HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide

February 2005 (First Edition)
Part Number 382328-001

HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide

February 2005 (First Edition)
Part Number 382328-001

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

Introduction

In this section

Guide overview

The HP iLO management processor provides multiple ways to configure, update, and operate. The *HP Integrated Lights-Out 1.70 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* describes in detail the syntax and tools available to use iLO through a command line or scripted interface.

New in this version

- Power Regulator configuration
- Moved all scripting and command line information to a new guide, HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide.
- Support for industry-standard CLP

Command line

In this section

Command line interface overview

HP has worked with key industry partners within Distributed Management Task Force, Inc, to define an industry-standard set of commands. DMTF is working on a suite of specifications, Systems Management Architecture for Server, to standardize manageability interfaces for servers. iLO 1.70 implements the command set defined in the *Server Management Command Line Protocol Specification, 1.00 Draft*. The CLP is intended to replace the simple CLI introduced in iLO 1.60.

Command line access

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

- Serial port using one connection
- Network using:
  - SSH allowing two simultaneous connections. IP address or DNS name, login name, and password are required to start a session using SSH.
  - Telnet protocol using three simultaneous connections.

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

Using the command line

After initiating a command line LI session, you will be presented with the iLO CLI prompt. Each time a command is executed (or you exit the Remote Console or VSP) you will be returned to the CLI prompt as shown in the following example.

```
hpiLO->
```

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

```
hpiLO-> {CLI command}
status=0
status_tag=COMMAND COMPLETED
… output returned…

hpiLO->
```

If an invalid command is entered, then the status and status_tag values will reflect the error as shown:

```
hpiLO-> boguscommand
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND NOT RECOGNIZED
```

If an invalid parameter is given to a valid command, the response is slightly different:

```
hpiLO-> show /bad
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND ERROR-UNSPECIFIED
Invalid property.

hpiLO->
```

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

The privilege level of the logged in user is checked against the privilege required for the command. The command is only executed if the privilege levels match. If the serial command line session status is set to `Enabled-No Authentication`, then all the commands are executed without checking the privilege level.

The general syntax of CLP command is:

```
<verb> <target> <option> <property>
```

- **Verbs**—The supported verbs are:
  - cd
  - create
  - delete
  - help
  - load
  - reset
  - set
  - show
  - start
  - stop
  - exit
  - version
- **Target**—The default target is the `/`. The target can be changed by the `cd` command or by specifying a target on the command line.
- **Options**—The valid options are:
  - -help/-h
  - -all/-a
- **Properties** are the attributes of the target that can be modified.
- **Output**—The output syntax is:

- status
- status_tag
- status_msg

The valid Boolean values for any command are `yes, no, true, false, y, n, t,` and `f.`

General notes:

If the commands on the CLP command span more than one line, you will not be able to navigate between different lines.

Operating system-specific notes:

- Windows 2000 telnet client does not support the Functions keys F1,.., F12, Insert, Home, and End keys. These keys will not work in an iLO command line session.
- The Backspace key in iLO's CLP implementation is mapped to the value `0x8`. Some client operating systems, Novell Linux Desktop and Red Hat Enterprise Linux 4 Desktop, map the Backspace key to the value `0x7f` which is used for the Delete key in Windows® telnet client. The Backspace key will not work from a client where it has value of `0x7f`. For the Linux clients, using the Home or the End key lets the iLO CLP service remap the Backspace key to use the value `0x7f`, making the key functional.

In the Windows Putty client, the Backspace key can be mapped to a value of 0x8 by changing the setting for Terminal Keyboard to Control-H.

Escape commands

The escape key commands are short-cuts to popular tasks.

- `ESC (` invokes the serial CLI connection. This is not necessary for SSH or telnet sessions because they automatically start a CLI session after a successful login.
- `ESC Q` stops the CLI session and terminates the SSH and telnet connection.

- `ESC R ESC r ESC R` resets the system.
- `ESC ^` powers on the system.
- `ESC ESC` erases the current line.

There is a one second timeout for entering any of the escape sequence characters.

Base commands

- **help** displays context-sensitive help.

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

- **exit** terminates the CLP session.
- **cd** sets the current default target. The context works like a directory path. The root context for the server is "/" and this is the starting point for a CLP system. By changing the context, you can shorten commands.

  For example, to find the current iLO firmware version, you could issue the command `show /map1/firmware version.` However, if you issue the `cd /map1/firmware` command, then a simple `show version` command will display the information.

- **show** displays values of a property or contents of a collection target. For example:

```
hpiLO-> show
status=0
status_tag=COMMAND COMPLETED


/
Targets
   system1
   map1
Properties
Verbs
   cd version exit show
```

The first line of information returned by the `show` command is the current context. In the example, `/` is the current context. Following the context is a list of sub-targets (Targets) and properties (Properties) applicable to the current context. The verbs (Verbs) section shows what commands are applicable to this context.

The show command can also be specified with an explicit or implicit context as well as a specific property desired. An explicit context is `/map1/firmware` and is not dependant on the current context. An implicit context assumes that the context specified is a child of the current context. If the current context is /map1 then a `show firmware` command will display the `/map1/firmware` data.

If a property is not specified, then all properties are shown. In the case of the `/map1/firmware` context, there are two properties available: version and date. If you execute `show /map1/firmware date` only the date is shown.

- **create**—Creates a new instance in the name space of the MAP.
- **delete**—Destroys instances in the name space of the MAP.
- **load**—Moves a binary image from an URI to the MAP.
- **reset**—Causes a target to cycle from enabled to disabled and back to enabled.
- **set**—Sets a property or set of properties to a specific value.
- **start**—Causes a target to change state to a higher run level.
- **stop**—Causes a target to change state to a lower run level.
- **version**—Queries the version of the CLP implementation or other CLP elements. For example:

```
hpiLO-> version
status=0
status_tag=COMMAND COMPLETED
SM-CLP Version 1.0
```

Specific commands

The following describes specific commands available when using the command line.

User commands

User commands enable you to display and modify user settings. User settings are located at:

```
/map1/accounts
```

Targets

All the local users are valid targets. For example, if three local users with the login names of Administrator, admin and test exist, then valid targets would be:

- Administrator
- admin
- test

Properties

Property	Access	Description
`username`	read/write	Corresponds to iLO login name.
`password`	read/write	Password for the current user.
`name`	read/write	Displays the name of the user. If this is not specified, it will, by default use the same value as the login name (username). This value corresponds to the iLO user name property.
`group`	read/write	Specifies the privilege level. The valid values are: • admin • config • oemhp_power • oemhp_rc • oemhp_vm If group is not specified, no privileges are assigned to the user.

Examples

The current path is `/map1/accounts`.

- `create username=lname1 password=password`

  In the example, *username* corresponds to the login name

- `set lname1 username=lname2 password=password1 name=name2 group=admin,configure,oemhp_power,oemhp_vm,oemhp_rc`

  In the example, *lname1* is the login name of the user.

Network commands

Network commands enable you to display or modify network settings. The network subsystem is located at:

`/map1/nic1`

Targets

No targets

Properties

Property	Access	Description
`enabledstate`	read/write	Specifies if iLO NIC is enabled. Boolean values accepted.
`oemhp_shared_network`	read/write	Specifies if iLO shared network port is enabled. Boolean values accepted.
`autosense`	read/write	Specifies if the autosense feature is enabled. Boolean values accepted.
`speed`	read/write	Specifies the network speed , 10 or 100 mb/s.
`fullduplex`	read/write	Specifies if the full duplex feature is enabled. Boolean values accepted.
`ipv4address`	read/write	Specifies the IP address of the NIC.

Property	Access	Description
subnetmask	read/write	Specifies the subnet mask of NIC.
oemhp_gateway	read/write	Specifies the gateway IP address for the NIC.
oemhp_dhcp_enable	read/write	Specifies if DHCP is enabled for the NIC. Boolean values accepted
oemhp_dhcp_gateway	read/write	Specifies if the gateway address has to be obtained from the DHCP server. Boolean values accepted.
oemhp_dhcp_dns	read/write	Specifies if the dns server address has to obtained from the DHCP server. Boolean values accepted.
oemhp_dhcp_wins	read/write	Specifies if the IP server address has to be obtained from the DHCP server. Boolean values accepted
oemhp_dhcp_route	read/write	Specifies if the static route addresses have to be obtained from the DHCP server. Boolean values accepted
oemhp_dhcp_domain	read/write	Specifies if the domain name has to be obtained from the DHCP server. Boolean values accepted
oemhp_wins_register	read/write	Specifies if the registration with the IP server is required. Boolean values accepted
oemhp_wins_primary	read/write	Specifies the IP address of the primary IP server.
oemhp_wins_secondary	read/write	Specifies the IP address of the secondary IP server.
oemhp_dns_primary	read/write	Specifies the IP address of the primary DNS server.
oemhp_dns_secondary	read/write	Specifies the IP address of the secondary DNS server.
oemhp_dns_tertiary	read/write	Specifies the IP address of the tertiary DNS server.
oemhp_ddns_register	read/write	Specifies if the registration with the DDNS server is required. Boolean values accepted.

Property	Access	Description
oemhp_route_dest1	read/write	Specifies the destination IP address for the first static route.
oemhp_route_gateway1	read/write	Specifies the gateway IP address for the first static route.
oemhp_route_dest2	read/write	Specifies the destination IP address for the second static route.
oemhp_route_gateway2	read/write	Specifies the gateway IP address for the second static route.
oemhp_route_dest3	read/write	Specifies the destination IP address for the third static route.
oemhp_route_gateway3	read/write	Specifies the gateway IP address for the third static route.
name	read/write	Specifies the DNS name of NIC.
domainname	read/write	Specifies the domain name for NIC.

Examples

```
set /map1/nic1 enabledstate=yes speed=100
ipv4address=192.168.0.13
```

One or more properties can be specified on the command line. If multiple properties are given on the same command line, they must to be separated by a space.

iLO will be reset after network settings have been applied.

iLO settings

iLO settings commands enable you to display or modify iLO settings. iLO settings are located at:

```
/map1/config
```

Targets

No targets

Properties

Property	Access	Description
enabledstate	read/write	Enables or disables iLO. Boolean value.
idletimeout	read/write	Sets session timeout in minutes. Valid values are 15, 30, 60, and 120.
oemhp_passthrough	read/write	Enables or disables terminal services passthrough. Boolean values accepted.
oemhp_rbsuenable	read/write	Enables or disables RBSU prompt during POST. Boolean values accepted.
oemhp_rbsulogin	read/write	Enables or disables login requirement for accessing RBSU. Boolean values accepted.
oemhp_rbsushowip	read/write	Enables or disables iLO IP address display during POST. Boolean values accepted.
oemhp_rcconfig	read/write	Sets the remote console configuration. Valid values are enabled, disabled, or automatic.
oemhp_rcencryp	read/write	Enables or disables encryption for remote console session. Boolean values accepted.
oemhp_httpport	read/write	Sets the HTTP port value.
oemhp_sslport	read/write	Sets the SSL port value.
oemhp_rcport	read/write	Sets remote console port value.
oemhp_vmport	read/write	Sets virtual media port value.
oemhp_tsport	read/write	Sets terminal services port value.
oemhp_sshport	read/write	Sets the SSH port value.
oemhp_sshstatus	read/write	Enables or disables SSH. Boolean values are accepted.

Property	Access	Description
oemhp_serialclistatus	read/write	Enables or disables CLP session through serial port. Boolean values accepted.
oemhp_serialcliauth	read/write	Enables or disables authorization requirement for CLP session through serial port. Boolean values accepted.
oemhp_serialclispeed	read/write	Sets the serial port speed for the CLP session. The valid values are 9600, 19200, 38400, 57600, and 115200.
oemhp_minpwdlen	read/write	Sets the minimum password length requirement.
oemhp_remotekbd	read/write	Sets the layout for the remote keyboard for remote console session.
oemhp_hotkey_t	read/write	Sets the value for hotkey Ctrl-T.
oemhp_hotkey_u	read/write	Sets the value for hotkey Ctrl-U.
oemhp_hotkey_v	read/write	Sets the value for hotkey Ctrl-V.
oemhp_hotkey_w	read/write	Sets the value for hotkey Ctrl-W.
oemhp_hotkey_x	read/write	Sets the value for hotkey Ctrl-X.
oemhp_hotkey_y	read/write	Sets the value for hotkey Ctrl-Y.

Examples

```
set /map1/config enabledstate=yes idletimeout=30
```

One or more properties can be specified on the command line. If multiple properties are given on the same command line, they must be separated by a space.

SNMP settings

SNMP settings commands enable you to display and modify SNMP settings. SNMP settings are available at:

```
/map1/snmp
```

Targets

No targets

Properties

Property	Access	Description
accessinfo1	read/write	Sets the first SNMP trap destination address.
accessinfo2	read/write	Sets the second SNMP trap destination address.
accessinfo3	read/write	Sets the third SNMP trap destination address.
oemhp_iloalert	read/write	Enables or disables iLO SNMP alerts. Boolean values accepted.
oemhp_agentalert	read/write	Enables or disables host agent SNMP alerts. Boolean values accepted.
oemhp_snmppassthru	read/write	Enables or disables iLO SNMP passthrough. Boolean values accepted.
oemhp_imagenturl	read/write	Sets the Insight Manager agent URL.
oemhp_imdatalevel	read/write	Sets the level of detail in the information returned to Insight Manager. Valid values are none, low, medium, and high.

Examples

```
set /map1/snmp accessinfo1=192.168.0.50
oemhp_imdatalevel=medium
```

One or more properties can be specified on the command line. If multiple properties are given on the same command line, they must be separated by a space.

License commands

License commands enable you to display and modify the iLO license. License commands are available at:

```
/map1
```

Targets

No targets

Commands

Command	Description
`cd`	Changes the current directory
`show`	Displays license information
`set`	Changes the current license

Examples

- `set /map1 license=1234500000678910000000001`
- `show /map1 license`
- `delete /map1 license`

Directory commands

Directory commands enable you to display and modify directory settings. Directory settings are available at:

```
/map1/oemhp_dircfg
```

Targets

No targets

Properties

Property	Access	Description
oemhp_dirauth	read/write	Enables or disables directory authentication. Boolean values accepted.
oemhp_localacct	read/write	Enables or disables local account authentication. This can be disabled only if directory authentication is enabled. Boolean values accepted.
oemhp_dirsrvaddr	read/write	Sets the directory server IP address or DNS name.
oemhp_ldapport	read/write	Sets the directory server port.
oemhp_dirdn	read/write	Displays the LOM object distinguished name.
oemhp_dirpassword	read/write	Sets the LOM object password.
oemhp_usercntxt1	read/write	Displays the directory user login search context.
oemhp_usercntxt2	read/write	Displays the directory user login search context.
oemhp_usercntxt3	read/write	Displays the directory user login search context.

Examples

```
set /map1/oemhp_dircfg
```

One or more properties can be specified on the command line. If multiple properties are given on the same command line, they must be separated by a space.

Virtual Media commands

Access to the iLO virtual media (refer to the HP Integrated Lights-Out 1.70 Users Guide for more information on this feature) is supported through the CLP. The virtual media subsystem is located at:

```
/map1/oemhp_vm
```

Targets

You can access the following sub-components of the virtual media:

Target	Description
/map1/oemhp_vm/floppydr	virtual floppy device
/map1/oemhp_vm/cddr	virtual CD-ROM device

Properties

Property	Access	Description
`oemhp_image`	Read/Write	The image path and name for virtual media access. The value is a URL with a maximum length of 80 characters. (described in more detail below)
`oemhp_connect`	Read	Displays if a virtual media device is already connected via the CLP or scriptable virtual media.

Property	Access	Description
oemhp_boot	Read/Write	Sets the boot flag. The valid values are: • never—Do not boot from the device. The value is displayed as No_Boot. • once—Boot from the device once and then not thereafter. The value is displayed as Once. • always—Boot from the device each time the server is reboot. The value is displayed as Always. • connect—Connect the virtual media device. Sets oemhp_connect to Yes and oemhp_boot to Always. • disconnect—Disconnects the virtual media device and sets the oemhp_boot to No_Boot.
oemhp_wp	Read/Write	Enables or disables the write protect flag. Boolean values accepted.
oemhp_applet_connected	Read	Indicates if the Java applet is connected or not.

Image URL

The oemhp_image value is a URL. The URL is limited to 80 characters, specifies the location of the virtual media image file on a HTTP server, and is in the same format as the scriptable virtual media image location.

<URL> example:

```
protocol://username:password@hostname:port/filename
```

- The protocol field is mandatory and must be either http or https.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional
- The filename field is mandatory.

The CLP only performs a cursory syntax verification of the <URL> value. You must visually ensure the <URL> is valid.

Examples

```
set
oemhp_image=http://imgserver.company.com/image/dosboot.b
in
set
oemhp_image=http://john:abc123@imgserver.company.com/VMi
mage/installlDisk.iso
```

iLO 1.60 CLI support

The `vm` simple CLI commands are still supported for virtual media:

- `vm` *device* `insert` *path*—inserts an image.
- `vm` *device* `eject`—ejects an image.
- `vm` *device* `get`—gets the status of the virtual media.
- `vm` *device* `set boot` *access*—sets the status of the virtual media

  Command options:

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

  – The path is the URL to the media image.

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

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

  Refer to the commands INSERT_VIRTUAL_MEDIA, EJECT_VIRTUAL_MEDIA, GET_VM_STATUS, and SET_VM_STATUS in the "Remote Insight Command Language (on page 95)" section for more details on how to use these commands.

  Composite Virtual Media is not supported using the CLI. You must specify Virtual Media images. Refer to the "Virtual media scripting (on page 71)" section for more information.

Tasks

- Insert a floppy image into the virtual floppy:

```
cd /map1/oemhp_vm/floppydr
show
set oemhp_image=http://my.imageserver.com/floppyimg.bin
set oemhp_boot=connect
show
```

where the example executes the following:

- Change the current context to the floppy drive.
- Show the current status to verify that the media is not in use.
- Insert the desired image into the drive.
- Connect the media. The boot setting will automatically be connected *always*.

- Eject a floppy image from the virtual floppy:

```
cd /map1/oemhp_vm/floppydr
set oemhp_boot=disconnect
```

where the example executes the following:

- Change the current context to the floppy drive.
- Issue the disconnect command. This will disconnect the media and clear the oemhp_image as well.

- Insert a CDROM image into the virtual CDROM:

```
cd /map1/oemhp_vm/cddr
show
set
oemhp_image=http://my.imageserver.com/ISO/install_disk1.
iso
set oemhp_boot=connect
show
```

where the example executes the following:

- Change the current context to the floppy drive.
- Show the current status to verify that the media is not in use.
- Insert the desired image into the drive.
- Connect the media. The boot setting will automatically be connected *always*.

- Eject a CDROM image from the virtual CDROM:

```
cd /map1/oemhp_vm/cddr
set oemhp_boot=disconnect
```

where the example executes the following:

- Change the current context to the CDROM drive.
- Issue the disconnect command. This will disconnect the media and clear the oemhp_image as well.

