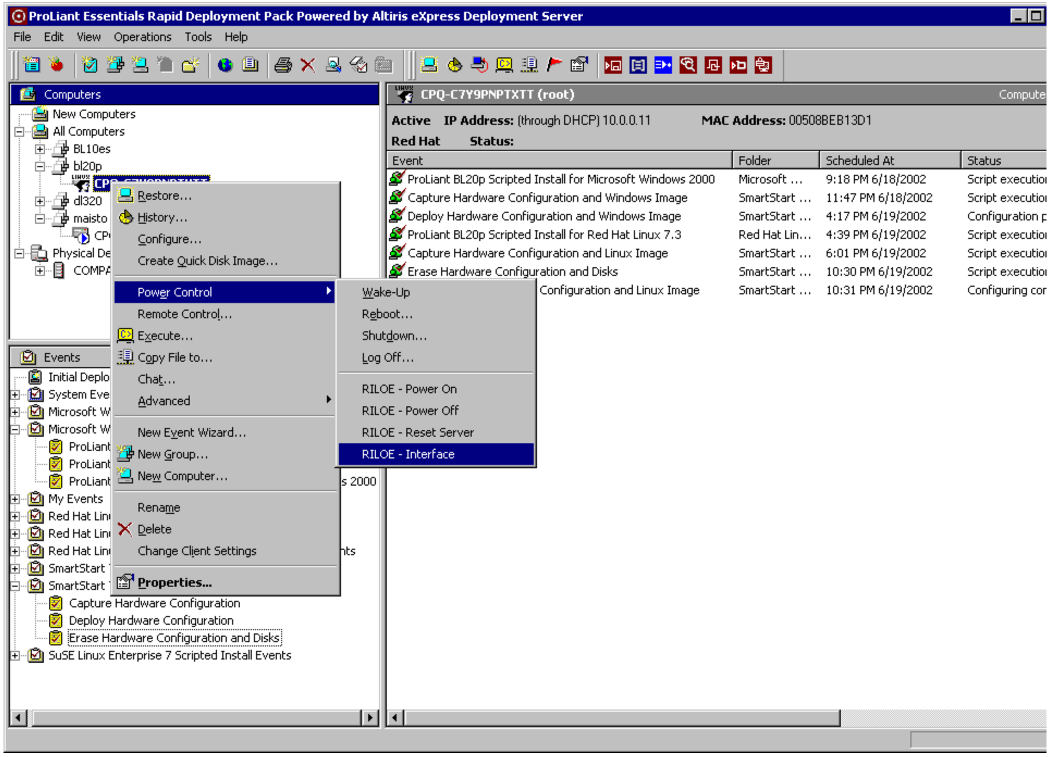
Deploying servers using Rapid Deployment Pack

The ProLiant Essentials Rapid Deployment Pack (RDP) gives administrators the ability to easily deploy one or many servers in an unattended, automated fashion. It combines the Altiris eXpress Deployment solution with the ProLiant Integration Module to provide a "drag and drop" solution for deploying a standard server configuration from a Remote Console. The Deployment Server function within RDP provides capabilities that incorporate the iLO management features of powering on, powering off, or cycling power on a target server.

An administrator can use RDP to browse to an iLO management processor and access the iLO interface:

1. From the Deployment Server Console in RDP, right-click on the server.
2. Select **Power Control** and then **RILOE-Interface** (Figure 5). Note that the RDP interface text uses the word RILOE to mean either a RILOE or an iLO management processor. This provides easy access to the iLO management features.

Figure 5. Using RDP to browse to the iLO management interface. Note that the RDP Interface text uses the word RILOE for connecting to either a RILOE or an iLO management processor.



CPQ-C7Y9PNPTXTT (root)

Active **IP Address:** (through DHCP) 10.0.0.11 **MAC Address:** 00508BEB13D1

Red Hat **Status:**

Event	Folder	Scheduled At	Status
ProLiant BL20p Scripted Install for Microsoft Windows 2000	Microsoft ...	9:18 PM 6/18/2002	Script executio
Capture Hardware Configuration and Windows Image	SmartStart ...	11:47 PM 6/18/2002	Script executio
Deploy Hardware Configuration and Windows Image	SmartStart ...	4:17 PM 6/19/2002	Configuration p
ProLiant BL20p Scripted Install for Red Hat Linux 7.3	Red Hat Lin...	4:39 PM 6/19/2002	Script executio
Capture Hardware Configuration and Linux Image	SmartStart ...	6:01 PM 6/19/2002	Script executio
Erase Hardware Configuration and Disks	SmartStart ...	10:30 PM 6/19/2002	Script executio
Configuration and Linux Image	SmartStart ...	10:31 PM 6/19/2002	Configuring cor

Using the Altiris Boot Disk Creator Utility, an administrator can also create boot floppies with the target server configuration. The administrator can then use these boot floppies with the Virtual Floppy and Virtual Media/universal serial bus (USB) tools to create a bootable image anywhere on the network. The administrator can boot from these virtual floppies and connect to the RDP Deployment Server to complete the installation and deployment process.

