

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



July 2005 (First Edition)
Part Number 395970-001

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

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

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

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation. Linux is a U.S. registered trademark of Linus Torvalds. Java is a U.S. trademark of Sun Microsystems, Inc.

July 2005 (First Edition)
Part Number 395970-001

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	7
Guide overview	7
New in this version	7
Command line	9
Specific commands	9
Network commands	9
iLO settings.....	11
SNMP settings	14
Directory commands.....	15
Virtual media commands.....	17
Virtual Media scripting	23
Scripting Web server requirements	23
Using virtual media scripting.....	24
Using Virtual Media on Linux servers through an SSH connection	25
Virtual media image files	27
CGI helper application	27
SSH key authorization	31
SSH key authorization introduction	31
Tool definition files.....	32
Mxagentconfig	32
Importing SSH keys from PuTTY	32
HPONCFG online configuration utility	37
HPONCFG	37
HPONCFG supported operating systems.....	37
HPONCFG requirements	37
Installing HPONCFG.....	39
Windows server installation	39
Linux server installation	39
Using HPONCFG	40
Using HPONCFG on Linux servers	41
HPONCFG command line parameters	41
Using HPONCFG on Windows servers.....	42
Obtaining an entire configuration	43

Obtaining a specific configuration.....	44
Setting a configuration.....	45

Remote Insight command language 47

GET_EVENT_LOG.....	47
GET_EVENT_LOG parameters.....	48
GET_EVENT_LOG runtime errors.....	48
GET_EVENT_LOG return messages.....	48
GET_NETWORK_SETTINGS.....	50
GET_NETWORK_SETTINGS parameters.....	50
GET_NETWORK_SETTINGS runtime errors.....	50
GET_NETWORK_SETTINGS return messages.....	50
GET_HOST_POWER_STATUS.....	51
GET_HOST_POWER_STATUS Parameters.....	52
GET_HOST_POWER_STATUS Runtime Errors.....	52
GET_HOST_POWER_STATUS Return Messages.....	52
SET_HOST_POWER.....	52
SET_HOST_POWER Parameters.....	53
SET_HOST_POWER Runtime Errors.....	53
MOD_NETWORK_SETTINGS.....	53
MOD_NETWORK_SETTINGS parameters.....	55
MOD_NETWORK_SETTINGS runtime errors.....	58
GET_GLOBAL_SETTINGS.....	58
GET_GLOBAL_SETTINGS parameters.....	58
GET_GLOBAL_SETTINGS runtime errors.....	58
GET_GLOBAL_SETTINGS return messages.....	58
MOD_GLOBAL_SETTINGS.....	59
MOD_GLOBAL_SETTINGS parameters.....	60
MOD_GLOBAL_SETTINGS runtime errors.....	63
GET_DIR_CONFIG.....	63
GET_DIR_CONFIG parameters.....	63
GET_DIR_CONFIG runtime errors.....	63
GET_DIR_CONFIG return messages.....	64
MOD_DIR_CONFIG.....	65
MOD_DIR_CONFIG parameters.....	66
MOD_DIR_CONFIG runtime errors.....	68
GET_TWOFACOR_SETTINGS.....	68
GET_TWOFACOR_SETTINGS parameters.....	68
GET_TWOFACOR_SETTINGS runtime errors.....	69
GET_TWOFACOR_SETTINGS return messages_Checkpoint.....	69
MOD_TWOFACOR_SETTINGS.....	69
MOD_TWOFACOR_SETTINGS parameters.....	71
MOD_TWOFACOR_SETTINGS runtime errors.....	72
GET_HOST_POWER_REG_INFO.....	73

GET_HOST_POWER_REG_INFO parameters.....	73
GET_HOST_POWER_REG_INFO runtime errors	74
GET_HOST_POWER_REG_INFO return messages	74
HPQLOMGC command language	77
Using HPQLOMGC.....	77
ILO_CONFIG	78
iLO parameters	79
Network Settings parameters	79
Directory settings parameters.....	82
Technical support	85
HP contact information	85
Before you contact HP	85
Acronyms and abbreviations	87
Index	95

Introduction

In this section

Guide overview	7
New in this version	7

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 Addendum* describes changes to the syntax and tools available to use iLO through a command line or scripted interface and is intended to be used in conjunction with the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*. For specific details on what has changed and included in this addendum, refer to the "New in this version (on page [7](#))" section.