- Insert a CDROM image and set for single boot:

```
cd /map1/oemhp_vm/cddr
set
oemhp_image=http://my.imageserver.com/ISO/install_disk1.
iso
set oemhp_boot=connect
set oemhp_boot=once
show
```

where the example executes the following:

- Change the current context to the CDROM drive.
- Show the current status to verify that the media is not in use.
- Insert the desired image into the drive.
- Connect the media. The boot setting will automatically be connected *always*.
- Override the boot setting to *once*.

- Eject a CDROM image from the virtual CDROM in a single command:

```
set /map1/oemhp_vm/cddr oemhp_boot=disconnect
```

If you attempt to disconnect when the drive is not connected, you will receive an error.

Start and reset commands

Start and reset commands enable you to power on and reboot iLO.

Command	Description
`start`	Turns server power on.
`stop`	Turns server power off.

Command	Description
`reset hard`	Power cycles the server.
`reset soft`	Warm boots the server.

Examples

If the current target is `/system1`, the following commands are supported:

- `start`—Turns server power on.
- `stop` —Turns server power off.
- `reset power` and `reset hard`—Power cycles the server.
- `reset` and `reset soft`—Warm boots the server.

If the current target is `/map1`, the following commands are supported:

- `reset` and `reset soft` resets iLO.

iLO 1.60 CLI support

- **Power**

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

  - `power`—Displays the current server power state
  - `power on`—Turns the server on
  - `power off`—Turns the server off
  - `power reset`—Resets the server (server power off followed by server power on)
  - `power warm`—Warm boots the server

  Instead of using the simple commands, the following examples show the new CLP format:

  - `start /system1`—Turns the server on
  - `stop /system1`—Turns the server off

- `reset /system1`—Resets the server
- `reset /system1 hard`—Performs a coldstart reboot of the server
- `reset /system1 soft`—Performs a warmstart reboot of the server
- `show /system1 enabledstate`—Shows the current power state, where enabled is powered on and disabled is powered off.

- **Vsp**

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

  Instead of using the simple commands, the following example shows the new CLP format:

  ```
  start /system1/oemhp_vsp1
  ```

- **Remcons**

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

  Instead of using the simple commands, the following example shows the new CLP format:

  ```
  start /system1/console1
  ```

Firmware update

Firmware commands enable you to display and modify the iLO firmware version. Firmware settings are available at:

```
/map1/firmware
```

Targets

No targets

Properties

Property	Access	Description
`version`	read	Displays the current firmware version.
`date`	read	Displays the release date of the current firmware version.

Command format

```
load -source <URL> [<target>]
```

where <*URL*> is the URL of firmware update image file on web server. The URL is limited to 50 characters in the iLO 1.70 release of the firmware.

<URL> example:

```
protocol://username:password@hostname:port/filename
```

- The protocol field is mandatory and must be either http or https.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional
- The filename field is mandatory.

The CLP only performs a cursory syntax verification of the <URL> value. You must visually ensure the <URL> is valid.

Examples

```
load -source
http://imgserver.company.com/firmware/iloFWimage.bin
load -source
http://john:abc123@imgserver.company.com/firmware/ilo.bi
n
```

The [<target>] field is `/map1/firmware`, and is optional if it is already the default target.

Eventlog commands

Eventlog commands enable you to display or delete the logs of both the system and iLO. Eventlog settings are available at:

- `/system1/log1 for the system event log`
- `/map1/log1 for the iLO event log`

Targets

`record:1..`*n*, where *n* is the total number of records.

Properties

Property	Access	Description
`number`	read	Displays the record number for the event.
`severity`	read	Displays the severity of the event. It can be informational, noncritical, critical, or unknown.
`date`	read	Displays the event date.
`time`	read	Displays the event time.
`description`	read	Displays a description of the event.

Examples

- `show /system1/log1`—Displays system event log.
- `show /map1/log1`—Displays iLO event log.
- `show /system1/log1/recordn`—Displays record n from the system event `log.`
- `show /map1/log1/recordn`—Displays record n from the iLO event log.
- `delete /system1/log1`—Deletes system event log.
- `delete /map1/log1`—Deletes iLO event log.

Blade commands

Blade commands enable you to display and modify setting on a p-Class server. Blade settings are available at:

```
/system1/map1/blade
```

Targets

You can access the following sub-components of the blade:

Target	Description
/map1/blade/diagport	Displays and modifies the front diagnostic port settings.
/map1/blade/rack	Displays and modifies the blade rack settings.
/map1/blade/rack/enclosure	Displays and modifies the blade enclosure settings.

Properties

Property	Access	Description
`bay_name`	read	Displays and modifies the blade bay name.
`bay_number`	read	Displays the blade bay number.
`facility_power`	read	Displays and modifies if the blade's 48v power is provided by the facility.
`auto_power`	read	Displays and modifies if the blade is enabled to automatically power on.
`log_alerts`	read/write	Displays and modifies if rack alert logging is enabled.
`autoselect`	read/write	Displays and modifies the diagport autoselect setting.
`speed`	read/write	Displays and modifies the diagport speed setting.

Property	Access	Description
fullduplex	read/write	Displays and modifies if the diagnostic port supports full-duplex or half-duplex mode.
ipaddress	read/write	Displays and modifies the IP address for the diagnostic port.
mask	read/write	Displays and modifies the subnet mask for the diagnostic port.
rack_name	read/write	Displays and modifies the rack name.
rack_sn	read	Displays the rack serial number.
encl_name	read/write	Displays and modifies the enclosure name.
ser	read	Displays the enclosure serial number.
encl_type	read	Displays the enclosure type.

Examples

- `set /map1/blade/bay_name=BayOne`—Sets the blade's bay name to BayOne.
- `show /map1/blade/diagport/ipaddress`—Displays the IP address of the front diagnostic port.
- `show /map1/blade/rack/enclosure(N)/encl_type`—Displays the enclosure type for blade enclosure N.

Boot commands

Boot commands enable you to modify the boot source and boot order of the system. Boot settings are available at:

`/system1/bootconfig1`

Targets

`bootsource1`..*n*, where *n* is the total number of boot sources.

Sets the boot source for the system. The possible values are:

- `BootFmCd : bootsource1`
- `BootFmFloppy : bootsource2`
- `BootFmDrive: bootsource3`
- `BootFmNetwork : bootsource4`

  or

- `BootFmCd : bootsource1`
- `BootFmFloppy : bootsource2`
- `BootFmDrive : bootsource3`
- `BootFmUSBKey : bootsource4`
- `BootFmNetwork : bootsource5`

Properties

Property	Access	Description
`bootorder`	read/write	Sets the boot order for a given boot source.

Examples

- `set /system1/bootconfig1/bootsource(n) bootorder=(num)`
- `show /system/bootconfig1`—Displays the complete boot configuration
- `show /system1/bootconfig1/bootsource1`—Displays bootorder for bootsource1

LED commands

UID commands are used to change the state of the Unit-ID light on the server. LED settings are available at:

`/system1/led1`

Command	Description
`start`	Turns the LED on.
`stop`	Turns the LED off.
`show`	Displays the LED status.

Examples

- `show /system1/led1`—Displays current led status
- `start /system1/led1`—Turns led on
- `stop /system1/led1`—Turns led off

iLO 1.60 CLI support

Simple UID CLI commands introduced in iLO 1.60 are still supported.

- `uid`—Displays the current Unit-ID state on the server.
- `uid on`—Turns the Unit-ID light on.
- `uid off`—Turns the Unit-ID light off.

Instead of using the simple commands, the following examples show the new CLP format:

- `show /system1/led1`—To find out LED status
- `start /system1/led1`—To turn LED on
- `stop /system1/led1`—To turn LED off

Other commands

- `start /system/console1`—Starts the text based remote console session. Press `ESC (` to revert back to the CLI session.
- `start /system1/oemhp_vsp1`—Starts virtual serial port session. Press `ESC (` to revert back to the CLI session.

- `nmi server`—Generates and sends an NMI to the server and is limited to users with the Power and Reset privilege.

System target and properties

The targets and properties described in this section provide information about the server.

The following properties are available in `/system1`:

Property	Access	Description
`name`	read	Displays the system name.
`number`	read	Displays the system serial number.
`enabledstate`	read	Displays if the server is powered on.
`oemhp_powerreg`	read/write	Displays the setting for dynamic power saver mode. The settings are auto, max, or min.

Examples

- `show /system1`
- `show /system1 name`
- `set /system1 oemhp_powergov=auto`

The following additional targets are available in `/system1`:

Cpu displays information about the system processor.

The following properties are available in `/system1/cpu<n>`:

Properties	Access	Description
speed	read	Displays the processor speed.
cachememory1	read	Displays the size of the processor level 1 cache.

Properties	Access	Description
cachememory2	read	Displays the size of the processor level 2 cache.

Memory displays information about the system memory.

The following properties are available in `/system1/memory<n>`:

Properties	Access	Description
size	read	Displays the memory size.
speed	read	Displays the memory speed.
location	read	Displays the location of the memory.

Slot displays information about the system slots.

The following properties are available in `/system1/slot<n>`:

Properties	Access	Description
type	read	Displays the slot type.
width	read	Displays the slot width.

Firmware displays information about the system ROM.

The following properties are available in `/system1/firmware`:

Properties	Access	Description
version	read	Displays the version for system ROM.
date	read	Displays the date for the system ROM.

Examples

- `show /system1/cpu1`—Displays information on 1 CPU.
- `show /system1/memory1`—Displays information on 1 memory slot.

- `show /system1/slot1`—Displays information on 1 slot.
- `show /system1/firmware`—Displays information about system ROM.

Telnet

In this section

Telnet support

iLO supports the use of telnet to access the iLO command line interface. Telnet access to iLO supports the CLI, which can invoke a Remote Console connection as well as a Virtual Serial Port connection. Refer to the "Command line (on page 13)" section for more information.

Using Telnet

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

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

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

To access iLO using telnet:

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

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

To terminate a telnet session:

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

   Refer to "iLO VT100+ Key Map (on page 47)" for a complete list of key sequences.

Telnet simple command set

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

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

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

Telnet security

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

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

Supported key sequences

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

iLO VT100+ key map

The following are VT100+ key sequences.

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

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

- Some terminals send `ASCII 127` (DEL) when they mean backspace. The DELETE key never sends DEL, it sends `"\e[3~"`.
- Some programs use the following mapping for HOME and END:

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

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

Key	Sequence	Key	Sequence
\010	\177	**ALT_AMPER**	\e&
UP_KEY	\e[A	**ALT_APOS**	\e'
DOWN_KEY	\e[B	**ALT_OPAREN**	\e(
RIGHT_KEY	\e[C	**ALT_CPAREN**	\e)
LEFT_KEY	\e[D	**ALT_STAR**	\e*
ALT_A	\eA	**ALT_PLUS**	\e+
ALT_B	\eB	**ALT_COMMA**	\e,
ALT_C	\eC	**ALT_MINUS**	\e-
ALT_D	\eD	**ALT_PERIOD**	\e.
ALT_E	\eE	**ALT_SLASH**	\e/
ALT_F	\eF	**ALT_COLON**	\e:
ALT_G	\eG	**ALT_SEMICO**	\e;
ALT_H	\eH	**ALT_LESS**	\e<
ALT_I	\eI	**ALT_EQUAL**	\e=
ALT_J	\eJ	**ALT_MORE**	\e>
ALT_K	\eK	**ALT_QUES**	\e?
ALT_L	\eL	**ALT_AT**	\e@
ALT_M	\eM	**ALT_OPENSQ**	\e[\?
ALT_N	\eN	**ALT_BSLASH**	\e\\
ALT_O	\eO\?	**ALT_CLOSESQ**	\e]
ALT_P	\eP	**ALT_CARAT**	\e^
ALT_Q	\eQ	**ALT_USCORE**	\e_
ALT_R	\eR	**ALT_ACCENT**	\e`
ALT_T	\eT	**ALT_PIPE**	\e|
ALT_U	\eU	**ALT_CBRACK**	\e}

Key	Sequence	Key	Sequence
ALT_V	\eV	**ALT_TILDE**	\e~
ALT_W	\eW	**ALT_TAB**	\e\t
ALT_X	\eX	**ALT_BS**	\e\010
ALT_Y	\eY	**ALT_CR**	\e\r
ALT_Z	\eZ	**ALT_ESC**	\e\e\?
ALT_LOWER_A	\ea	**ALT_F1**	\e\eOP
ALT_LOWER_B	\eb	**ALT_F2**	\e\eOQ
ALT_LOWER_C	\ec	**ALT_F3**	\e\eOR
ALT_LOWER_D	\ed	**ALT_F4**	\e\eOS
ALT_LOWER_E	\ee	**ALT_F5**	\e\eOT
ALT_LOWER_F	\ef	**ALT_F6**	\e\eOU
ALT_LOWER_G	\eg	**ALT_F7**	\e\eOV
ALT_LOWER_H	\eh	**ALT_F8**	\e\eOW
ALT_LOWER_I	\ei	**ALT_F9**	\e\eOX
ALT_LOWER_J	\ej	**ALT_F10**	\e\eOY
ALT_LOWER_K	\ek	**ALT_F11**	\e\eOZ
ALT_LOWER_L	\el	**ALT_F12**	\e\eO[
ALT_LOWER_M	\em	**ALT_F5**	\e\e[15~
ALT_LOWER_N	\en	**ALT_F6**	\e\e[17~
ALT_LOWER_O	\eo	**ALT_F7**	\e\e[18~
ALT_LOWER_P	\ep	**ALT_F8**	\e\e[19~
ALT_LOWER_Q	\eq	**ALT_F9**	\e\e[20~
ALT_LOWER_R	\er	**ALT_F10**	\e\e[21~
ALT_LOWER_S	\es	**ALT_F11**	\e\e[23~

Key	Sequence	Key	Sequence
ALT_LOWER_T	\et	**ALT_F12**	\e\e[24~
ALT_LOWER_U	\eu	**ALT_HOME**	\e\e[1~
ALT_LOWER_V	\ev	**ALT_INS**	\e\e[2~
ALT_LOWER_W	\ew	**ALT_DEL**	\e\e[3~
ALT_LOWER_X	\ex	**ALT_END**	\e\e[4~
ALT_LOWER_Y	\ey	**ALT_PGUP**	\e\e[5~
ALT_LOWER_Z	\ez	**ALT_PGDN**	\e\e[6~
ALT_SPACE	\e\040	**ALT_HOME**	\e\e[H
ALT_EXCL	\e!	**ALT_END**	\e\e[F
ALT_QUOTE	\e\"	**ALT_UP**	\e\e[A
ALT_POUND	\e#	**ALT_DOWN**	\e\e[B
ALT_DOLLAR	\e$	**ALT_RIGHT**	\e\e[C
ALT_PERCENT	\e%	**ALT_LEFT**	\e\e[D

VT100+ codes for the F-keys

Key	Sequence
F1_KEY	\eOP
F2_KEY	\eOQ
F3_KEY	\eOR
F4_KEY	\eOS
F5_KEY	\eOT
F6_KEY	\eOU
F7_KEY	\eOV
F8_KEY	\eOW

Key	Sequence
F9_KEY	\eOX
F10_KEY	\eOY
F11_KEY	eOZ
F12_KEY	\eO[

Linux codes for the F-keys

Key	Sequence
F5_KEY	\e[15~
F6_KEY	\e[17~
F7_KEY	\e[18~
F8_KEY	\e[19~
F9_KEY	\e[20~
F10_KEY	\e[21~
F11_KEY	\e[23~
F12_KEY	\e[24~
HOME_KEY	\e[1~
INSERT_KEY	\e[2~
DELETE_KEY	\e[3~
END_KEY	\e[4~
PG_UP	\e[5~
PG_DOWN	\e[6~

Secure Shell

In this section

SSH overview

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

iLO supports:

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

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

iLO supported SSH features

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

Feature	
Server host key algorithms	ssh-dsa , ssh-rsa
Encryption (same set supported both ways)	3des-cbc, aes128-cbc
Hashing algorithms	hmac-sha1, hmac-md5
Public key algorithms	ssh-dss, ssh-rsa
Key exchange	Diffie-hellman-group1-sha1
Compression	None
Language	English
Client/User authentication method	Password
Authentication timeout	2 minutes
Authentication attempts	3
Default SSH port	22

Using Secure Shell

Using SSH

To access iLO using SSH:

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

Using OpenSSH

To start an OpenSSH client in Linux, use:

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

Using PuTTY

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

    ```
    putty.exe [-ssh | -telnet | -rlogin | -raw]
    [user@]host
    ```

  - For telnet sessions, the following alternative syntax is supported:

    ```
    putty.exe telnet://host[:port]/
    ```

  - To start an existing saved session called *sessionname:*

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

Group administration and iLO scripting

In this section

Lights-Out Configuration Utility

The Lights-Out Configuration Utility (CPQLOCFG.EXE) is a Windows®-based utility that connects to iLO using a secure connection over the network. RIBCL scripts are passed to iLO over the secure connection to CPQLOCFG. This utility requires a valid user ID and password with the appropriate privileges. The CPQLOCFG utility can be launched from Insight Manager 7 or Systems Insight Manager for Group Administration or used independently from a command prompt for batch processing. This utility can be downloaded from the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Version 2.20 or later of CPQLOCFG.EXE is required to configure iLO Directory Settings using RIBCL scripts.

Insight Manager 7 and Systems Insight Manager discover iLO devices as management processors. The Lights-Out Configuration Utility sends a RIBCL file to a group of iLO processors to manage the user accounts for those iLO processors. iLO processors then perform the action designated by the RIBCL file and send a response to the log file.

The Lights-Out Configuration Utility is used to execute RIBCL scripts on iLO and must reside on the same server as Insight Manager 7 or Systems Insight Manager. The Lights-Out Configuration Utility generates two types of error messages: runtime and syntax.

- Runtime errors occur when an invalid action is requested. Runtime errors are logged to the following directories:

  - Insight Manager 7—C:\PROGRAM FILES\INSIGHT MANAGER 7
  - Systems Insight Manager—C:\PROGRAM FILES\INSIGHT MANAGER\HP\SYSTEMS

- Syntax errors occur when an invalid XML tag is encountered. When a syntax error occurs, the Lights-Out Configuration Utility stops running and logs the error in the runtime script and output log file.

  Syntax errors take the format of "Syntax error: expected 'x' but found 'y'" as shown in the following example: `Syntax error: expected USER_LOGIN=userlogin` but found `USER_NAME=username`.

Refer to the RIBCL section ("Remote Insight command language" on page 95) for a complete listing of errors.

Group administration using the Lights-Out Configuration Utility

The IT administrator can manage multiple iLO processors through Insight Manager 7. The components of Group Administration are:

- Insight Manager 7
  - RIBCL ("Remote Insight command language" on page 95)
  - Lights-Out Configuration Utility (on page 57)
  - Query Definition in Insight Manager 7 ("Query definition in Insight Manager 7" on page 59)
  - Application Launch ("Application launch using Insight Manager 7" on page 60)
- Systems Insight Manager
  - RIBCL ("Remote Insight command language" on page 95)
  - Lights-Out Configuration Utility (on page 57)
  - Create a Customized List (on page 61)
  - Create a Custom Command (on page 61)

– Create a Task (on page 62)

Using the Lights-Out Configuration Utility with Insight Manager 7

Insight Manager 7 can manage the group administration of iLO devices using query definitions ("Query definition in Insight Manager 7" on page 59) and Application Launch ("Application launch using Insight Manager 7" on page 60).