More information is available about RDP from the HP website at: http://h18004.www1.hp.com/products/servers/management/rdp/index.html

Virtual Media/USB support

The Virtual Media functionality of iLO provides remote server access to a local client floppy and CD or to a floppy image available anywhere on the network, at the OS level.

The iLO Virtual Media devices are available for all operating systems when the host system is booting. Before the OS loads, the Virtual Media devices are supported through the server ROM. After the OS is booted, a USB-aware operating system will load the standard USB driver that is part of the server OS, without any need for additional HP drivers running on the host server. However, because iLO uses the built-in USB drivers of the operating systems, the level of USB support varies according to the OS. Certain operating systems do not support USB media and therefore do not have access to the Virtual Floppy during system run time. Certain Linux operating systems do not correctly support USB Virtual Floppy drives at OS install time, without special alteration of the Linux kernel. To use the iLO Virtual Media to install a Linux OS, refer to the information in the section titled “Linux OS Tips.” The user should also refer to the chapter “Operating System USB Support” in the User Guide for more detailed information about OS support.

The Virtual Device may be a physical floppy drive on the client PC, an image filed stored on the hard drive of the client PC, or an image file stored on a network drive. For best performance of the Virtual Media, HP recommends using image files stored on the hard drive or on a network drive accessible through a high-speed network link.

Additional information about USB support is available at http://h18004.www1.hp.com/products/servers/platforms/usb-support.html

Using RILOE-II in an iLO server

The RILOE II board is supported as an option in servers with iLO. Starting with firmware version 1.10, iLO will automatically recognize when a RILOE II board is installed in the host server and will disable itself.

Because the iLO functionality is disabled, if the administrator removes the RILOE II board, the iLO device has no way of recognizing this. Therefore, the administrator must re-enable the iLO functionality by using the iLO Security Override Switch. Use the following steps to re-enable the iLO functionality:

1. Turn off server power and unplug the power cord to turn off auxiliary power.
2. Enable the iLO Security Override Switch according to the server manual instructions.
3. Power on the server.
4. The server will go through POST and show the following:
   “iLO security override switch is set. ILO security is disabled!”
5. Press F8 at the prompt (“Integrated Lights-Out. Press F8 to continue”) to enter iLO ROM-Based Setup Utility (RBSU).
6. Navigate to the Configure Tab and set iLO to **enabled.**

With the exception of the ProLiant DL560 server, all iLO-enabled servers recognize the RILOE II boards automatically. If an administrator wants to use a RILOE II board in a ProLiant DL560 server, the administrator must disable the iLO functionality ***before*** inserting the RILOE-II board. The iLO functionality can be disabled through the iLO web pages in either of two ways:

- Set the "Enabled Lights-Out Functionality" Global Setting to **No**.
- In the iLO RBSU, navigate to the **Configure Tab** and set iLO to **disabled**.

Linux tips

The following tips may be helpful for users of Linux operating systems.

Telnet

As discussed in the section titled "Enhancing Security," the configuration of the Remote Console port affects the ability to conduct a Telnet session. Because Telnet sessions connect to port 23 (the Remote Console port), an administrator that has disabled the Remote Console port or set the Remote Console port to auto-enable will not have Telnet support. Telnet support is available only when the Remote Console port is enabled and Remote Console encryption is disabled.

Kickstarting Linux OS with Virtual Floppy

The iLO Virtual Floppy functionality is available when the host system is booting, if the host server's OS contains USB support. For versions of Linux that do not include a USB floppy driver, there is a way to successfully perform a kickstart install using a Virtual Floppy image.

The administrator needs to install the kickstart file, ks.cfg, into the initrd.img file. This can be done using software utilities. An example of such a utility is the rdstuff utility, available from http://sourceforge.net/projects/rdstuff/.

The initrd.img file should be put back onto the floppy.