New in this version

- Command line (on page [9](#)) changes to following areas:
 - Added VLAN tagging to Network commands (on page [9](#)) (replaces the network commands in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*).
 - Virtual media commands (on page [17](#)) (replaces the virtual media commands in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*).
 - Directory commands (on page [15](#)) (replaces the directory commands in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*).

- iLO settings (on page [11](#)) commands (replaces the iLO settings in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*).
- SNMP settings (on page [14](#)) commands (replaces the SNMP settings in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*).
- Added "SSH key authorization (on page [31](#))" section.
- Updated Virtual Media scripting (on page [23](#)). The entire section is included in this addendum.
- Updated HPNOCFG ("HPNOCFG online configuration utility" on page [37](#)). The entire section is included in this addendum.
- RIBCL ("Remote Insight command language" on page [47](#)) updates. Only the commands that have changed are included in this addendum and replace the commands in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*.
- Updated HPLOMGC ("HPQLOMGC command language" on page [77](#)). The entire section is included in this addendum.
- Updated iLO parameters (on page [79](#)). Only the parameters that have changed are included in this addendum and replace the commands in the *HP Integrated Lights-Out 1.70 Scripting and Command Line Resource Guide*.
- Added the commands:
 - GET_EVENT_LOG (on page [47](#))
 - GET_TWOFACOR_SETTINGS (on page [68](#))
 - MOD_TWOFACOR_SETTINGS (on page [69](#))
 - GET_HOST_POWER_REG_INFO (on page [73](#))

Command line

In this section

Specific commands.....[9](#)

Specific commands

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

Network commands

oemhp_vlan_enablestate 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.
oemhp_vlan_enablestate	Read/Write	Specifies if iLO shared network VLAN ID is enabled. Boolean values accepted.
oemhp_vlan_id	Read/Write	Specifies the VLAN ID. Only values from 1 to 4094 are valid.
autosense	Read/Write	Specifies if the autosense feature is enabled. Boolean values accepted.

Property	Access	Description
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.
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 be 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 DNS server is required. Boolean values accepted.
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.

Property	Access	Description
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_serialcliath	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.
oemhp_rc_seize	Read/Write	Enables/disables remote console acquire operations.

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_iiloalert	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_snmpassthru	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	Determines if the LOM device will respond to anonymous XML queries. Valid selections are enabled and disabled.

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.

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. Valid settings are: <ul style="list-style-type: none"> extended_schema—Use HP's extended schema default_schema—Use schema-free directories disabled—Directory-based authentication is disabled
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. The schema-free directory configuration requires a DNS name.
oemhp_ldapport	Read/Write	Sets the directory server port.
oemhp_dirdn	Read/Write	Displays the LOM object distinguished name. This field is ignored when the schema-free directory configuration is used.

Property	Access	Description
oemhp_dirpassword	Read/Write	Sets the LOM object password. This field is ignored when the default schema configuration is used.
oemhp_usercntxt1, 2, or 3	Read/Write	Displays the directory user login search context. Not necessary when the schema-free directory configuration is used.
oemhp_group{n}_name where n = 1..6	Read/Write	Security group distinguished name. Used with the schema-free directory configuration only.
oemhp_group{n}_priv where n = 1..6	Read/Write	Privileges to assign to this group. A comma-separated list of the following: <ul style="list-style-type: none"> • 1 (Administer Group Accounts) • 2 (Remote Console Access) • 3 (Virtual Power & Reset) • 4 (Virtual Media) • 5 (Configure iLO Settings) Used with the schema-free directory configuration only.

Examples

- `set /map1/oemhp_dircfg`
- `set /map1/oemhp_dircfg oemhp_dirauth=groups
oemhp_dirsrvaddr=adserv.demo.com
oemhp_group1_name="CN=iLOAdmins,CN=Users,DC=demo,DC=com" oemhp_group1_priv="1,2,3,4,5"`

Additional groups can be defined using additional set commands.