Query definition in Insight Manager 7

To group all of the LOM devices, log in to Insight Manager 7 and create a query.

To create the query:

1. Log in to Insight Manager 7.
2. Click **Device** in the navigation bar on the top left side of the screen.
3. Click **Queries,** then click **Device.**
4. Locate the Personal Queries section in the main window. If a query category exists, proceed to step 7, otherwise proceed to step 5.
5. Click **New** to create a new category. For this example, the name of the new category is RIB Cards. Click **Create Category.**
6. Click **Queries** to return to the Device Queries screen.
7. Click **New,** within the appropriate query category, to open the Create/Edit Query screen where the query definition is created.
8. Define the query name, for example "Mgmt Processors."
9. Select **Device(s) of type** and then select **Devices by product name.** In the criteria windows, set the product name to **Integrated Lights-Out.**
10. Click **type** in the Query Description field. A pop-up window opens where you define the device type.
11. Select **Management Processor** and click **OK.**
12. Click **Save** to return to the Device Query screen.
13. Find the newly created query in the appropriate query category and click the query name to run it for verification.

14. Click **Overview** on the left side of the screen after the verification has taken place. The initial page for devices opens.

Application launch using Insight Manager 7

The Application Launch combines the RIBCL, the Lights-Out Configuration Utility, and the query definition to manage the Group Administration of iLO management processors.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task.** A drop-down menu is displayed.
4. Click **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
5. Enter the full path and name for the Lights-Out Configuration Utility in the area provided. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
6. Enter the parameters in the area provided. Insight Manager 7 requires the following parameters for the Lights-Out Configuration Utility:

   -F is the full path of the RIBCL file name.

   -V is the verbose message (optional).

   If the RIBCL file is in the root directory of on the C:\ drive, then the parameters are:

   ```
   -F C:\MANAGEUSERS.xml -V
   ```

   NOTE: The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

7. Click **Next.** A screen displays the options for naming the task, defining the query association, and setting a schedule for the task.
8. Enter a task name in the Enter a name for this task field.
9. Select the query that had been created earlier, for example "Mgmt Processors."

10. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window is displayed.
11. Click **OK** to set the schedule.

    NOTE: The default schedule for a control task is **Now.**

12. Click **Finish** to save the Application Launch task.
13. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

Lights-Out Configuration Utility for Systems Insight Manager

Using CPQLOCFG with Systems Insight Manager requires:

1. Creating a customized list
2. Creating a custom command
3. Creating a task

Create a customized list

A customized list allows you to create a list of a group of management processors and run a task on that list. To create a customized list:

1. In the Systems List pane in the left window, click **Customize.**
2. In the Customize Lists window, select System List using the Show dropdown menu and click **New List.**
3. Select the search parameters using the **Search for** and **where** dropdown menus. Click **Go.**
4. When the systems display, click **Save As.**
5. Enter a name for your list and where it is to be saved.
6. Click **OK.**

Create a custom command

To create a custom command:

1. Click **Tools>Custom Commands>New Custom Command.**

2. In the New Custom Command screen, enter the appropriate information in the **Name, Description,** and **Comments** fields.
3. In the Command field, be sure to enter the full path and the file name of the application. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
4. Enter the Parameters.
5. Enter the Variable Name and Value. Click Add after entering each set of variables and values. To clear an added variable, select the variable, and click **Delete.**
6. After entering the Custom Command information, click **OK.** The new tool is added to the dropdown menu Tools>Custom Commands.

Create a task

Create a task to execute a custom command on specific systems or events.

1. Select the custom command from the Tools>Custom Commands dropdown menu. The Target Selection page is displayed.
2. Choose targets by selecting either:
   - **All systems in the list**—Selecting an option in the drop-down menu automatically targets all systems in that list.
   - **Individual systems in the list**—Selecting an option in the drop-down menu displays the available systems for the selected list. Select the target system.
3. Click **Apply Selections.** The items selected display in the Verify Target Systems page.

   If the systems selected are not compatible with the tool, the Tool Launch OK column provides a brief explanation of the problem. To change the selected target list click **Change Targets.** If you want to remove the system selected, click **Remove** and you will return to the Select Target Systems page.
4. Click **Next** to specify the tool parameters.

   The Next option displays only if the tool parameters need to be specified.
5. Click either **Schedule** or **Run Now.**

– If you click **Schedule,** the schedule task screen appears. Schedule the task. For more information on the scheduling options, see the HP Systems Insight Manager documentation.

  The Schedule option is available only if the tool can be scheduled.

– If you click **Run Now,** the Task Results screen appears with a summary of the task, the target details, and the status.

Batch processing using the Lights-Out Configuration Utility

Group Administration can also be delivered to iLO through batch processing. The components used by batch processing are the Lights-Out Configuration Utility, an RIBCL file, and a batch file.

The following example shows a sample batch file that can be used to perform the Group Administration for iLO:

```
REM Updating the Integrated Lights-Out board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V
```

The Lights-Out Configuration Utility overwrites any existing log files.

Lights-Out Configuration Utility parameters

- -S is the switch that determines the iLO that is to be updated. This switch is either the DNS name or IP address of the target server.

  Do **not** use this switch if you are launching from Insight Manager 7 or Systems Insight Manager. Insight Manager 7 and Systems Insight Manager will provide the address of the iLO when CPQLOCFG.EXE is launched.

- -F is the switch that gives the full path location and name of the RIBCL file that contains the actions to be performed on the board.
- -U and -P specify the user login name and password.

Be sure that the Lights-Out Configuration Utility is in a directory referenced by the PATH environment variable. Any log files generated are placed in the same directory as the Lights-Out Configuration Utility executable

The switches -L and -V might or might not be set depending on the IT administrator's preferences.

- -L is the switch that defines where the log file will be generated and what the file name will be. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch CPQLOCFG.

  Do **not** use this switch if launching from Insight Manager 7 or Systems Insight Manager.

  NOTE: The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

- -V is the optional switch that turns on the verbose message return. The resulting log file contains all commands sent to the Remote Insight board, all responses from the Remote Insight board, and any errors. By default, only errors and responses from GET commands are logged without this switch.

Refer to the "Remote Insight Command Language (on page 95)" section for information on the syntax of the XML data files. Sample XML scripts are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

Perl scripting

In this section

Using Perl with the XML scripting interface

The scripting interface provided enables administrators to manage virtually every aspect of the device in an automated fashion. Primarily, administrators use tools like the `cpqlocfg.exe` ("Lights-Out Configuration Utility" on page 57) to assist deployment efforts. Administrators using a non-Windows® client can use Perl scripts to send XML scripts to the Lights-Out devices. Administrators can also use Perl to perform more complex tasks than `cpqlocfg.exe` can perform.

This section discusses how to use Perl scripting in conjunction with the Lights-Out XML scripting language. Perl scripts require a valid user ID and password with appropriate privileges. Sample XML scripts for Lights-Out devices and a sample Perl script are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

XML enhancements

Previous versions of iLO firmware do not return properly formatted XML syntax. This issue has been addressed in iLO 1.50 when the client parsing utility is properly configured. If the iLO firmware determines the client utility being used does not support the return of properly formatted XML syntax, the following message appears:

```
<INFORM>Scripting utility should be updated to the
latest version.</INFORM>
```

This message informs the customer to update to a later version of the cpqlocfg scripting utility. The latest version of cpqlocfg.exe is currently 2.21.

For customers using a utility other than cpqlocfg.exe, such as Perl scripts, the following steps can help ensure the iLO firmware returns properly formatted XML. Assuming the version of firmware is 1.50, `<LOCFG version="2.21">` should be incorporated into the script sent to iLO. This tag can be placed in either the Perl script or the XML script. Placement of this tag is important. If placing this tag in the Perl script, the tag should be sent after `<?xml version="1.0"?>` and before the XML script is sent. If placing the tag in the XML script, the tag should be placed before `<RIBCL version="2.0">`. If you are using the Perl script provided by HP, then the bold line in the following example can be added to return properly formatted XML syntax.

- Perl script modification

```
…
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr =>
$host);
open(F, "<$file") || die "Can't open $file\n";

# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
#Send tag to iLO firmware to insure properly formatted
XML is returned.
print $client '<LOCFG version="2.21">' . "\r\n";
…
```

- XML script modification

```
<!--
The bold line could be added for the return of properly
formatted XML.
-->
<LOCFG version="2.21"/>
<RIBCL version="2.0">
   <LOGIN USER_LOGIN="Adminname" PASSWORD = "password">
      <!--
      Add XML script here.
      -->
   </LOGIN>
</RIBCL>
</LOCFG>
```

Opening an SSL connection

Perl scripts must open an SSL connection to the device's HTTPS port, by default port 443. For example:

```
use Socket;
use Net::SSLeay qw(die_now die_if_ssl_error);

Net::SSLeay::load_error_strings();
Net::SSLeay::SSLeay_add_ssl_algorithms();
Net::SSLeay::randomize();

#
# opens an ssl connection to port 443 of the passed host
#
sub openSSLconnection($)
{
   my $host = shift;
   my ($ctx, $ssl, $sin, $ip, $nip);

   if (not $ip = inet_aton($host))
   {
      print "$host is a DNS Name, performing lookup\n" if
      $debug;
      $ip = gethostbyname($host) or die "ERROR: Host
      $hostname not found.\n";
   }
   $nip = inet_ntoa($ip);
   print STDERR "Connecting to $nip:443\n";

   $sin = sockaddr_in(443, $ip);
   socket  (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR:
   socket: $!";
   connect (S, $sin) or die "connect: $!";

   $ctx = Net::SSLeay::CTX_new() or die_now("ERROR:
   Failed to create SSL_CTX $! ");
   Net::SSLeay::CTX_set_options($ctx,
   &Net::SSLeay::OP_ALL);
   die_if_ssl_error("ERROR: ssl ctx set options");
   $ssl = Net::SSLeay::new($ctx) or die_now("ERROR:
   Failed to create SSL $!");
   Net::SSLeay::set_fd($ssl, fileno(S));
```

```
   Net::SSLeay::connect($ssl) and
   die_if_ssl_error("ERROR: ssl connect");
   print STDERR 'SSL Connected ';
   print 'Using Cipher: ' .
   Net::SSLeay::get_cipher($ssl) if $debug;
   print STDERR "\n\n";

   return $ssl;
}
```

Sending the XML header and script body

After the connection is established, the first line of script sent must be an XML document header, which tells the device's HTTPS Web server that the following content is an XML script. The header must match the header used in the example exactly. After the header has been completely sent, the remainder of the script can be sent. In this example, the script is sent all at once. For example:

```
# usage: sendscript(host, script)
# sends the xmlscript script to host, returns reply
sub sendscript($$)
{
   my $host = shift;
   my $script = shift;
   my ($ssl, $reply, $lastreply, $res, $n);

   $ssl = openSSLconnection($host);

   # write header
   $n = Net::SSLeay::ssl_write_all($ssl, '<?xml
   version="1.0"?>'."\r\n");
    rint "Wrote $n\n" if $debug;

   # write script
   $n = Net::SSLeay::ssl_write_all($ssl, $script);
   print "Wrote $n\n$script\n" if $debug;

   $reply = "";
   $lastreply = "";

   READLOOP:
   while(1)
   {
```

```
        $n++;
        $reply .= $lastreply;
        $lastreply = Net::SSLeay::read($ssl);
        die_if_ssl_error("ERROR: ssl read");
        if($lastreply eq "")
        {
        sleep(2); # wait 2 sec for more text.
        $lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
        }
        sleep(2); # wait 2 sec for more text.
        $lastreply = Net::SSLeay::read($ssl);
        last READLOOP if($lastreply eq "");
        }
        print "READ: $lastreply\n" if $debug;
        if($lastreply =~ m/STATUS="(0x[0-9A-
        F]+)"[\s]+MESSAGE=
        '(.*)'[\s]+\/>[\s]*(([\s]|.)*?)<\/RIBCL>/)
        {
        if($1 eq "0x0000")
        {
        print STDERR "$3\n" if $3;
        }
        else
        {
        print STDERR "ERROR: STATUS: $1, MESSAGE: $2\n";
        }
        }
    }
    $reply .= $lastreply;
    closeSSLconnection($ssl);
    return $reply;
}
```

PERL scripts can also send a portion of the XML script, wait for the reply, and send more XML later. Using this technique, it is possible to use the reply produced by an earlier command as input to a later command. However, the PERL script must send data within a few seconds or the device will time out and disconnect.

When using the XML scripting interface with PERL scripts, the following restrictions apply:

- PERL scripts must send the XML header before sending the body of the script.
- PERL scripts must provide script data fast enough to prevent the device from timing out.
- XML scripts cannot contain the update firmware command, which requires extra work on the part of the PERL script to open the file containing the firmware image and send it to the device.
- Only one XML document is allowed per connection, which means one pair of RIBCL tags.
- The device will not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

Virtual Media scripting

In this section

Using Virtual Media scripting

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

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

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

Command line syntax:

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

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

Using Virtual Media on Linux servers through an SSH connection

1. Log in to the iLO through SSH (SSH connection from another Linux system, using putty from Windows®.)
2. Enter `vm` to display a list of commands available for Virtual Media.
3. Enter `vm floppy insert http://<address>/<image-name>`.

   The image is available to boot from, but will not be seen by the operating system. (Boot options can be configured with `vm floppy set <option>`, the options are boot_once, boot_always, and no_boot.)
4. Enter `vm floppy set connect` to make the floppy available to the operating system.

5. Enter `vm floppy get` to display the current status. For example:

   ```
   VM Applet = Disconnected
   Boot Option = BOOT_ONCE
   Write Protect = Yes
   Image Inserted = Connected
   ```

   The status of VM Applet always is disconnected, unless a virtual floppy or CD-ROM is connected through the graphical iLO interface.

   The virtual floppy can be disconnected using the `vm floppy set disconnect` or `vm floppy eject` commands. To connect or disconnect a virtual CD-ROM use `cdrom` instead of `floppy`.

The link to the CD-ROM or floppy image must be a URL. It is not possible to specify a drive letter. The CD-ROM image should be in .iso format. The floppy image can be created from a physical floppy by using `rawrite` or the image creation tool included with the Virtual Media applet in the graphical iLO interface.

Mounting Virtual Media on the Linux server:

1. Use `lsmod` to check that the following modules are loaded:
   - usbcore
   - usb-storage
   - usb-ohci
   - sd_mod

   If any of the modules are missing, use `modprobe <`*module*`>` to load them.
2. Mount the drive using one of following:
   - `mount /dev/sda /mnt/floppy -t vfat`—Mounts a virtual floppy.
   - `mount /dev/cdrom1 /mnt/cdrom`—Mounts a virtual CD-ROM on a RedHat system. (Use `/dev/cdrom` if the server does not have a locally attached CD-ROM drive.)
   - `mount /dev/scd0 /mnt/cdrom`—Mounts a virtual CD-ROM on a SUSE system.

Scripting Web server requirements

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

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

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

Virtual media image files

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

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

CGI helper application

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

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

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

Example:

```
#!/usr/bin/perl

use CGI;
use Fcntl;

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

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

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

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

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

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

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

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

HPONCFG online configuration utility

In this section

HPONCFG

The HPONCFG utility is an online configuration tool used to set up and configure iLO and RILOE II from within the Windows and Linux operating systems without requiring a reboot of the server operating system. The utility runs in a command line mode, and must be executed from an operating system command line.

HPONCFG supported operating systems

HPONCFG is supported on:

- Windows NT® Server
- Windows® 2000 Server
- Windows® 2003 Server
- Red Hat Linux Enterprise Linux 2.1
- Red Hat Linux Enterprise Linux 3.0
- United Linux 1.0/SUSE LINUX Enterprise Server 8

HPONCFG requirements

- iLO-based server

For an iLO-based servers, the server must have loaded onto it the iLO Management Interface Driver. The Smart Start operating system install process normally installs this driver. During execution, HPONCFG will warn if it cannot find the driver. If the driver is not installed, it must be downloaded and installed on the server: You can download the driver from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/locate/20_5867.html#0).

For iLO based servers, HPONCFG requires iLO firmware version 1.41 or later.

- RILOE II-based server

  For a RILOE II-based servers, the server must have loaded onto it the RILOE II Management Interface Driver. During execution, HPONCFG will warn if it cannot find the driver. If the driver is not installed, it must be downloaded and installed on the server. You can download the driver from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/locate/20_5868.html).

  For RILOE II-based servers, HPONCFG requires RILOE II firmware version 1.13 or later. For a server Windows® 2000/Windows® 2003, it requires RILOE II Management Interface Driver version 3.2.1.0 or later.

- All servers

  For both iLO-based servers and RILOE II-based servers, the server must have loaded onto it the sm2user.dll. This file is automatically loaded along with the HP Insight Management Agents. During execution, HPONCFG will warn if it cannot find the sm2user.dll file. This file can be installed separately from the component HP Insight Management Agents for Windows® 2000/Windows® Server 2003, component number CP003732, that can be downloaded as a part of the ProLiant Support Pack on the HP website (http://h18004.www1.hp.com/support/files/server/us/download/18416.html).

  After downloading the ProLiant Support Pack, extract its contents to a temporary directory. In the temporary directory, locate CP003732.exe. Extract the contents of this component to a temporary directory. In the temporary directory, locate the subdirectory cqmgserv. The sm2user.dll file can be found in this subdirectory. Copy the sm2user.dll file to the following directory on the server:

  ```
  Winnt\system32\
  ```

HPONCFG installation and usage

The HPONCFG utility is delivered in separate packages for Windows® and Linux systems. For Windows® systems, it is delivered as a softpaq. For Linux systems, it is delivered as a tar file. This same document is delivered as a part of each delivery package.

Windows server installation

To install HPONCFG, run the self-extracting executable delivered in this package from within a directory of your choice on the managed server. This will be the directory from which the HPONCFG utility is executed. This directory will also contain the XML formatted input scripts, and will store the output files from execution of the utility. Make sure that the appropriate Management Interface Driver is installed. The sm2user.dll file must also be installed. Refer to the "HPONCFG requirements (on page 77)" for details on where to obtain this driver and file.

Linux server installation

1. Copy the delivered zip file hponcfg-windows bin.tar to a temporary directory on the managed server. Use the tar utility to extract all of the files. The delivery package contains the following files:
   - hponcfg-1.0.rh72-1.1.i386.rpm—RPM package for Red Hat 7.2
   - hponcfg-1.0.rh73-1.1.i386.rpm—RPM package for Red Hat 7.3
   - hponcfg-1.0.rh8-1.1.i386.rpm—RPM package for Red Hat 8.0
   - hponcfg-1.0.RHAS2.1-1.1.i386.rpm—RPM package for Red Hat Enterprise Linux 2.1
   - hponcfg-1.0.RHAS3.0-1.1.i386.rpm—RPM package for Red Hat Enterprise Linux 3.0
   - hponcfg-1.0.sles7-1.1.i386.rpm—RPM package for SLES 7
   - hponcfg-1.0.sles8-1.1.i386.rpm—RPM package for SLES 8
   - hponcfg-1.0.ul10-1.1.i386.rpm—RPM package for United Linux 1.0

The "hprsm" RPM package must be installed before installing the "hponcfg" RPM package.

2. Install the appropriate package using the "rpm" installation utility. For example, hponcfg RPM on Red Hat Linux 8.0 can be installed by:

   ```
   rpm -ivh hponcfg-1.0.rh8-1.1.i386.rpm
   ```

After installation, the hponcfg executable can be found in the /sbin directory. Make sure that the appropriate Management Interface Driver is installed. Refer to the "HPONCFG requirements (on page 77)" for details on where to obtain this driver and file.

Using HPONCFG

The HPONCFG configuration utility reads an XML input file, formatted according to the rules of the RIBCL language, and produces a log file containing the requested output. A few sample scripts are included in the HPONCFG delivery package. A package containing various and comprehensive sample scripts is available for download on the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/download/20110.html).

Typical usage is to select a script that is similar to the desired functionality and modify it for the exact desired functionality. Note that, although no authentication to the iLO or the RILOE II is required, the XML syntax requires that the USER_LOGIN and PASSWORD tags be present in the LOGIN tag, and that these fields contain data. Any data will be accepted in these fields. To successfully execute HPONCFG, the utility must be invoked as `Administrator` on Windows® servers and as `root` on Linux servers. An error message will be returned by HPONCFG if the user does not possess sufficient privileges.

Using HPONCFG on Windows servers

Start the HPONCFG configuration utility from the command line. When using Microsoft® Windows®, cmd.exe is available by selecting **Start>Run>cmd.** HPONCFG displays a usage page if HPONCFG is entered with no command line parameters. HPONCFG accepts a correctly formatted XML script. Refer to the "Remote Insight Command Language (on page 95)" section for more information on formatting XML scripts. HPONCFG sample scripts are included in the HPONCFG package.

The command line format is:

```
HPONCFG [ /help | /? | /m firmwarelevel | /reset [/m
firmwarelevel]
          | /f filename [/l filename][/xmlverbose or
   /v][/m firmwarelevel]
    | /w filename [/m firmwarelevel]
    | /get_hostinfo [/m firmwarelevel]
    | /mouse [/dualcursor][/allusers]  ]
```

Refer to the "HPONCFG command line parameters (on page 82)" section an explanation of the usage.

Using HPONCFG on Linux servers

Invoke the HPONCFG configuration utility from the command line. HPONCFG will display a usage page if it is entered with no command line parameters.

HPONCFG accepts as input an XML script formatted according to the rules of RIBCL (documented in the *HP Integrated Lights-Out 1.70 User Guide* and *HP Remote Insight Lights-Out Edition II User Guide* in the section describing the use of CPQLOCFG).

The command line format is:

- hponcfg -?
- hponcfg -h
- hponcfg -m minFw
- hponcfg -r [-m minFw]

- hponcfg -w filename [-m minFw]
- hponcfg -g [-m minFw]
- hponcfg -f filename [-l filename] [-v] [-m minFw]

Refer to the "HPONCFG command line parameters (on page 82)" section an explanation of the usage.

HPONCFG command line parameters

HPONCFG accepts the following command line parameters:

- /help or ?—Displays the help page.
- /reset—Resets the RILOE II or iLO to factory default values.
- /f <*filename*>—Sets the RILOE II or iLO configuration from the information given in the XML input file that has name "filename."
- /w <filename>—Writes the RILOE II or iLO configuration obtained from the device to the XML output file that has name *filename*.
- /l <*filename*>—Log replies to the text log file that has name *filename*.
- /get_hostinfo—Gets the host information. Returns the server name and server serial number.
- /m—Indicates to HPONCFG the minimum firmware level that should be present in the management device to execute the RIBCL script. If at least this level of firmware is not present, HPONCFG returns an error without performing any additional action.
- /mouse—Tells HPONCFG to configure the server for optimized mouse handling, there by optimizing graphical remote console performance. By default it optimizes for remote console single cursor mode for the current user. The `dualcursor` command line option along with the `mouse` option will optimize mouse handling as suited for remote console dual cursor mode. The 'allusers' command line option will optimize the mouse handling for all the users on the system. This option is available only for Windows®.

The options must be preceded by a / (slash) for Windows® and - or - for Linux as specified in the usage string.

Example HPONCFG command line:

```
HPONCFG /f add_user.xml /l log.txt > output.txt
```

Obtaining an entire configuration

HPONCFG can be used to obtain an entire configuration from an iLO or a RILOE II. In this case, the utility executes from the command line without specification of an input file. The name of the output file is given on the command line. For example:

```
HPONCFG /w config.xml
```

In this example, the utility indicated that it obtained the data successfully and wrote it to the output file as requested. The following is a typical example of the contents of the output file:

```
<HPONCFG VERSION = "1.1">
<!--- Generated 04/15/04 15:20:36 --->
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
<DIR_LOCAL_USER_ACCT VALUE = "Y"/>
<DIR_SERVER_ADDRESS VALUE = ""/>
<DIR_SERVER_PORT VALUE = "25"/>
<DIR_OBJECT_DN VALUE = " "/>
<DIR_OBJECT_PASSWORD VALUE = ""/>
<DIR_USER_CONTEXT_1 VALUE = ""/>
<DIR_USER_CONTEXT_2 VALUE = "_"/>
<DIR_USER_CONTEXT_3 VALUE = ""/>
</MOD_DIR_CONFIG>
<MOD_NETWORK_SETTINGS>
<SPEED_AUTOSELECT VALUE = "Y"/>
<NIC_SPEED VALUE = "100"/>
<FULL_DUPLEX VALUE = "Y"/>
<IP_ADDRESS VALUE = "16.100.241.229"/>
<SUBNET_MASK VALUE = "255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
<DNS_NAME VALUE = "ILOD234KJ44D002"/>
<PRIM_DNS_SERVER value = "16.81.3.242"/>
<DHCP_ENABLE VALUE = "Y"/>
<DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
```

```
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "Y"/>
<PRIM_WINS_SERVER value = "16.81.3.247"/>
<STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
</MOD_NETWORK_SETTINGS>
<ADD_USER
USER_NAME = "Administrator"
USER_LOGIN = "Administrator"
PASSWORD = "">
</ADD_USER>
<ADD_USER
USER_NAME = "Landy9"
USER_LOGIN = "mandy9"
PASSWORD = "">
</ADD_USER>
<RESET_RIB VALUE = "Y"/>
</HPONCFG>
```

For security reasons, the user passwords are not returned.

Obtaining a specific configuration

A specific configuration can be obtained using the appropriate XML input file. For example, here are the contents of a typical XML input file, `get_global.xml`:

```
<!-- Sample file for Get Global command -->
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<RIB_INFO MODE="read">
<GET_GLOBAL_SETTINGS />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

The XML commands are read from the input file `get_global.xml` and are processed by the device:

```
HPONCFG /f get_global.xml /l log.txt > output.txt
```

The requested information is returned in the log file, which, in this example, is named `log.txt`. The contents of the log file are shown below.

```
<GET_GLOBAL_SETTINGS>
<SESSION_TIMEOUT VALUE="30"/>
<ILO_FUNCT_ENABLED VALUE="Y"/>
<F8_PROMPT_ENABLED VALUE="Y"/>
<REMOTE_CONSOLE_PORT_STATUS VALUE="3"/>
<REMOTE_CONSOLE_ENCRYPTION VALUE="N"/>
<PREFER_TERMINAL_SERVICES VALUE="N"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="23"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<MIN_PASSWORD VALUE="4"/>
</GET_GLOBAL_SETTINGS>
```

Setting a configuration

A specific configuration can be sent to the iLO or RILOE II by using the command format:

```
HPONCFG /f add_user.xml /l log.txt
```

In this example, the input file has contents:

```
<!-- Add user with minimal privileges to test default
setting of
assigned privileges to 'N' -->
<RIBCL version="1.2">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
<ADD_USER USER_NAME="Landy9" USER_LOGIN="mandy9"
PASSWORD="floppyshoes">
<RESET_SERVER_PRIV value="Y" />
<ADMIN_PRIV value="Y" />
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

The specified user will be added to the device.

Lights-Out DOS Utility

In this section

Overview of the Lights-Out DOS Utility

CPQLODOS is a command line utility that is a part of the SmartStart Scripting Toolkit. It is intended to be an initial configuration program to set up only those iLO settings necessary to allow one of the other full-featured configuration methods. Because of this limited usage model, it processes only a small subset of the iLO scripting language.

CPQLODOS is a DOS-only tool that requires MS-DOS® 6.22. CPQLODOS can also be executed from a DOS-bootable diskette or a PXE diskette image as part of the SmartStart Scripting Tool kit. Lights-Out scripting is not supported on Linux operating systems or when using the Novell NetWare Client. This utility does not require a user ID or password because it is executed locally.

CPQLODOS enables you to configure features exposed through F8 startup or the GUI. CPQLODOS processes an XML file with the configuration settings to the iLO in the server on which CPQLODOS is executing. The RIBCL should be used to administer user rights and network functionality on the server.

CPQLODOS is primarily a reconfiguration tool. Any existing configuration will be removed. This utility is not intended for continued administration.

CPQLODOS recommended usage

HP recommends using CPQLODOS `/WRITE_XML=filename.ext` to capture the current iLO settings. The output from the `/WRITE_XML` command should be used as a template for further CPQLODOS scripting.

For security reasons, the `/WRITE_XML` command does not output the passwords for current user accounts or the iLO Advanced Pack license key.

Edit the template file created with the `/WRITE_XML` parameter to reflect the desired configuration.

Use CPQLODOS `/LOAD_XML=filename.ext` to reset the iLO to its factory-default settings, then apply the settings in the XML scripts file.

CPQLODOS general guidelines

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

Command line arguments

All of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allow the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

The following table lists the arguments recognized by CPQLODOS.

Command Line Argument	Description
/HELP or /?	Displays simple help messages
/DETECT	Detects the iLO management processor on the target server
/RESET	Resets the iLO management processor
/VIRT_FLOPPY	Ignores the virtual floppy inserted error
/MIN_FW-xxx	Enables you to set the minimum firmware version on which the iLO management processor runs
/GET_STATUS	Returns the status of the iLO management processor
/GET_HOSTINFO	Retrieves and displays the current host server information on the iLO management processor and displays the server name and number
/GET_USERINFO	Obtains the current users stored in the iLO management processor board and displays the names, login names, and security mask information
/GET_NICCONFIG	Retrieves and displays the NIC settings stored in the iLO management processor
/GET_DHCPCONFIG	Retrieves and displays the DHCP settings stored in the iLO management processor
/GET_DIRCONFIG	Retrieves and displays the DIRECTORY settings in the iLO management processo
/WRITE_XML=path\file name.ext	Reads the settings on the iLO management processor and writes the NIC, DHCP, DIRECTORY, and user settings into an XML hardware configuration script file
/LOAD_XML=path\file name.ext	Loads the script file and applies its changes to the current configuration on the iLO management processor
/VERIFY_XML	Verifies the accuracy of the script file and generates an error message for any incorrect data

RIBCL XML commands for CPQLODOS

CPQLODOS uses the same RIBCL XML commands as CPQLOCFG for the <MOD_NETWORK_SETTINGS>, and the <MOD_DIR_CONFIG> XML scripting language blocks. Only those parameters unique to CPQLODOS are discussed. For more information on <MOD_NETWORK_SETTINGS>, and <MOD_DIR_CONFIG> refer to:

- MOD_NETWORK_SETTINGS (on page 116)
- MOD_DIR_CONFIG

The following XML blocks are unique to CPQLODOS:

- CPQLODOS (on page 90)
- ADD_USER
- SET_LICENSE (on page 92)

CPQLODOS

This command is used to start and end a CPQLODOS session. It can be used only once in a script, and it must be the first and last statement in an XML script.

Example:

```
<CPQLODOS VERSION="2.0">
</CPQLODOS>
```

CPQLODOS parameter

VERSION is a numeric string that indicates the version of CPQLODOS necessary to process this script. The VERSION string is compared to the version that CPQLODOS can process. An error is returned if the version of CPQLODOS and the version of the script do not match. The VERSION parameter can never be blank.

CPQLODOS runtime errors

The CPQLODOS utility sends the MS-DOS® shell a 0 (zero) when no error occurred or a 1 (one) when an error is detected. This can be misleading in that an error might have occurred even if a 0 is returned to the shell. The following can cause a 1 to be returned:

- Version incompatibility
- Wrong operating system (MS-DOS® is required)
- No Lights-Out processor found
- Flash in progress
- Virtual floppy inhibited
- Communication error
- XML error

An XML error implies that there was a problem during the XML transport but not that there was a problem with the XML content. XML content errors can go undetected and result in a zero error return.

To work around this issue, use the log feature to capture the output. The captured output will have more details about XML content errors.

ADD_USER

This command is used to add a user to iLO. If multiple ADD_USER commands are in the XML script, CPQLODOS will use only the settings from the last command.

Example:

```
<ADD_USER
   USER_NAME = "James Madison"
   USER_LOGIN = "jmadison"
   PASSWORD = "president">
</ADD_USER>
```

ADD_USER parameters

USER_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER_LOGIN is the name that the user types in to log in to iLO. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. The string must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

There are no user privilege parameters when ADD_USER is used with CPQLODOS. The added user will have all privileges.

ADD_USER runtime errors

- Login name is too long. Maximum length is 39 characters.
- Password is too short. Minimum length is 8 characters.
- Password is too long. Maximum length is 39 characters.
- Blank user name not allowed. Maximum length is 39 characters.
- Blank user login name not allowed. Maximum length is 39 characters.

SET_LICENSE

This command is used to apply the iLO Advanced Pack License key to the iLO. On a ProLiant BL p-class server, this parameter is not necessary because the advanced features are activated by default.

Example:

```
<SET_LICENSE>
   <LICENSE_KEY VALUE = "12345ABCDE12345FGHIJ12345"/>
</SET_LICENSE>
```

SET_LICENSE parameter

LICENSE_KEY is the text value of the iLO Advanced Pack activation key. This is a 25-byte, alphanumeric string. Do not include any hyphens or spaces in the string.

SET_LICENSE runtime errors

The possible SET_LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

MS-DOS® error codes

The CPQLODOS utility sends the MS-DOS® shell a 0 (zero) when no error occurred or a 1 (one) when an error is detected. This can be misleading in that an error might have occurred even if a 0 is returned to the shell. The following can cause a 1 to be returned:

- Version incompatibility
- Wrong operating system (MS-DOS® is required)
- No Lights-Out processor found
- Flash in progress
- Virtual floppy inhibited
- Communication error
- XML error

An XML error implies that there was a problem during the XML transport but not that there was a problem with the XML content. XML content errors can go undetected and result in a zero error return.

To work around this issue, use the log feature to capture the output. The captured output will have more details about XML content errors.

Remote Insight command language

In this section

Overview of the Remote Insight Board Command Language

The Remote Insight Board Command Language enables you to write scripts to manage user accounts and to configure settings.

IMPORTANT: Comments should not interrupt a command. If they do, an error message will be generated.

RIBCL and ProLiant BL p-Class Servers

The "Remote Insight Command Language" section describes the XML commands and their parameters common to most LOM products and servers. For more information on ProLiant BL p-class server and rack XML commands, refer to the "BL p-Class Configuration" section.

RIBCL sample scripts

Sample scripts for all iLO commands described in this section are available for download from the HP website (http://www.hp.com/servers/lights-out).

RIBCL general guidelines

In this section, all of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allows the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are as follows:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

XML header

The XML header ensures the connection is an XML connection, not an HTTP connection. The XML header is built into the cpqlocfg utility and has the following format:

```
<?xml version="1.0"?>
```

Data types

The three data types that are allowed in the parameter are:

- String

- Specific string
- Boolean string

String

A string is any text enclosed in quotes. It can include spaces, numbers, or any printable character. A string may start with either a double or single quote and it must end with the same type of quote. The string may contain a quote if it is different from the string delimiter quotes.

For example, if a string is started with a double quote, a single quote can be used within the string and the string must be closed with a double quote.

Specific string

A specific string is one that is required to contain certain characters. In general, you have a choice of words that are accepted as correct syntax and all other words produce an error.

Boolean string

A Boolean string is a specific string that specifies a "yes" or "no" condition. Acceptable Boolean strings are "yes," "y," "no," "n," "true," "t," "false," and "f." These strings are not case sensitive.

Response definitions

Every command that is sent to iLO generates a response. The response indicates whether the command succeeded or failed. Some commands generate additional information. The additional information is displayed in execution sequence, provided that no error occurred.

Example:

```
<RESPONSE
   STATUS="0x0001"
   MSG="There has been a severe error."
```

```
/>
```

- RESPONSE

  This tag name indicates that iLO is sending a response to the previous commands back to the client application to indicate the success or failure of the commands that have been sent to iLO.

- STATUS

  This parameter contains an error number. The number “0x0000” indicates that there is no error.

- MSG

  This element contains a message describing the error that happened. If no error occurred, the message “No error” is displayed.

RIBCL

This command is used to start and end an RIBCL session. You can use it only once to start an RIBCL session, and it must be the first command to display in the script. The RIBCL tags are required to mark the beginning and the end of the RIBCL document.

Example:

```
<RIBCL VERSION="2.0">
</RIBCL>
```

RIBCL parameters

VERSION is a string that indicates the version of the RIBCL that the client application is expecting to use. The VERSION string is compared to the version of the RIBCL that is expected, and an error is returned if the string and the version do not match. The preferred value for the VERSION parameter is "2.0." The VERSION parameter is no longer checked for an exact match; however, this parameter can never be blank.

RIBCL runtime errors

The possible RIBCL error messages include:

Version must not be blank.

LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level will be used when performing RIBCL actions. The specified user must have a valid account on the respective iLO to execute RIBCL commands. The user's privileges are checked against the required privilege for a particular command, and an error is returned if the privilege level does not match.

Example:

```
<LOGIN USER_LOGIN="username" PASSWORD="password">
</LOGIN>
```

Alternatively, the CPQLOCFG utility can specify the login information as parameters on its command line:

```
cpqlocfg  -u <username> -p <password>
```

When using this format, the utility returns an `Overriding credentials` warning message but still shows the error log message entry as `Login name must not be blank.`

LOGIN parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters.

LOGIN runtime errors

The possible runtime error messages include:

- User login name was not found.
- Password must not be blank.

- Logged-in user does not have required privilege for this command.

USER_INFO

The USER_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local user information database into memory and prepares to edit it. Only commands that are USER_INFO type commands are valid inside the USER_INFO command block. The USER_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If database is open for writing by another application, then this call will fail.

Example:

```
<USER_INFO MODE="write">
   …… USER_INFO commands ……
</USER_INFO>
```

USER_INFO parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of iLO information. Read mode prevents modification of the iLO information.

USER_INFO runtime error

None

ADD_USER

The ADD_USER command is used to add a local user account. The USER_NAME and USER_LOGIN parameters must not exist in the current user database. Use the MOD_USER command to change an existing user's information. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

All of the attributes that pertain to the user are set using the following parameters.

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="loginname" PASSWORD="password">
   <USER_INFO MODE="write">
   <ADD_USER
      USER_NAME="User"
      USER_LOGIN="username" PASSWORD="password">
      <ADMIN_PRIV value ="No"/>
      <REMOTE_CONS_PRIV value ="Yes"/>
      <RESET_SERVER_PRIV value ="No"/>
      <VIRTUAL_MEDIA_PRIV value ="No"/>
      <CONFIG_ILO_PRIV value ="No"/>
   </ADD_USER>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

ADD_USER parameters

USER_NAME is the actual name of the user. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

The following parameters are not applicable to a user's privileges in the iLO firmware versions 1.40 and higher. The parameters will parse correctly, but user privileges will not be affected.

VIEW_LOGS_PRIV is a Boolean parameter that gives the user permission to view the iLO system logs. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to view logs. If this parameter is used, the Boolean string value must never be blank.

CLEAR_LOGS_PRIV is a Boolean parameter that gives the user permission to clear the event log. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to clear the iLO event log. If this parameter is used, the Boolean string value must never be blank.

EMS_PRIV is a Boolean parameter that gives the user permission to use the Windows® Server 2003 EMS service. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to use EMS services. If this parameter is used, the Boolean string value must never be blank.

UPDATE_ILO_PRIV is a Boolean parameter that allows the user to copy a new firmware image into the iLO system ROM. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO. If this parameter is used, the Boolean string value must never be blank.

CONFIG_RACK_PRIV is a Boolean parameter that gives the user permission to configure and manage the server rack resources. This parameter is applicable to ProLiant BL p-Class servers only. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to manage or configure rack resources. If this parameter is used, the Boolean string value must never be blank.

DIAG_PRIV is a Boolean parameter that gives the user permission to view diagnostic information about iLO. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have diagnostic privileges. If this parameter is used, the Boolean string value must never be blank.

ADD_USER runtime errors

The possible ADD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.

- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.
- User name cannot be blank.
- User login ID cannot be blank.
- Boolean value not specified.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_USER

The DELETE_USER command is used to remove an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname"
   PASSWORD="password">
   <USER_INFO MODE="write">
   <DELETE_USER USER_LOGIN="username"/>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

DELETE_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

DELETE_USER runtime errors

The possible DELETE_USER errors include:

- User information is open for read-only access. Write access is required for this operation.
- Cannot delete user information for currently logged in user.
- User login name was not found.
- User login name must not be blank.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_CURRENT_USER

The DELETE_CURRENT_USER command is used to remove the user account defined by the USER_LOGIN attribute. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

This command is intended for customers who desire to delete all user accounts on iLO.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname"
   PASSWORD="password">
   <USER_INFO MODE="write">
   <DELETE_CURRENT_USER/>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

DELETE_CURRENT_USER parameters

None

DELETE_CURRENT_USER runtime errors

The possible DELETE_CURRENT_USER errors include:

User information is open for read-only access. Write access is required for this operation.

GET_USER

The GET_USER command will return a local user's information, excluding the password. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve other user accounts; else the user can only view their individual account information.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_USER USER_LOGIN="username"/>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

GET_USER runtime errors

The possible GET_USER error messages include:

- User login name must not be blank.
- User login name was not found.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER return messages

A possible GET_USER return message includes:

```
<RESPONSE
   STATUS="0x0000"
   MSG="No Errors"
/>
   <GET_USER
   USER_NAME="Admin User"
   USER_LOGIN= "username"
   ADMIN_PRIV="N"
   REMOTE_CONS_PRIV="Y"
   RESET_SERVER_PRIV="N"
   VIRTUAL_MEDIA_PRIV="N"
   CONFIG_ILO_PRIV value ="No"
/>
```

MOD_USER

The MOD_USER command is used to modify an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege. A user without the administrative privilege can only modify their individual account password.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="write">
   <MOD_USER USER_LOGIN="loginname">
      <USER_NAME value="username"/>
      <USER_LOGIN value="newloginname"/>
      <PASSWORD value="password"/>
      <ADMIN_PRIV value="No"/>
      <REMOTE_CONS_PRIV value="Yes"/>
      <RESET_SERVER_PRIV value="No"/>
      <VIRTUAL_MEDIA_PRIV value="No"/>
      <CONFIG_ILO_PRIV value="Yes"/>
   </MOD_USER>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

MOD_USER parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

If the following parameters are not specified, then the parameter value for the specified user is preserved.

USER_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

MOD_USER runtime errors

The possible MOD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.
- User information is open for read-only access. Write access is required for this operation.
- User login name must not be blank.
- Cannot modify user information for currently logged user.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS

The GET_ALL_USERS command will return all USER_LOGIN parameters in the user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve all user accounts.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_ALL_USERS />
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_ALL_USERS parameters

None

GET_ALL_USERS runtime errors

The possible GET_ALL_USERS error messages include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS return messages

A possible GET_ALL_USERS return message is:

```
<RESPONSE
   STATUS="0x0000"
   MESSAGE='No Error'
/>
<GET_ALL_USERS>
   <USER_LOGIN VALUE="username"/>
   <USER_LOGIN VALUE="user2"/>
   <USER_LOGIN VALUE="user3"/>
   <USER_LOGIN VALUE="user4"/>
   <USER_LOGIN VALUE="user5"/>
   <USER_LOGIN VALUE="user6"/>
   <USER_LOGIN VALUE="user7"/>
   <USER_LOGIN VALUE="user8"/>
   <USER_LOGIN VALUE="user9"/>
   <USER_LOGIN VALUE="user10"/>
   <USER_LOGIN VALUE=""/>
   <USER_LOGIN VALUE=""/>
</GET_ALL_USERS>
```

A possible unsuccessful request is:

```
<RESPONSE
   STATUS = "0x0001"
   MSG = "Error Message"/>
```

GET_ALL_USER_INFO

The GET_ALL_USER_INFO command will return all local users information in the user database, excluding passwords. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have administrative privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="read">
   <GET_ALL_USER_INFO />
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

GET_ALL_USER_INFO parameters

None

GET_ALL_USER_INFO runtime errors

The possible GET_ALL_USER_INFO error message include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USER_INFO return messages

A possible GET_ALL_USER_INFO return message is:

```
<GET_ALL_USER_INFO/>
   <GET_USER
```

```
   USER_NAME="Admin"
   USER_LOGIN="Admin"
   ADMIN_PRIV="Y"
   CONFIG_RILO_PRIV="Y"
   LOGIN_PRIV="Y"
   REMOTE_CONS_PRIV="Y"
   RESET_SERVER_PRIV="Y"
   VIRTUAL_MEDIA_PRIV="Y"
/> ......
The same information will be repeated for all the users.
</GET_ALL_USER_INFO>
```

A possible unsuccessful request is:

```
<RESPONSE
   STATUS = "0x0001"
MSG = "Error Message"/>
```

RIB_INFO

The RIB_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the iLO configuration information database into memory and prepares to edit it. Only commands that are RIB_INFO type commands are valid inside the RIB_INFO command block. The RIB_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:

```
<RIB_INFO MODE="write">
…… RIB_INFO commands ……
</RIB_INFO>
```

RIB_INFO parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of iLO information. Read mode prevents modification of iLO information.

RIB_INFO runtime errors

None

RESET_RIB

The RESET_RIB command is used to reset iLO. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
   <RIB_INFO MODE = "write">
   <RESET_RIB/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

RESET_RIB parameters

None

RESET_RIB runtime errors

The possible RESET_RIB error message include:

User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_NETWORK_SETTINGS

The GET_NETWORK_SETTINGS command requests the respective iLO network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="read">
   <GET_NETWORK_SETTINGS/>
   </RIB_INFO>
   </LOGIN>
 </RIBCL>
```

GET_NETWORK_SETTINGS parameters

None

GET_NETWORK_SETTINGS runtime errors

None

GET_NETWORK_SETTINGS return messages

A possible GET_NETWORK_SETTINGS return message is:

```
<GET_NETWORK_SETTINGS
   <SPEED_AUTOSELECT VALUE="Y"/>
   <NIC_SPEED VALUE="100"/>
   <FULL_DUPLEX VALUE="N"/>
   <DHCP_ENABLE VALUE="Y"/>
   <DHCP_GATEWAY VALUE="Y"/>
   <DHCP_DNS_SERVER VALUE="Y"/>
   <DHCP_STATIC_ROUTE VALUE="Y"/>
   <DHCP_WINS_SERVER VALUE="Y"/>
   <REG_WINS_SERVER VALUE="Y"/>
   <IP_ADDRESS VALUE="111.111.111.111"/>
   <SUBNET_MASK VALUE="255.255.255.0"/>
   <GATEWAY_IP_ADDRESS VALUE="111.111.111.1"/>
   <DNS_NAME VALUE="test"/>
   <DOMAIN_NAME VALUE="test.com"/>
   <PRIM_DNS_SERVER VALUE="111.111.111.242"/>
   <SEC_DNS_SERVER VALUE="111.111.111.242"/>
   <TER_DNS_SERVER VALUE="111.111.111.242"/>
   <PRIM_WINS_SERVER VALUE="111.111.111.246"/>
```

```
   <SEC_WINS_SERVER VALUE="111.111.111.247"/>
   <STATIC_ROUTE_1 DEST VALUE="0.0.0.0"/> <GATEWAY
   VALUE="0.0.0.0"/>
   STATIC_ROUTE_2 DEST VALUE="0.0.0.0"/> GATEWAY
   VALUE="0.0.0.0"/>
   STATIC_ROUTE_3 DEST VALUE="0.0.0.0"/> GATEWAY
   VALUE="0.0.0.0"/>
   WEB_AGENT_IP_ADDRESS VALUE=""/>
</GET_NETWORK_SETTINGS>
```

A possible unsuccessful request is:

```
<RESPONSE
   STATUS = "0x0001"
   MSG = "Error Message"/>
```

MOD_NETWORK_SETTINGS

MOD_NETWORK_SETTINGS is used to modify network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

iLO scripting firmware does not attempt to decipher if the network modifications are appropriate for the network environment. When modifying network settings, be aware of the network commands provided to the management processor. In some cases, the management processor ignores commands and no error is returned. For example, when a script includes the command to enable DHCP and a command to modify the IP address, the IP address is ignored. Changing the network settings to values that are not correct for the network environment might cause a loss of connectivity to the iLO.

The iLO management processor reboots to apply the changes after the script has successfully completed. If connectivity is lost to the iLO, use RBSU to reconfigure the network settings to values that are compatible with the network environment. For more information, refer to "iLO RBSU."

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_NETWORK_SETTINGS>
```

```
        <ENABLE_NIC value="Yes"/>
        <SPEED_AUTOSELECT value="No"/>
        <SHARED_NETWORK_PORT VALUE="No"/>
        <NIC_SPEED value="100"/>
        <FULL_DUPLEX value="Yes"/>
        <DHCP_ENABLE value="Yes"/>
        <IP_ADDRESS value="192.168.132.25"/>
        <SUBNET_MASK value="255.255.0.0"/>
        <GATEWAY_IP_ADDRESS value="192.168.132.2"/>
        <DNS_NAME value="demorib"/>
        <DOMAIN_NAME value="internal.net"/>
        <DHCP_GATEWAY value="No"/>
        <DHCP_DNS_SERVER value="No"/>
        <DHCP_WINS_SERVER value="No"/>
        <DHCP_STATIC_ROUTE value="No"/>
        <REG_WINS_SERVER value="No"/>
        <REG_DDNS_SERVER value="No"/>
        <PING_GATEWAY value="Yes"/>
        <PRIM_DNS_SERVER value="192.168.12.14"/>
        <SEC_DNS_SERVER value="192.168.12.15"/>
        <TER_DNS_SERVER value="192.168.12.16"/>
        <PRIM_WINS_SERVER value="192.168.145.1"/>
        <SEC_WINS_SERVER value="192.168.145.2"/>
        <STATIC_ROUTE_1 DEST="192.168.129.144"
        GATEWAY="192.168.129.1"/>
        <STATIC_ROUTE_2 DEST="192.168.129.145"
        GATEWAY="192.168.129.2"/>
        <STATIC_ROUTE_3 DEST="192.168.129.146"
        GATEWAY="192.168.129.3"/>
      </MOD_NETWORK_SETTINGS>
      </RIB_INFO>
      </LOGIN>
</RIBCL>
```

MOD_NETWORK_SETTINGS parameters

If the following parameters are not specified, then the parameter value for the specified setting is preserved. Zero values are not permitted in some fields. Consequently, an empty string deletes the current value in some fields.

ENABLE_NIC enables the NIC to reflect the state of iLO. The values are "Yes" or "No." It is case insensitive.

SHARED_NETWORK_PORT is used to set the iLO Shared Network Port value. The values are "Yes" or "No." The Shared Network Port command is supported on ProLiant 3xx G4 series servers.

SPEED_AUTOSELECT is a Boolean parameter to enable or disable the iLO transceiver to auto-detect the speed and duplex of the network. This parameter is optional, and the Boolean string must be set to "Yes" if this behavior is desired. If this parameter is used, the Boolean string value must never be left blank. The possible values are "Yes" or "No." It is case insensitive.

FULL_DUPLEX is used to decide if the iLO is to support full-duplex or half-duplex mode. It is only applicable if SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

NIC_SPEED is used to set the transceiver speed if SPEED_AUTOSELECT was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

DHCP_ENABLE is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

IP_ADDRESS is used to select the IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET_MASK is used to select the subnet mask for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY_IP_ADDRESS is used to select the default gateway IP address for the iLO if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS_NAME is used to specify the DNS name for the iLO. If an empty string is entered, the current value is deleted.

DOMAIN_NAME is used to specify the domain name for the network where the iLO resides. If an empty string is entered, the current value is deleted.

DHCP_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_DNS_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_WINS_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_STATIC_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG_WINS_SERVER specifies if the iLO must be register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM_DNS_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_DNS_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER_DNS_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM_WINS_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_WINS_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC_ROUTE_1, STATIC_ROUTE_2, and STATIC_ROUTE_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.
- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

WEB_AGENT_IP_ADDRESS specifies the address for the Web-enabled agents. If an empty string is entered, the current value is deleted.

MOD_NETWORK_SETTINGS runtime errors

The possible MOD_NETWORK_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_GLOBAL_SETTINGS

The GET_GLOBAL_SETTINGS command requests the respective iLO global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

GET_GLOBAL_SETTINGS parameters

None

GET_GLOBAL_SETTINGS runtime errors

None

GET_GLOBAL_SETTINGS return messages

A possible GET_GLOBAL_SETTINGS return message is:

```
<GET_GLOBAL_SETTINGS>
   <SESSION_TIMEOUT="120">
   <ILO_FUNCT_ENABLED VALUE="Y"/>
   <F8_PROMPT_ENABLED="Y"/>
   <F8_LOGIN_REQUIRED="Y"/>
   <REMOTE_CONSOLE_PORT_STATUS VALUE="2"/>
   <REMOTE_CONSOLE_ENCRYPTION VALUE="Y"/>
   <PASSTHROUGH_CONFIG VALUE=”3”/>
   <HTTPS_PORT VALUE="443"/>
   <HTTP_PORT VALUE="80"/>
   <REMOTE_CONSOLE_PORT VALUE="23"/>
   <TERMINAL_SERVICES_PORT VALUE="3389"/>
   <VIRTUAL_MEDIA_PORT VALUE="17988"/>
   <MIN_PASSWORD VALUE="8"/>
   <REMOTE_KEYBOARD_MODEL VALUE="US"/>
   <SSH_PORT value="22"/>
   <SSH_STATUS value="YES"/>
   <SERIAL_CLI_STATUS value="3"/>
   <SERIAL_CLI_SPEED value="1"/>
</GET_GLOBAL_SETTINGS>
```

This reply differs from RILOE II.

MOD_GLOBAL_SETTINGS

MOD_GLOBAL_SETTINGS is used to modify global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_GLOBAL_SETTINGS>
      <SESSION_TIMEOUT value="60"/>
      <ILO_FUNCT_ENABLED value="Yes"/>
```

```
   <F8_PROMPT_ENABLED value="Yes"/>
   <F8_LOGIN_REQUIRED="Y"/>
   <REMOTE_CONSOLE_PORT_STATUS value="2"/>
   <REMOTE_CONSOLE_ENCRYPTION value="Y"/>
   <PASSTHROUGH_CONFIG value=”3”/>
   <HTTPS_PORT value="443"/>
   <HTTP_PORT value="80"/>
   <REMOTE_CONSOLE_PORT value="23"/>
   <TERMINAL_SERVICES_PORT VALUE="3389"/>
   <VIRTUAL_MEDIA_PORT value="17988"/>
   <MIN_PASSWORD VALUE="8"/>
   <REMOTE_KEYBOARD_MODEL VALUE="US"/>
   <VIRTUAL_MEDIA_PORT value="55"/>
   <SSH_PORT value="22"/>
   <SSH_STATUS value="YES"/>
   <SERIAL_CLI_STATUS value="3"/>
   <SERIAL_CLI_SPEED value="1"/>
</MOD_GLOBAL_SETTINGS>
</RIB_INFO>
</LOGIN>
```

MOD_GLOBAL_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

SESSION_TIMEOUT determines the maximum session timeout value in minutes. The accepted values are 15, 30, 60 and 120.

ILO_FUNCT_ENABLED determines if the Lights-Out functionality is enabled or disabled for iLO. The possible values are "Yes" or "No." It is case insensitive.

F8_PROMPT_ENABLED determines if the F8 prompt for ROM-based configuration is displayed during POST. The possible values are "Yes" or "No."

F8_LOGIN_REQUIRED determines if login credentials are required to access the RBSU for iLO. The possible values are "Yes" or "No."

REMOTE_CONSOLE_PORT_STATUS determines the behavior of remote console service. The possible values are:

- **0**—No change

- **1**—Disabled (The remote console port is disabled. This will prevent remote console and telnet sessions from being utilized.)
- **2**—Automatic (This is the default setting. The remote console port will remain closed unless a remote console session is started.)
- **3**—Enabled (The remote console port is always enabled. This will allow remote console and telnet sessions to be utilized)

REMOTE_CONSOLE_ENCRYPTION determines if remote console data encryption is enabled or disabled. The possible values are "Yes" and "No."

PASSTHROUGH_CONFIG determines the behavior of a Microsoft® Terminal Services client. The possible values are:

- **0**—No change
- **1**—Disabled (The Terminal Services feature is disabled.)
- **2**—Automatic (The Terminal Services client will be launched when remote console is started.)
- **3**—Enabled (This is the default setting. The terminal services feature is enabled but will not automatically be launched when remote console is started.)

HTTPS_PORT specifies the HTTPS (SSL) port number.

HTTP_PORT specifies the HTTP port number.

REMOTE_CONSOLE_PORT specifies the port used for remote console.

TERMINAL_SERVICES_PORT specifies the port used for terminal services.

VIRTUAL_MEDIA_PORT specifies the port used for virtual media.

> **NOTE:** If port changes are detected, the iLO management processor will be rebooted to apply the changes after the script has completed successfully.

MIN_PASSWORD command specifies how many characters are required in all user passwords. The value can be from zero to 39 characters.