Edit the syslinux.cfg file as follows:

```
default ks
label ks
        kernel vm linux
        append ks = file:/ks.cfg initrd=initrd.img
```

Proceed with the creation of the Virtual Floppy image. With the kickstart file embedded into the initrd.img file, the Linux OS can use the Virtual Floppy.

For more information

To learn more about the HP management products, visit:
http://h18004.www1.hp.com/products/servers/management/index.html

Feedback

Please direct comments regarding this communication to the ISS Technology Communications Group at this Internet address: TechCom@HP.com

The information in this document is subject to change without notice.

06/2003

TC030606BP

Appendix A: Barcode scanning

Using a bar code scanner to deploy multiple iLO devices requires the following:

- Bar code scanner
- Perl interpreter
- DHCP server
- Lights-Out Configuration Utility (CPQLOCFG.EXE file which connects to each iLO-enabled server)
- ilodply.pl (Perl script which calls the other XML scripts)
- ilotpl.xml (template XML file for initial setup of iLO devices)

Other sample script files include:

- `upgrade.xml` (template file for sending new firmware images to iLO devices)
- `deluser.xml` (template file for deleting users from the database)

These sample script files are available from the website at: http://www.hp.com/servers/ilo

Command-line switches

The Perl script commands are used in the following ways:

```
      perl ilodply.pl -[s|i|m] <dnsfile.*> <file.*> -d
<dnsSuffix>
```

`-s` – Switch to scan/enter management processor information. The desired new DNS names should be located in the file specified by `<dnsfile.*>.` The scanned information including the new DNS name will be saved to the file specified by `<file.*>.`

`-i` - Switch to initially set up a group of management processor. The processor information including the new DNS names should be located in the file specified by `<dnsfile.*>.` The template XML script `ilotpl.xml` should be specified by `<file.*>.`

`-m` - Switch to send an XML script to a group of management processors. The DNS names of the management processors to receive the script should specified in `<dnsfile.*>.` The XML script to send to each processor should be specified in `<file.*>.`

`-d` - Optional switch to specify a DNS suffix. The DNS suffix of the domain where the management processors will reside should be specified in <dnsSuffix>. The DNS suffix should omit the beginning period; for example, -d hp.internal.lab.

Deploying iLO devices

To deploy a group of new management processors, the user would do the following:

- Create a file, `websrv.dns`, that includes the desired DNS name for each management processor. HP recommends that the administrator change the default DNS name to something more easily remembered. Each DNS name in the file should be followed by a carriage return, as shown below. If the default DNS name is desired, create a blank file or create the DNS file by scanning all of the default DNS names from the iLO network settings tags.

  discostus_lab
  moestavrn_lab
  joesgrill_lab

- Invoke `ilodply.pl` with the following command line options to save the management processor information to a new file called `websrv.txt`.

  ```
  perl ilodply.pl -s websrv.dns websrv.txt
  ```

- The Perl script automatically prompts the user for the serial number, default DNS name, password, and Advanced License key for each iLO device. Use the bar code scanner to enter the appropriate information from the iLO network settings tag.
- If the user desires to use the default DNS name and has created a blank file, the Perl script will prompt for both the default DNS name and the new DNS name. Simply scan the default DNS barcode twice from the network settings tag.
- The ProLiant p-class BL servers include the advanced license key. Press **Enter** when prompted for a license on a blade server; otherwise, the XML script will not be executed on the designated server.
- The Perl script then creates the new `websrv.txt` file containing all the pertinent iLO information in a single file.
- If desired, modify the XML template script, ilodply.xml, with any extra options desired for each processor.
- Now, all management processors defined in `websrv.txt` can be set up with the XML script, `ilotpl.xml`, by invoking `ilodply.pl` with the following command line options:

  ```
  perl -i websrv.txt ilotpl.xml-d nuclear.plant
  ```

- To verify an XML script executed correctly on a particular management processor, the log file generated by cpqlocfg.exe can be viewed. The log file is the DNS name of the management processor receiving the XML script.

Updating iLO devices

To upgrade the firmware on a group of management processors, the user should follow the same procedures as in the deployment script, but invoke the Perl script using the –m switch and an XML script such as `upgrade.xml`.

The `–m` switch can be used to send other XML scripts for maintenance purposes. This is helpful in situations where a user needs to upgrade system firmware, add or delete users, etc. For instance, to upgrade a group of management processors specified in `websrv.txt`, invoke the Perl script `ilodply.pl` with the following command line options:

```
perl -m websrv.txt upgrade.xml -d nuclear.plant
```