REMOTE_KEYBOARD_MODEL determines the remote keyboard language translation used during remote console operation. The possible values are:

US	Belgian	British
Danish	Finnish	French
French Canadian	German	Italian
Japanese	Latin American	Portuguese
Spanish	Swedish	Swiss French
Swiss German		

SSH_PORT specifies the port used for SSH connection on iLO. The processor must be reset if this value is changed.

SSH_STATUS determines if SSH is enabled. The valid value are Yes or No, which enables or disables SSH functionality.

SERIAL_CLI_STATUS specifies the status of the CLI. The possible values are:

- **0**—No change
- **1**—Disabled
- **2**—Enabled (no authentication required)
- **3**—Enabled (authentication required)

SERIAL_CLI_SPEED specifies the CLI port speed. The possible values are :

- **0**—No change
- **1**—9,600 bps
- **2**—19,200 bps
- **3**—38,400 bps
- **4**—57,600 bps
- **5**—115,200 bps

MOD_GLOBAL_SETTINGS runtime errors

The possible MOD_GLOBAL_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.
- Unrecognized keyboard model.

GET_SNMP_IM_SETTINGS

The GET_SNMP_IM_SETTINGS command requests the respective iLO SNMP IM settings. For this command to parse correctly, the GET_SNMP_IM_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

GET_SNMP_IM_SETTINGS parameters

None

GET_SNMP_IM_SETTINGS runtime errors

None

GET_SNMP_IM_SETTINGS return messages

A possible GET_SNMP_IM_SETTINGS return message is:

```
<GET_SNMP_IM_SETTINGS>
   <SNMP_ADDRESS_1 VALUE="192.168.125.121"/>
   <SNMP_ADDRESS_2 VALUE="192.168.125.122"/>
   <SNMP_ADDRESS_3 VALUE="192.168.125.123"/>
   <OS_TRAPS VALUE="Yes"/>
   <RIB_TRAPS VALUE="No"/>
   <SNMP_PASSTHROUGH_STATUS VALUE="No"/>
   <WEB_AGENT_IP_ADDRESS VALUE="192.168.125.120"/>
```

```
   <CIM_SECURITY_MASK VALUE="3"/>
</GET_SNMP_IM_SETTINGS>
```

MOD_SNMP_IM_SETTINGS

MOD_SNMP_IM_SETTINGS is used to modify SNMP and Insight Manager settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <MOD_SNMP_IM_SETTINGS>
      <WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
      <SNMP_ADDRESS_1 value="192.168.125.121"/>
      <SNMP_ADDRESS_2 value="192.168.125.122"/>
      <SNMP_ADDRESS_3 value="192.168.125.123"/>
      <OS_TRAPS value="Yes"/>
      <RIB_TRAPS value="No"/>
      <SNMP_PASSTHROUGH_STATUS value="No"/>
      <CIM_SECURITY_MASK value="3"/>
   </MOD_SNMP_IM_SETTINGS>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

MOD_SNMP_IM_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

WEB_AGENT_IP_ADDRESS is the address for the Web-enabled agents. The value for this element has a maximum length of 50 characters. It can be any valid IP address. If an empty string is entered, the current value is deleted.

SNMP_ADDRESS_1, SNMP_ADDRESS_2, and SNMP_ADDRESS_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address and has a maximum value of 50 characters.

OS_TRAPS determines if the user should receive SNMP traps that are generated by the operating system. The possible values are "Yes" and "No." By default, the value is set to "No."

RIB_TRAPS determines if the user should receive SNMP traps that are generated by the RIB. The possible values are "Yes" and "No." By default, the value is set to "No."

SNMP_PASSTHROUGH_STATUS determines if iLO can receive/ send SNMP request from/ to the host OS. By default, the value is set to "Yes."

CIM_SECURITY_MASK accepts an integer between 0 and 4. The possible values are:

- **0**—No change
- **1**—None (No data is returned.)
- **2**—Low (Name and status data are returned. Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.)
- **3**—Medium (iLO and server associations are present but the summary page contains less detail than at high security.)
- **4**—High (Associations are present and all data is present on the summary page.)

Each value indicates the level of data returned over the HTTP port.

MOD_SNMP_IM_SETTINGS runtime errors

The possible MOD_SNMP_IM_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

CLEAR_EVENTLOG

The CLEAR_EVENTLOG command clears the iLO Event Log. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <CLEAR_EVENTLOG/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

CLEAR_EVENTLOG parameters

None

CLEAR_EVENTLOG runtime errors

The possible CLEAR_EVENTLOG error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

UPDATE_RIB_FIRMWARE

The UPDATE_RIB_FIRMWARE command copies a specified file to iLO, starts the upgrade process and reboots the board after the image has been successfully flashed. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\ILO140.BIN"/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

UPDATE_RIB_FIRMWARE parameters

IMAGE_LOCATION takes the full path file name of the firmware upgrade file.

UPDATE_RIB_FIRMWARE runtime errors

The possible UPDATE_RIB_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.
- IMAGE_LOCATION must not be blank.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_FW_VERSION

The GET_FW_VERSION command requests the respective iLO firmware information. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="read">
   <GET_FW_VERSION/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

GET_FW_VERSION parameters

None

GET_FW_VERSION runtime errors

None

GET_FW_VERSION return messages

The following information is returned within the response:

```
<GET_FW_VERSION
   FIRMWARE_VERSION = <firmware version>
   FIRMWARE_DATE = <firmware date>
   MANAGEMENT_PROCESSOR = <management processor type>
/>
```

HOTKEY_CONFIG

The HOTKEY_CONFIG command configures the remote console hot key settings in iLO. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Uppercase letters are not supported, and they will be converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. Specifying a blank string removes the current value.

Refer to the "Supported Hot Keys" section for a complete list of supported hotkeys.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <HOTKEY_CONFIG>
      <CTRL_T value="CTRL,ALT,ESC"/>
      <CTRL_U value="L_SHIFT,F10,F12"/>
      <CTRL_V value=""/>
      <CTRL_Y value=""/>
      <CTRL_X value=""/>
      <CTRL_Y value=""/>
   </HOTKEY_CONFIG>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

HOTKEY_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

CTRL_T specifies settings for the CTRL_T hot key. The settings must be separated by commas. For example, CTRL_T="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_U specifies settings for the CTRL_U hot key. The settings must be separated by commas. For example, CTRL_U="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_V specifies settings for the CTRL_V hot key. The settings must be separated by commas. For example, CTRL_V="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_W specifies settings for the CTRL_W hot key. The settings must be separated by commas. For example, CTRL_W="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_X specifies settings for the CTRL_X hot key. The settings must be separated by commas. For example, CTRL_X="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_Y specifies settings for the CTRL_Y hot key. The settings must be separated by commas. For example, CTRL_Y="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

HOTKEY_CONFIG runtime errors

The possible HOTKEY_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

LICENSE

The LICENSE command activates or deactivates the iLO's advanced features. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

On a ProLiant BL Class server, there is no need for a licensing key. Advanced features are automatically activated.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <LICENSE>
      <ACTIVATE KEY="11111222223333344444455555"/>
   </LICENSE>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

LICENSE parameters

ACTIVATE followed by a valid KEY value signals the activation of the iLO advanced pack licensing.

KEY specifies the license key value. The key should be entered as one continuous string. Commas, periods, or other characters should not separate the key value. The key will only accept 25 characters; other characters entered to separate key values will be interpreted as a part of the key and result in the wrong key being entered.

DEACTIVATE signals the deactivation of the iLO advanced pack licensing.

LICENSE runtime errors

The possible LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

DIR_INFO

The DIR_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local directory information database into memory and prepares to edit it. Only commands that are DIR_INFO type commands are valid inside the DIR_INFO command block. The DIR_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:

```
<DIR_INFO MODE="read">
   …… DIR_INFO commands ……
</DIR_INFO>
```

DIR_INFO parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of directory information. Read mode prevents modification of directory information.

DIR_INFO runtime errors

None

GET_DIR_CONFIG

The GET_DIR_CONFIG command requests the respective iLO directory settings. For this command to parse correctly, the GET_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
```

```
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <DIR_INFO MODE="read">
   <GET_DIR_CONFIG/>
   </DIR_INFO>
   </LOGIN>
</RIBCL>
```

GET_DIR_CONFIG parameters

None

GET_DIR_CONFIG runtime errors

None

GET_DIR_CONFIG return messages

A possible GET_DIR_CONFIG return message is:

```
<GET_DIR_CONFIG>
   <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
   <DIR_LOCAL_USER_ACCT VALUE="Y"/>
   <DIR_SERVER_ADDRESS VALUE="server1.hprib.labs"/>
   <DIR_SERVER_PORT VALUE="636"/>
   <DIR_OBJECT_DN VALUE="CN=SERVER1_RIB, OU=RIB,
   DC=HPRIB, DC=LABS"/>
   <DIR_USER_CONTEXT1 VALUE="CN=Users0, DC=HPRIB0,
   DC=LABS"/>
   <DIR_USER_CONTEXT2 VALUE="CN=Users1, DC=HPRIB1,
   DC=LABS"/>
   <DIR_USER_CONTEXT3 VALUE=""/>
</GET_DIR_CONFOG>>
```

MOD_DIR_CONFIG

MOD_DIR_CONFIG command is used modify the directory settings on iLO. For this command to parse correctly, the MOD_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <DIR_INFO MODE="write">
   <MOD_DIR_CONFIG>
      <DIR_AUTHENTICATION_ENABLED value="Yes"/>
      <DIR_LOCAL_USER_ACCT value="Yes"/>
      <DIR_SERVER_ADDRESS value="16.141.100.44"/>
      <DIR_SERVER_PORT value="636"/>
      <DIR_OBJECT_DN value="CN=server1_rib, OU=RIB,
      DC=HPRIB, DC=LABS"/>
      <DIR_OBJECT_PASSWORD value="password"/>
      <DIR_USER_CONTEXT_1 value="CN=Users, DC=HPRIB,
      DC=LABS"/>
   </MOD_DIR_CONFIG>
   </DIR_INFO>
   </LOGIN>
</RIBCL>
```

MOD_DIR_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DIR_AUTHENTICATION_ENABLED enables or disables directory authentication. The possible values are "Yes" and "No."

DIR_LOCAL_USER_ACCT enables or disables local user accounts. The possible values are "Yes" and "No."

DIR_SERVER_ADDRESS specifies the location of the directory server. The directory server location is specified as an IP address or DNS name.

DIR_SERVER_PORT specifies the port number used to connect to the directory server. This value is obtained from the directory administrator. The secure LDAP port is 636, but the directory server can be configured for a different port number.

DIR_OBJECT_DN specifies the unique name of iLO in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

DIR_OBJECT_PASSWORD specifies the password associated with the iLO object in the directory server. Passwords are limited to 39 characters.

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2, and DIR_USER_CONTEXT_3 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user could not be located using the first path, then the parameters specified in the second and third paths are used. The values for these parameters are obtained from the directory administrator. Directory User Contexts are limited to 128 characters each.

MOD_DIR_CONFIG runtime errors

The possible MOD_DIR_CONFIG error messages include:

- Directory information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

RACK_INFO

The RACK_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the rack infrastructure database into memory and prepares to edit it. Only commands that are RACK_INFO type commands are valid inside the RACK_INFO command block. The RACK_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

This command block is only valid on ProLiant BL Class servers.

Example:

```
<RACK_INFO MODE="read">
…… RACK_INFO commands ……
</RACK_INFO>
```

RACK_INFO parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of rack infrastructure information. Read mode prevents modification of rack infrastructure information.

RACK_INFO runtime errors

The possible RACK_INFO error messages include:

- Invalid Mode.
- Server is not a rack server; rack commands do not apply.

RIBCL RACK_INFO commands

Several new XML commands have been added to the RIBCL structure to support reading and writing of Static IP Bay Configuration in scripting. The new RIBCL commands must be scripted within a RACK_INFO (on page 137) command block. The new attributes are:

- MOD_ENCLOSURE_IP_SETTINGS—Modifies the Static IP Bay Configuration settings. This command is only valid inside a RACK_INFO block. The logged-in user must have the configure iLO privilege. This attribute must appear inside the RACK_INFO command block with MODE = "write."

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

RIBCL RACK_INFO command examples

Getting Static IP Bay Configuration Settings

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

Modifying Static IP Bay Configuration Settings

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RACK_INFO MODE="write">
   <MOD_ENCLOSURE_IP_SETTINGS>
      <BAY_ENABLE MASK="0x3FE"/>
      <IP_ADDRESS VALUE="16.100.222.111"/>
      <SUBNET_MASK VALUE="255.255.252.0"/>
      <GATEWAY_IP_ADDRESS VALUE="16.100.222.1"/>
      <DOMAIN_NAME VALUE="sum.won.here.now"/>
```

```
      <PRIM_DNS_SERVER VALUE="16.11.1.111"/>
      <SEC_DNS_SERVER VALUE=""/>
      <TER_DNS_SERVER VALUE=""/>
      <PRIM_WINS_SERVER VALUE="16.22.2.222"/>
      <SEC_WINS_SERVER VALUE=""/>
      <STATIC_ROUTE_1 DEST="16.33.3.33"
      GATEWAY="16.100.11.11"/>
      <STATIC_ROUTE_2 DEST="" GATEWAY=""/>
      <STATIC_ROUTE_3 DEST="" GATEWAY=""/>
   </MOD_ENCLOSURE_IP_SETTINGS>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

Modify Network Settings to Enable Static IP Bay Configuration

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

MOD_BLADE_RACK

MOD_BLADE_RACK command is used to modify the rack infrastructure settings. For this command to parse properly, the MOD_BLADE_RACK command must appear within a RACK_INFO command block, and RACK_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="write">
   <MOD_BLADE_RACK>
      <RACK_NAME value="CPQ_Rack_1"/>
      <ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
      <BAY_NAME value="CPQ_Bay_5"/>
      <FACILITY_PWR_SOURCE value="Yes"/>
```

```
        <RACK_AUTO_PWR value="Yes"/>
        <SNMP_RACK_ALERTS value="Yes"/>
        <LOG_RACK_ALERTS value="Yes"/>
    </MOD_BLADE_RACK>
    </RACK_INFO>
    </LOGIN>
</RIBCL>
```

MOD_BLADE_RACK parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

RACK_NAME is the name used to logically group together enclosures in a single rack infrastructure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

ENCLOSURE_NAME is the name used to logically group together the ProLiant BL-Class servers that compose a single enclosure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

BAY_NAME is the name used to identify a particular ProLiant BL-Class server. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

FACILITY_PWR_SOURCE determines the source of power for the blade servers. A value of "Yes" directs the server to use facility power and a value of "No" directs the server to use the server blade power supplies.

RACK_AUTO_PWR determines if the blade server should automatically power when inserted into the enclosure. A value of "Yes" causes the blade server to automatically power up and begin normal booting process if power is available. A value of "No" requires the blade server to be manually powered on.

SNMP_RACK_ALERTS determines if alerts from the rack infrastructure should be forwarded to user-defined SNMP trap destinations. A value of "Yes" enables rack alerts to be forwarded. A value of "No" disables rack alerts from being forwarded.

LOG_RACK_ALERTS determines if alerts from the rack infrastructure should be logged. A value of "Yes" enables rack alerts to be logged in the IML log. A value of "No" disables the logging of rack alerts in the IML log.

MOD_BLADE_RACK runtime errors

The possible MOD_BLADE_RACK error messages include:

- Rack information is open for read-only access. Write access is required for this operation.
- Rack Name too long.
- Enclosure Name too long.
- Bay Name too long.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_RACK_SETTINGS

The GET_RACK_SETTINGS command requests the respective iLO's rack settings. For this command to parse correctly, the GET_RACK_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="read">
   <GET_RACK_SETTINGS/>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

GET_RACK_SETTINGS parameters

None

GET_RACK_SETTINGS runtime errors

None

GET_RACK_SETTINGS return messages

A possible GET_RACK_SETTINGS return message is:

```
<GET_RACK_SETTINGS>
   <RACK_NAME VALUE="HPspace"/>
   <ENCLOSURE_NAME VALUE="Home"/>
   <ENCLOSURE_SN VALUE="44XP0606XP33"/>
   <BAY_NAME VALUE="Library"/>
   <BAY VALUE="2"/>
   <FACILITY_PWR_SOURCE VALUE="N"/>
   <RACK_AUTO_PWR VALUE="Y"/>
   <SNMP_RACK_ALERTS VALUE="Y"/>
   <LOG_RACK_ALERTS VALUE="N"/>
</GET_RACK_SETTINGS >
```

GET_DIAGPORT_SETTINGS

The GET_DIAGPORT_SETTINGS command requests the respective iLO diagnostic port settings. For this command to parse correctly, the GET_DIAGPORT_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="read">
   <GET_DIAGPORT_SETTINGS/>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

GET_DIAGPORT_SETTINGS parameters

None

GET_DIAGPORT_SETTINGS runtime errors

None

GET_DIAGPORT_SETTINGS return messages

A possible GET_DIAGPORT_SETTINGS return message is:

```
<GET_DIAGPORT_SETTINGS>
   <DP_SPEED_AUTOSELECT value="No"/>
   <DP_NIC_SPEED value="100"/>
   <DP_FULL_DUPLEX value="Yes"/>
   <DP_IP_ADDRESS value="192.168.142.56"/>
   <DP_SUBNET_MASK value="255.255.0.0"/>
</GET_DIAGPORT_SETTINGS >
```

MOD_DIAGPORT_SETTINGS

The MOD_DIAGPORT_SETTINGS command is used modify the diagnostic port network settings on iLO. For this command to parse correctly, the MOD_DIAGPORT_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE must be set to write. The user must have the configure iLO privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="username" PASSWORD="password">
   <RACK_INFO MODE="write">
   <MOD_DIAGPORT_SETTINGS>
      <DP_SPEED_AUTOSELECT value="No"/>
      <DP_NIC_SPEED value="100"/>
      <DP_FULL_DUPLEX value="Yes"/>
      <DP_IP_ADDRESS value="192.168.142.56"/>
      <DP_SUBNET_MASK value="255.255.0.0"/>
   </MOD_DIAGPORT_SETTINGS>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

MOD_DIAGPORT_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DP_SPEED_AUTOSELECT is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

DP_NIC_SPEED is used to set the transceiver speed if DP_SPEED_AUTOSELECT was set to "No." The possible values are 10 or 100. Any other value results in a syntax error.

DP_FULL_DUPLEX is used to decide if the iLO diagnostic port is to support full-duplex or half-duplex mode. It is only applicable if DP_SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

DP_IP_ADDRESS is used to select the IP address for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is *XXX.XXX.XXX.XXX*.

DP_SUBNET_MASK is used to select the subnet mask for the iLO Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is *XXX.XXX.XXX.XXX*.

The iLO management processor will be rebooted to apply the changes after the script has completed successfully.

MOD_DIAGPORT_SETTINGS runtime errors

Possible MOD_DIAGPORT_SETTINGS error messages include:

- iLO information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_TOPOLOGY

The GET_TOPOLOGY command requests the respective iLO to return the current topology of the rack infrastructure. For this command to parse correctly, the GET_TOPOLOGY command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RACK_INFO MODE="read">
      <GET_TOPOLOGY/>
   </RACK_INFO>
   </LOGIN>
</RIBCL>
```

GET_TOPOLOGY parameters

None

GET_TOPOLOGY return message

An example of a successful request follows:

```
<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123"
NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456"
NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789"
NAME="Power_2">
<RIGHT/>
</ICMB>
```

```
</RK_TPLGY>
```

SERVER_INFO

The SERVER_INFO command can only appear within a LOGIN command block. Only commands that are SERVER_INFO type commands are valid inside the SERVER_INFO command block.

Example:

```
<SERVER_INFO MODE="read">
…… SERVER_INFO commands ……
</SERVER_INFO>
```

SERVER_INFO parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and modifying of server functionality. Read mode prevents modification of server functionality.

SERVER_INFO runtime errors

None

GET_HOST_POWER_SAVER_STATUS

The GET_HOST_POWER_SAVER_STATUS command requests the state of the processor power regulator feature of the server. For this command to parse correctly, the GET_HOST_POWER_SAVER_STATUS command must appear within a SERVER_INFO command block, and SEVER_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
```

```
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <GET_HOST_POWER_SAVER_STATUS/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

GET_HOST_POWER_SAVER_STATUS parameters

None

GET_HOST_POWER_SAVER_STATUS runtime errors

The possible GET_HOST_POWER_SAVER_STATUS error messages include:

- Feature not supported

GET_HOST_POWER_SAVER_STATUS return messages

The following information is returned within one of the following responses:

- ```
  <GET_HOST_POWER_SAVER
     HOST POWER_SAVER="MAX"
     />
  ```
- ```
  <GET_HOST_POWER_SAVER
     HOST POWER_SAVER="MIN"
     />
  ```
- ```
  <GET_HOST_POWER_SAVER
     HOST POWER_SAVER="AUTO"
     />
  ```
  ```

SET_HOST_POWER_SAVER

The SET_HOST_POWER_SAVER command is used to set the Power Regulator Setting for the server processor. For this command to parse correctly, the SET_HOST_POWER_SAVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <SET_HOST_POWER_SAVER HOST_POWER_SAVER="1"/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

SET_HOST_POWER_SAVER parameters

HOST_POWER_SAVER controls the Dynamic Power Saver feature of the server processor if the feature is supported. The possible values are:

- 1 for Max
- 2 for Min
- 3 for Auto

SET_HOST_POWER_SAVER runtime errors

The possible SET_HOST_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Power Regulator feature is not supported on this server.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

RESET_SERVER

The RESET_SERVER command will force a warm boot of the server, if the server is currently on. For this command to parse correctly, the RESET_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
   <RESET_SERVER/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

RESET_SERVER errors

The possible RESET_SERVER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Server is currently powered off.
- User does NOT have correct privilege for action. RESET_SERVER_PRIV required.

RESET_SERVER parameters

None

PRESS_PWR_BTN

This PRESS_PWR_BTN command is used to simulate a physical press of the server power button. For this command to parse correctly, the PRESS_PWR_BTN command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <PRESS_PWR_BTN/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

PRESS_PWR_BTN parameters

There are no parameters for this command.

PRESS_PWR_BTN runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

HOLD_PWR_BTN

This HOLD_PWR_BTN command is used to simulate a physical press and hold of the server power button. For this command to parse correctly, the HOLD_PWR_BTN command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <HOLD_PWR_BTN/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

HOLD_PWR_BTN parameters

There are no parameters for this command.

HOLD_PWR_BTN runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

COLD_BOOT_SERVER

This COLD_BOOT_SERVER command will force a cold boot of the server, if the server is currently on. For this command to parse correctly, the COLD_BOOT_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <COLD_BOOT_SERVER/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

COLD_BOOT_SERVER parameters

There are no parameters for this command.

COLD_BOOT_SERVER runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

WARM_BOOT_SERVER

This WARM_BOOT_SERVER command will force a warm boot of the server, if the server is currently on. For this command to parse correctly, the WARM_BOOT_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <WARM_BOOT_SERVER/>
   </SERVER_INFO>
</LOGIN>
</RIBCL>
```

WARM_BOOT_SERVER parameters

There are no parameters for this command.

WARM_BOOT_SERVER runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

GET_UID_STATUS

The UID_STATUS command requests the state of the server UID. For this command to parse correctly, the UID_STATUS command must appear within a SERVER_INFO command block, and SEVER_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <GET UID_STATUS />
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

GET_UID_STATUS parameters

None

GET_UID_STATUS response

The following information is returned within the response:

```
<GET_UID_STATUS
   UID="OFF"
/>
```

UID_CONTROL

The UID_CONTROL command toggles the server UID. For this command to parse correctly, the UID_CONTROL command must appear within a SERVER_INFO command block, and SEVER_INFO MODE must be set to write.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <SERVER_INFO MODE="write">
      <UID_CONTROL UID="Yes"/>
   </SERVER_INFO>
   </LOGIN>
</RIBCL>
```

UID_CONTROL parameters

UID determines the state of the UID. A value of "Yes" turns the UID light on, and a value of "No" turns the UID light off.

UID_CONTROL errors

The possible UID_CONTROL error messages include:

- UID is already ON.
- UID is already OFF.

INSERT_VIRTUAL_MEDIA

This command notifies iLO of the location of a diskette image. The INSERT_VIRTUAL_MEDIA command must display within a RIB_INFO element, and RIB_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
```

```
   <LOGIN USER_LOGIN = "adminname" PASSWORD =
   "password">
   <RIB_INFO MODE = "write">
      <INSERT_VIRTUAL_MEDIA DEVICE "FLOPPY" IMAGE_URL =
      "http://servername/path/to/file"/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

INSERT_VIRTUAL_MEDIA Parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

IMAGE_URL specifies the URL to the diskette image. The URL format is as follows:

```
protocol://username:password@hostname:port/filename,cgi-
helper
```

- The protocol field is mandatory and must be either http or https.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional
- The filename field is mandatory.
- The cgi-helper field is optional.

In addition, the filename field may contain tokens that expand to host specific strings:

- %m expands to the iLO MAC address.
- %i expands to the iLO IP address in dotted-quad form.
- %h expands to the iLO hostname.

Examples:

```
http://john:abc123@imgserver.company.com/disk/win98dos.b
in,/cgi-bin/hpvfhelp.pl
```

```
http://imgserver.company.com/disk/boot%m.bin
```

This command only specifies the location of the image to be used. For the image to be connected to the server, the appropriate BOOT_OPTION must be specified using the SET_VM_STATUS command.

If BOOT_OPTION is set to BOOT_ONCE and the server is rebooted, any subsequent server reboots eject the image.

After an image is inserted using this command, the Virtual Media applet cannot connect its Virtual Media devices and subsequent scripts cannot use the INSERT_VIRTUAL_FLOPPY command until the image is ejected.

INSERT_VIRTUAL_FLOPPY runtime errors

The possible INSERT_VIRTUAL_FLOPPY error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- IMAGE_URL must not be blank.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- Unable to parse Virtual Media URL
- An invalid Virtual Media option has been given.
- Virtual Media already connected through a script. You must eject or disconnect before inserting new media.

EJECT_VIRTUAL_MEDIA

EJECT_VIRTUAL_MEDIA ejects the Virtual Media image if one is inserted. The EJECT_VIRTUAL_MEDIA command must display within a RIB_INFO element and RIB_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="Password">
```

```
   <RIB_INFO MODE="write">
      <EJECT_VIRTUAL_MEDIA />
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

EJECT_VIRTUAL_MEDIA parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

EJECT_VIRTUAL_MEDIA runtime errors

The possible EJECT_VIRTUAL_MEDIA errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- No image present in the Virtual Media drive.
- An invalid Virtual Media option has been given.

GET_VM_STATUS

GET_VM_STATUS returns the Virtual Media drive status. This command must display within a RIB_INFO element.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
   <RIB_INFO MODE = "read">
      <GET_VM_STATUS DEVICE = "CDROM"/>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

GET_VM_STATUS parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

GET_VM_STATUS runtime errors

The possible GET_VM_STATUS error is:

An invalid Virtual Media option has been given.

GET_VM_STATUS return messages

The return message displays the current state of the Virtual Media. The VM_APPLET parameter shows if a virtual media device is already connected via the Virtual Media Applet. If the VM_APPLET = CONNECTED, then the Virtual Media is already in use and cannot be connected via scriptable Virtual Media or Virtual Media XML commands. The DEVICE parameter tells which device this return message is for. The BOOT_OPTION shows the current setting; BOOT_ALWAYS means that the server will always use the Virtual Media device for booting, BOOT_ONCE means that the server will boot to the Virtual Device once and then disconnect the Virtual Media on the subsequent server reboot, and NO_BOOT means that the Virtual Media will not be connected during a server reboot. The WRITE_PROTECT_FLAG parameter shows if the Virtual Media image can be written to. The IMAGE_INSERTED parameter tells if the Virtual Media device is connected via the scriptable Virtual Media or the Virtual Media XML command.

A possible GET_VM_STATUS return message is:

```
VM_APPLET = CONNECTED | DISCONNECTED
DEVICE = FLOPPY | CDROM
BOOT_OPTION = BOOT_ALWAYS | BOOT_ONCE | NO_BOOT
WRITE_PROTECT_FLAG = YES | NO
IMAGE_INSERTED = YES | NO
```

NOTE: If the BOOT_ONCE boot option is selected, all scriptable virtual media parameters are reset to default settings after the server boots. Specifically BOOT_OPTION = NO_BOOT, WRITE_PROTECT = NO, and IMAGE_INSERTED = NO.

SET_VM_STATUS

SET_VM_STATUS sets the Virtual Media drive status. This command must display within a RIB_INFO element, and RIB_INFO must be in write mode. All the parameters in the command are optional.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
   <RIB_INFO MODE = "write">
   <SET_VM_STATUS DEVICE = "CDROM">
      <VM_BOOT_OPTION value = "BOOT_ONCE"/>
      <VM_WRITE_PROTECT value = "Y"/>
   </ SET_VF_STATUS>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

SET_VM_STATUS parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

VM_BOOT_OPTION specifies the boot option parameter for the Virtual Media. The possible values are BOOT_ALWAYS, BOOT_ONCE, or NO_BOOT. These values control how the Virtual Media device behaves during the boot phase of the server. Setting these values does not affect the current state of the Virtual Media device. These settings only take affect if the Virtual Media device is connected at server boot.

- BOOT_ALWAYS sets the VM_BOOT_OPTION to BOOT_ALWAYS. The Virtual Media device will always be connected during server boot. The Virtual Media device is not connected immediately when the VM_BOOT_OPTION is set. The Virtual Media device is connected on the next server boot after setting of the VM_BOOT_OPTION.

- BOOT_ONCE sets the VM_BOOT_OPTION to BOOT_ONCE. The Virtual Media device is connected during the next server boot, but on any subsequent server boots, it will not be connected. The BOOT_ONCE option is intended to boot one time to the Virtual Media device, use that device while the server is running, and then not have the Virtual Media device available on subsequent server reboots. The Virtual Media device is not connected immediately when the VM_BOOT_OPTION is set. The Virtual Media device is connected on the next server boot following the setting of the VM_BOOT_OPTION. After the server has booted once with the Virtual Media device connected, on the subsequent server reboot, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
  - BOOT_OPTION=NO_BOOT
  - IMAGE_INSERTED = NO
- NO_BOOT sets the VM_BOOT_OPTION to NO_BOOT. The Virtual Media device is not connected during the next server boot. The Virtual Media device is not disconnected immediately when the VM_BOOT_OPTION is set. The Virtual Media device will be disconnected on the next server boot following the setting of the VM_BOOT_OPTION. After the server has booted, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
  - BOOT_OPTION = NO_BOOT
  - IMAGE_INSERTED = NO

In addition to the VM_BOOT_OPTIONS, CONNECT and DISCONNECT are also possible values. The CONNECT and DISCONNECT settings can be used to control the Virtual Media devices in the same way that they are controlled in the Virtual Media applet. Whenever the CONNECT or DISCONNECT parameters are set, the Virtual Media device immediately connects or disconnects, respectively, to the server.

- CONNECT sets the VM_BOOT_OPTION to CONNECT. The Virtual Media device is immediately connected to the server. Setting the VM_BOOT_OPTION to CONNECT is equivalent to clicking the device **Connect** button on the Virtual Media Applet. After setting the VM_BOOT_OPTION to CONNECT, the VM_GET_STATUS command will show the VM_BOOT_OPTION as BOOT_ALWAYS. This is by design and shows that the Virtual Media device is connected like the Virtual Media device in the applet which with always be connected during all server boots.
- DISCONNECT sets the VM_BOOT_OPTION to DISCONNECT. The Virtual Media device is immediately disconnected from the server. Setting the VM_BOOT_OPTION to DISCONNECT is equivalent to clicking the device **Disconnect** button on the Virtual Media Applet. Additionally, setting the VM_BOOT_OPTION to DISCONNECT is equivalent to issuing the EJECT_VIRTUAL_MEDIA command. When the VM_BOOT_OPTION is set to DISCONNECT, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
  - BOOT_OPTION = NO_BOOT
  - IMAGE_INSERTED = NO

VM_WRITE_PROTECT sets the write protect flag value for the Virtual Floppy. This value is not significant for the Virtual Media CD-ROM. The possible values are Y or N.

SET_VM_STATUS runtime errors

The possible runtime errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- An invalid Virtual Media option has been given.

CERTIFICATE_SIGNING_REQUEST

This command requests a certificate from iLO. When this command is received iLO generates a certificate signing request. The request is returned to the user enclosed in a CERTIFICATE_SIGNING_REQUEST tag. This command requires CPQLOCFG version 2.23 or later.

Example:

```
<RIBCL VERSION="1.2">
   <LOGIN USER_LOGIN = "adminname" PASSWORD =
   "password">
   <RIB_INFO MODE = "write">
      <CERTIFICATE_SIGNING_REQUEST/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

CERTIFICATE_SIGNING_REQUEST parameters

There are no parameters for this command.

CERTIFICATE_SIGNING_REQUEST errors

There are no errors for this command.

IMPORT_CERTIFICATE

The IMPORT_CERTIFICATE command imports a signed certificate into iLO. The signed certificate must be a signed version of a certificate signing request. This command requires CPQLOCFG version 2.23 or later.

Example:

```
<RIBCL VERSION="1.2">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
   <RIB_INFO MODE = "write">
      <IMPORT_CERTIFICATE>
      -----BEGIN CERTIFICATE-----
      ….
```

```
      -----END CERTIFICATE-----
      </IMPORT_CERTIFICATE>
   </RIB_INFO>
</LOGIN>
</RIBCL>
```

IMPORT_CERTIFICATE parameters

There are no parameters for this command.

IMPORT_CERTIFICATE errors

The possible IMPORT_CERTIFICATE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Error reading certificate: The imported certificate is invalid.
- Invalid certificate common name: The common name in the certificate does not match iLO's hostname.
- Certificate signature does not match private key: The certificate does not correspond to the private key stored in iLO.

HPQLOMGC command language

When using HPQLOMGC, the directory settings for the management processor are read from an XML file. The script used is a subset of the RIBCL and has been extended to support multiple management processor firmware images. For more information concerning RIBCL for your management processor, refer to the RILOE, RILOE II, or iLO user guide.

The following is an example of an XML file:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="user" PASSWORD="password">
<DIR_INFO MODE="write">
<ILO_CONFIG>
```

```
   <UPDATE_RIB_FIRMWARE
   IMAGE_LOCATION="C:\fw\ilo140.brk" />
</ILO_CONFIG>
<RILOE_CONFIG>
   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloe.brk"
   />
</RILOE_CONFIG>
<RILOE2_CONFIG>
   <UPDATE_RIB_FIRMWARE
   IMAGE_LOCATION="C:\fw\riloeii.brk" />
</RILOE2_CONFIG>
<MOD_DIR_CONFIG>
   <DIR_AUTHENTICATION_ENABLED value="YES" />
   <DIR_LOCAL_USER_ACCT value="YES" />
   <DIR_SERVER_ADDRESS
   value="administration.wins.hp.com" />
   <DIR_SERVER_PORT value="636" />
   <DIR_OBJECT_DN
   value="CN=RILOP5,CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_OBJECT_PASSWORD value="aurora" />
   <DIR_USER_CONTEXT_1
   value="CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_USER_CONTEXT_2 value="" />
   <DIR_USER_CONTEXT_3 value="" />
   <DIR_ROLE
   value="CN=RILOEROLE,CN=Users,DC=RILOEGRP2,DC=HP" />
   <DIR_LOGIN_NAME value="RILOEGRP2\Adminl" />
   <DIR_LOGIN_PASSWORD value="aurora" />
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

ILO_CONFIG

RIBCL allows for only one firmware image per XML file. The command language for HPQLOMGC has been modified to allow for each management processor to have a specified firmware image within a single XML file. These commands must be displayed within a DIR_INFO block, and DIR_INFO must be in write mode. The management processor is reset after the firmware upgrade is complete. To update the firmware, the user must be logged in with the appropriate privilege.

This command line uses the following parameters:

- UPDATE_RIB_FIRMWARE IMAGE_LOCATION ("UPDATE_RIB_FIRMWARE parameters" on page 129)
- MOD_DIR_CONFIG

iLO ports

In this section

Enabling the iLO Shared Network Port feature through XML scripting

For information on how to use the SHARED_NETWORK_PORT command to enable the iLO Shared Network Port through XML scripting, refer to the "Remote Insight command language (on page 95)" section.

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

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

Re-enabling the dedicated iLO management port

The iLO RBSU (described in the *HP Insight-Lights Out 1.70 User Guide*) or XML scripting must be used to re-enable the iLO dedicated NIC management port. For information on how to use the SHARED_NETWORK_PORT command to re-enable the iLO dedicated management port refer to the "Remote Insight command language (on page 95)" section.

To re-enable the dedicated management port:

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

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

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

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

iLO parameters

In this section

iLO Status parameters

Parameter	Default value	Definition
Current user		Display the user currently logged into iLO through this browser.
Remote console		Displays whether the remote console is available to the current user.
Terminal services	Disabled	Displays whether the pass-through software to support Microsoft® Terminal Services is present.
iLO time		Displays the time as indicated by the Integrated Lights-Out subsystem internal clock. The iLO internal clock is synchronized with the host system at POST and when the Insight Agents run.
iLO date		Displays the date (MM/DD/YYYY) as indicated by the iLO subsystem internal calendar. The iLO internal calendar is synchronized with the host system at POST and when the Insight Agents run.
iLO firmware version	*XX.XX*	Displays the firmware revision level of the iLO subsystem.

Parameter	Default value	Definition
iLO serial number	iLO*XXXXXXXXXXXX*	Displays the serial number, derived from the host serial number, associated with this iLO.
Product version		Displays the iLO product functionality currently licensed.
License expires		Displays the remaining time in the iLO Advanced evaluation period and is only displayed only when evaluation licenses are installed.

Server Status parameters

Parameter	Default value	Definition
Server name		If the Insight Management agents are being used with the host server operating system, they will provide iLO with the server name.
Server ID		Displays the serial number of the server.
Server power status		Displays whether the host is powered ON, or in STANDBY (OFF) mode.
Server video mode		Displays the state of the host server video controller as interpreted by Remote Console.
Server keyboard		Displays the keyboard type as emulated by Remote Console.
Server mouse		Displays the mouse type as emulated by Remote Console.

User Administration parameters

Parameter	Default value	Definition
User name	Administrator	This parameter is the user's real name as it is displayed in the user list and event log. It is not the name used to log in. The maximum length of the user name is 39 characters.

Parameter	Default value	Definition
Login name	Administrator	This is a case-sensitive name that the user must provide to log in to iLO.
Password	A random, eight-character alphanumeric string that is factory assigned	This is a case-sensitive password that the user must provide to log in to iLO. In Security Options, the minimum password length can be assigned. The minimum password can be from 0 to 39 characters. The default minimum password length is eight characters. You must enter the password twice for verification.
Administer user accounts	Yes	This privilege allows a user to add, modify, and delete user accounts. It also allows the user to alter privileges for all users, including granting all permissions to a user.
Remote console access	Yes	This privilege allows a user to remotely manage the Remote Console of a managed system, including video, keyboard, and mouse controls.
Virtual power and reset	Yes	This privilege allows a user to power-cycle or reset the host platform.
Virtual media	Yes	This privilege allows a user to use virtual media on the host platform.
Configure iLO settings	Yes	This privilege enables a user to configure most iLO settings, including security settings. It does not include user account administration. After iLO is correctly configured, revoking this privilege from all users prevents reconfiguration. A user with the Administer User Accounts privilege can enable or disable this privilege. iLO can also be reconfigured if iLO RBSU is enabled.

Global Settings parameters

Parameter	Default value	Definition
Idle connection timeout (minutes)	30 minutes	This setting specifies the interval of user inactivity, in minutes, before the Web server and Remote Console session are automatically terminated.
Enable Lights-Out functionality	Yes	This option enables connection to iLO. If disabled, all connections to iLO are prevented. The default setting is Yes. • The iLO 10/100 network and communications with operating system drivers will be turned off if Lights-Out functionality is disabled. The iLO Diagnostic Port for a ProLiant BL p Class server is disabled as well. • If iLO functionality, including the iLO Diagnostic Port, is disabled, you must use the Security Override Switch in the server to enable iLO functionality. Follow the server documentation of the server to locate the Security Override Switch and set it to the override position. Power on the server and use the iLO RBSU to set Enable Lights-Out Functionality.
Pass-Through configuration	Disabled	
Enable iLO ROM-Based Setup Utility	Yes	This setting enables a user with access (physical or virtual) to the host to configure iLO for that system using iLO RBSU. RBSU is invoked when the host system reboots and performs POST. The default setting is Yes. You can restrict RBSU access to authorized users by selecting **Require Login for iLO RBSU.** **NOTE:** If the physical security jumper is set, the RBSU prompt displays during reboot.

Parameter	Default value	Definition
Require login for iLO RBSU	No	This setting controls the ability of iLO to pass-through a connection between a Microsoft® Terminal Services client and Terminal Services server running on the server that has the iLO installed. There are three options: • **Automatic** means when remote console is started, the Terminal Services client will be launched. • **Enabled** means the pass-through feature is enabled but will not launch automatically. You must click the Terminal Svcs button in Remote Console to start the client. • **Disabled** means that the pass-through feature is off.
Show iLO during POST	No	This setting specifies if iLO is displayed during POST. The default setting is No.
Remote console port configuration	Automatic	This setting enables or disables configuring of the port address. • **Enabled** allows Telnet and Remote Console applet access. • **Automatic** allows Remote Console applet access but not Telnet access. • **Disabled** turns off both Telnet and Remote Console applet access. Remote Console Data Encryption must be set to **No** to use Telnet to access the text Remote Console.
Remote console data encryption	Yes	This setting enables encryption of Remote Console data. If using a standard Telnet client to access iLO, this setting must be set to No. When using the Remote Console applet, all data is encrypted regardless of this setting.
SSL encryption strength	128-bit	This setting displays the current cipher strength setting. The most secure is 128-bit (High).
Current cipher	Negotiated by the iLO and the browser	This setting displays the encryption algorithm currently being used to protect data during transmission between the browser and the iLO.
Web server Non-SSL port	80	The embedded Web server in iLO is configured by default to use port 80 for unencrypted communications. This port setting is configurable in the Global Settings option of the Administration tab.

Parameter	Default value	Definition
Web server SSL port	443	The embedded Web server in iLO is configured by default to use port 443 for encrypted communications. This port setting is configurable in the Global Settings option of the Administration tab.
Virtual media port	17988	The Virtual Media support in iLO uses a configurable port for its communications. This port can be set in the Global Settings option of the Administration tab. The default setting is to use port 17988.
Remote console port	23	The iLO Remote Console is configured by default to use port 23 for Remote Console communications. This port setting is configurable in the Global Settings option of the Administration tab.
Terminal services port	3389	The Terminal Services port is the port that iLO uses to communicate with Terminal Services pass-through software on the server. The iLO Terminal Services pass-through is configured by default to use port 3389 for encrypted communications. If the Terminal Services pass-through port is configured to anything other than the default, the port number in Windows® 2000 must be manually changed to match it. This port setting is configurable in the Global Settings option of the Administration tab.
Secure shell(SSH) port	22	The iLO SSH port is configured by default to use port 22 for SSH communications. This port setting is configurable in the Global Settings option of the Administration tab. Valid values are from 1 to 65535.
Secure shell(SSH) Access	Enabled	This setting enables you to specify if the SSH feature on iLO is enabled or disabled. The default is enabled.
Serial command line interface status	Enabled (authentication required)	This setting allows you to change the status of the CLI feature through the serial port. Valid settings are: • Enabled (authentication required) • Enabled (no authentication) • Disabled The default setting is Enabled—authentication required.

Parameter	Default value	Definition
Serial command line interface speed (bits/second)	9600	This setting enables you to change the speed of the serial port for the CLI feature through the serial port. Valid speeds are (bits/s) 9,600, 19,200, 38,400, 57,600 and 115,200. The default setting is 9600 bits/s. The serial port configuration must be set to No parity, 8 data bits, and 1 stop bit (N/8/1) for proper operation. The serial port speed set by this parameter must match the speed of the serial port set in the System ROM RBSU setup.
Minimum password length	8	This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from zero to 39. The default setting is eight characters.
Remote keyboard model	US	This setting allows you to specify the language model of the keyboard during a Remote Console session. The default setting is US.

Network Settings parameters

Parameter	Default Value	Definition
Enable NIC	Yes	This parameter enables the NIC to reflect the state of iLO. The default setting for the NIC is Yes, which is enabled. If DHCP is disabled, you must assign a static IP address to iLO. Assign the IP address using the iLO IP Address parameter.
Shared network port	No	This option only displays on servers that support the iLO Shared Network Port. If the option is available, the help content for iLO Shared Network Port is also displayed. The iLO Shared Network Port option is disabled by default. Selecting this option disables the iLO NIC and directs iLO network traffic over the designated host NIC. Refer to your server documentation for additional information.
Transceiver speed autoselect	Yes	Autoselect detects the interface speed and sets the interface to operate at 10 Mb/s or 100 Mb/s and at half or full duplex. If necessary, this parameter can be set to manual to allow manual adjustment of speed and duplex settings.
Speed	N/A (autoselect)	Use this setting to assign 10-Mb/s or 100-Mb/s connect speeds if Transceiver Speed Autoselect is not enabled.

Parameter	Default Value	Definition
Duplex	N/A (autoselect)	Use this setting to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.
Enable DHCP	Yes	Allows you to select static IP (disabled) or Enables the use of a DHCP server to obtain an IP address for the iLO subsystem. You cannot set the iLO IP Address and Subnet Mask if DHCP is enabled. Enabling DHCP allows you to configure the following DHCP options: • Use DHCP Supplied Gateway • Use DHCP Supplied DNS Servers • Use DHCP Supplied WINS Servers • Use DHCP Supplied Static Routes • Use DHCP Supplied Domain Name
Use DHCP supplied gateway	Yes	Toggles whether iLO will use the DHCP server-supplied gateway. If not, enter one in the Gateway IP Address box.
Use DHCP supplied DNS servers	Yes	Toggles whether iLO will use the DHCP server-supplied DNS server list. If not, enter one in the Primary/Secondary/Tertiary DNS Server boxes.
Use DHCP supplied WINS servers	Yes	Toggles whether iLO will use the DHCP server-supplied WINS server list. If not, enter one in the Primary/Secondary WINS Server boxes.
Use DHCP supplied Static routes	Yes	Toggles whether iLO will use the DHCP server-supplied static route. If not, enter one in the Static Route #1, #2, #3 boxes.
Use DHCP supplied domain name	Yes	Toggles whether iLO will use the DHCP server-supplied domain name. If not, enter one in the Domain Name box.
Register with WINS server	N/A (DHCP)	iLO automatically registers with a WINS server. The default setting is Yes. By default, WINS server addresses are assigned by DHCP.
Register with DNS server	N/A (DHCP)	iLO automatically registers with a DNS server. The default setting is Yes. By default, DNS server addresses are assigned by DHCP.

Parameter	Default Value	Definition
Ping gateway on startup	No	This option causes iLO to send four ICMP echo request packets to the gateway when iLO initializes. This option ensures that the ARP cache entry for iLO is current on the router responsible for routing packets to and from iLO.
iLO IP address	N/A (DHCP)	Use this parameter to assign a static IP address to iLO on your network. By default, the IP address is assigned by DHCP.
iLO subnet mask	N/A (DHCP)	Use the subnet mask parameter to assign the subnet mask for the default gateway. By default, the subnet mask is assigned by DHCP.
iLO gateway IP address	N/A (DHCP)	Use the gateway parameter to assign the IP address of the network router that connects the iLO subnet to another subnet where the management console resides. The default gateway is assigned by DHCP.
iLO subsystem name	iLO*XXXXXXXXXXXX*, where the 12 *X*s are the server serial number (assigned at the factory)	iLO comes preset with a DNS/WINS name. The DNS/WINS name is "iLO" plus the serial number of the server. This name also is displayed on the tag attached to the bracket of iLO. You can change this value.
Domain name	N/A (DHCP)	Enter the name of the domain in which iLO will participate. By default, the domain name is assigned by DHCP.
DHCP server	N/A (DHCP)	This setting is automatically detected if DHCP is set to Yes. You cannot change this setting.
Primary, secondary, and tertiary DNS server	N/A (DHCP)	Use this parameter to assign a unique DNS server IP address on the network. By default, the primary, secondary, and tertiary DNS servers are assigned by DHCP.
Primary and secondary WINS server	N/A (DHCP)	Use this parameter to assign a unique WINS server IP address on the network. By default, the primary and secondary WINS servers are assigned by DHCP.
Static routes #1, #2, #3	N/A for both the destination and gateway address (DHCP)	Use this parameter to assign a unique static route destination and gateway IP address pair on the network. Up to three static route pairs can be assigned. By default, the static routes are assigned by DHCP.

Parameter	Default Value	Definition
Blade server parameters		
iLO diagnostic port configuration parameters		
Transceiver speed autoselect	Yes	Toggles the ability of the Transceiver to auto-detect the speed and duplex of the network on the Diagnostic Port. Speed and Duplex are disabled if Autoselect is set to Yes.
Speed	N/A (autoselect)	Configures the speed of the Diagnostic Port. This speed must match the speed of the Diagnostic Port network. If the Autoselect option is set to Yes, the speed will be automatically configured by Integrated Lights-Out.
Duplex	N/A (autoselect)	Configures the duplex of the Diagnostic Port. The duplex should match the duplex of the Diagnostic Port network. If the Autoselect option is set to Yes, the duplex will be automatically configured by Integrated Lights-Out.
IP address	192.168.1.1	The Diagnostic Port IP address. If DHCP is being used, the Diagnostic Port IP address is automatically supplied. If not, enter a static IP address here.
Subnet mask	255.255.255.0	The subnet mask for the Diagnostic Port IP network. If DHCP is being used, the Subnet Mask is automatically supplied. If not, enter the subnet mask for the network.

SNMP/Insight Manager settings parameters

Parameter	Default Value	Definition
SNMP alert destination(s)	No	Enter the IP address of the remote management PC that will receive SNMP trap alerts from iLO. Up to three IP addresses can be designated to receive SNMP alerts.

Parameter	Default Value	Definition
Enable iLO SNMP alerts	No	iLO alert conditions are detected by iLO and are independent of the host server operating system. These alerts can be Insight Manager SNMP traps. These alerts include major events, such as remote server power outages or server resets. They also include iLO events, such as security disabled or failed login attempt. iLO forwards the alerts to an Insight Manager 7 or Systems Insight Manager console using the destinations provided. The default setting is No.
Forward Insight Manager Agent SNMP alerts	No	These alerts are generated by the Insight Management agents, which are provided for each supported network operating system. The agents must be installed on the host server to receive these alerts. These alerts are sent to Insight Manager 7 or Systems Insight Manager clients on the network and are forwarded asynchronously by iLO to the IP addresses that have been configured to receive them. The default setting is Yes.
Enable SNMP pass-thru	Yes	The Enable SNMP pass-through option enables the system to pass SNMP packets from the Insight Management Agent. When set to No, all SNMP traffic is stopped and will not pass-through iLO. The default setting is Yes.
Insight Manager Web Agent URL		The Insight Manager Web Agent URL option enables you to enter the IP address or the DNS name of the host server on which the Insight Manager Web Agents are running. Entering this data in the field provided enables iLO to create a link from the iLO Web pages to the pages of the Web Agent.
Level of data returned	Medium	The Level of Data Returned option regulates how much data is returned to an anonymous request for iLO information from Insight Manager 7 or Systems Insight Manager. All settings, except the None Data Level, provide sufficient data to allow integration with Insight Manager 7. The Medium and High settings enable Insight Manager 7 and Systems Insight Manager to associate the management processor with the host server. The None Data Level prevents iLO from responding to the Insight Manager 7 and Systems Insight Manager requests. The default setting is Medium.

Directory settings parameters

Parameter	Default Value	Definition
Enable directory authentication	No	This parameter enables or disables directory authentication. If directory support is properly configured, this enables user login to iLO using directory credentials.
Enable local user accounts	Yes	This option enables a user to log in using a local user account instead of a directory account. By default, this setting is Enabled.
Directory server address	0.0.0.0	This parameter specifies the Directory Server DNS name or IP address. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.
Directory server LDAP port	636	This option sets the port number used to connect to the directory server. The SSL-secured LDAP port number is 636.
LOM object distinguished name		This option specifies the unique name for the iLO in the directory. LOM Object Distinguished Names are limited to 256 characters.
LOM object password		This parameter specifies the password for the iLO object to access the directory. LOM Object Passwords are limited to 39 characters. **NOTE:** At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.
LOM object password confirm		Prevents mistyped passwords. If you change the LOM Object Password, also enter the new password in this field.

Parameter	Default Value	Definition
Directory user context 1, directory user context 2, directory user context 3		This parameter enables you to specify up to three searchable contexts used to locate the user when the user is trying to authenticate using the directory. Directory User Contexts are limited to 128 characters each. Directory User Contexts enable you to specify directory user containers that are automatically searched when an iLO login is attempted. This eliminates the requirement of entering a fully distinguished user name at the login screen. For example, the search context, "ou=lights out devices,o=corp" would allow the user "cn=manager,ou=lights out devices,o=corp" to login to iLO using just "manager." Active Directory allows an additional search context format, "@hostname" for example, "@directory.corp."

BL p-Class parameters

Parameter	Default Value	Definition
Rack name	Provided by rack	The rack name is used to logically group together the components that compose a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component.
Enclosure name	Provided by rack	The enclosure name is used to logically group together the server blades that compose a single enclosure. When changed, the enclosure name is communicated to all other server blades connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component.
Bay name		The bay name is used when logging and alerting to assist in identifying a component or its function.
Bay	Provided by rack	The ProLiant BL p-Class enclosure can support one to eight server blades. The bays are numbered from left to right starting with 1 and finishing with 8. The bay number is used to assist in physically identifying the faulty server blade or other error conditions. This information is for viewing only.

Parameter	Default Value	Definition
Rack serial number	Provided by rack	The rack serial number identifies the components in the rack as a logical grouping. The serial number is determined during power-up of the various components to create a unique rack serial number. Switching components (server blade enclosure or power supplies) alters the rack serial number.
Enclosure serial number	Provided by rack	The enclosure serial number identifies the particular server blade enclosure in which a server blade resides.
Blade serial number	Provided by blade server	The blade serial number identifies the serial number for the server blade product.
Power source	Rack provides power	The server blade enclosure can be installed in a rack by using one of two configurations: • The server blade power supplies can be used to convert normal AC facility power to 48 V DC to power the rack. In this configuration, select the power source as **Rack Provides Power.** This setting enables each server blade, enclosure, and power supply to communicate power requirements to ensure proper power consumption without risking power failures. • If the facility can provide 48 V DC power directly, without the need for the provided power supplies, then select **Facility Provides 48V.** Each server blade will not be required to communicate with the infrastructure for power when powering on or off. **NOTE:** It is essential that proper power sizing requirements be performed to ensure sufficient power for all the server blades and other components of the rack.
Enable automatic power on	On	Each server blade can be configured to automatically power on when inserted into the enclosure. Depending on the Power Source setting, the server blade communicates with the rack to determine if enough power is available to power on. If the power is available, then the server blade automatically powers on and begins the normal server booting process.

Parameter	Default Value	Definition
Enable rack alert logging (IML)	On	As the server blade receives alerts, these events can be logged to the IML. You can view these events by using the iLO System Status—IML tab. Additional IML viewing tools are available to allow viewing from the installed operating system on the server blade.

iLO Advanced Pack License Key

The iLO Advanced Pack License Key option is used to enable the iLO Advanced Features including Graphical Remote Console, virtual media (floppy and CD-ROM), and directory support . Enter the 25-character key in this field to enable the features.

Technical support

In this section

HP contact information

For the name of the nearest HP authorized reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- In other locations, refer to the HP website (http://www.hp.com).

For HP technical support:

- In North America:
  - Call 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

CR

Certificate Request

DAV

Distributed Authoring and Versioning

DDNS

Dynamic Domain Name System

DHCP

Dynamic Host Configuration Protocol

DLL

dynamic link library

DNS

domain name system

DSA

Digital Signature Algorithm

EMS

Emergency Management Services

EULA

end user license agreement

FEH

fatal exception handler

FSMO

Flexible Single-Master Operation

GUI

graphical user interface

HB

heartbeat

HPONCFG

HP Lights-Out Online Configuration utility

HPQLOMGC

HP Lights-Out Migration Command Line

HPQLOMIG

HP Lights-Out Migration

ICMP

Internet Control Message Protocol

iLO

Integrated Lights-Out

IML

Integrated Management Log

IP

Internet Protocol

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

SNMP

Simple Network Management Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

TCP

Transmission Control Protocol

UART

universal asynchronous receiver-transmitter

UID

unit identification

USB

universal serial bus

VM

Virtual Machine

VPN

virtual private networking

WINS

Windows® Internet Naming Service

XML

extensible markup language

Index

H

I

L

M

N

O

P

R

S

T

U

V

W

X