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 or key drive 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.
oemhp_connect	Read	Displays if a virtual media device is already connected through the CLP or scriptable virtual media.
oemhp_boot	Read/Write	Sets the boot flag. The valid values are: <ul style="list-style-type: none"> never—Do not boot from the device. The value is displayed as <code>No_Boot</code>. once—Boot from the device once and then not thereafter. The value is displayed as <code>Once</code>. always—Boot from the device each time the server is rebooted. The value is displayed as <code>Always</code>. connect—Connect the virtual media device. Sets <code>oemhp_connect</code> to <code>Yes</code> and <code>oemhp_boot</code> to <code>Always</code>. disconnect—Disconnects the virtual media device and sets the <code>oemhp_boot</code> to <code>No_Boot</code>.

Property	Access	Description
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.bin`
- `set`
`oemhp_image=http://john:abc123@imgserver.company.com/VMimage/install1Disk.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`.



NOTE: USB key drives must be used with the `floppy` keyword syntax.

- 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 47)" section for more details on how to use these commands.

Multi-device Virtual Media is not supported using the CLI. You must specify Virtual Media images. Refer to the "Virtual media scripting (on page 23)" section for more information.

Tasks

- Insert a floppy USB key image into the Virtual Floppy/USBKey:


```
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 or key 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 or USB key image from the Virtual Floppy/USBKey:

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

where the example executes the following:
 - Change the current context to the floppy or key drive.
 - Issue the disconnect command. This will disconnect the media and clear the oemhp_image as well.
- Insert a CDROM image into the Virtual CD-ROM:

```
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 CD-ROM 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 CD-ROM image from the Virtual CD-ROM:

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

where the example executes the following:
 - Change the current context to the CD-ROM drive.
 - Issue the disconnect command. This will disconnect the media and clear the oemhp_image as well.
- Insert a CD-ROM 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 CD-ROM 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 CD-ROM image from the virtual CD-ROM 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.

Virtual Media scripting

In this section

Scripting Web server requirements	23
Using virtual media scripting	24
Using Virtual Media on Linux servers through an SSH connection	25
Virtual media image files	27
CGI helper application.....	27

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.

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 floppy, USB key, and CD-ROM images.

Virtual media scripting enables you to use other methods than a browser to configure iLO for virtual media use. iLO can be configured remotely using CPQLOCFG XML commands, locally using HPONCFG XML commands, or locally, using the HPLOVM utility that replaces the VFLOP utility from the SmartStart Scripting toolkit.



NOTE: Virtual media scripting does not operate Virtual Media using the browser. Likewise, the browser does not support scripting capabilities. For example, a floppy disk mounted using the browser cannot later be dismounted using the scripting interface.

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 on the same network as iLO. After the image location is configured, iLO retrieves the virtual media data directly from the web server.



NOTE: Virtual media scripting does not support composite devices. Only single Virtual Media devices (either Virtual Media Floppy/USBKey or Virtual Media CD-ROM) are supported.



NOTE: USB key drives must be used with the floppy keyword syntax.

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
<code>[-device <floppy cdrom>]</code>	Defines which virtual media device is active.
<code>[-insert <url>]</code>	Defines the location of the virtual media image file that will be connected.
<code>[-eject]</code>	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.
<code>[-wp <y n>]</code>	Defines the write-protected status of the Virtual Floppy/USBKey drive. This argument has no effect on the Virtual CD-ROM drive.
<code>[-boot <once always never>]</code>	Defines how the virtual media drive is used to boot the target server.
<code>[-mgmt <iilo riloe>]</code>	Defines which management processor is being used with LOVM utility. If RILOE is specified, the VFLOP.EXE utility is used. The default setting of this argument is iLO.
<code>[-ver]</code>	Displays the HPLOVM utility version.
<code>[-?]</code>	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`.) Boot options from a USB key drive are only valid on servers with ProLiant USB key drive support.

4. Enter `vm floppy set connect` to make the floppy or key drive 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 the Virtual Media applet is always disconnected, unless a Virtual Floppy/USBKey or CD-ROM is connected through the graphical iLO interface.

The Virtual Floppy/USBKey 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 Virtual Floppy/USBKey or CD-ROM 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/sda1 /mnt/keydrive`—Mounts a virtual USB key drive.

- `mount /dev/cdrom1 /mnt/cdrom`—Mounts a virtual CD-ROM on a Red Hat 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.

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);
```

SSH key authorization

In this section

SSH key authorization introduction	31
Tool definition files	32
Mxagentconfig.....	32
Importing SSH keys from PuTTY.....	32

SSH key authorization introduction

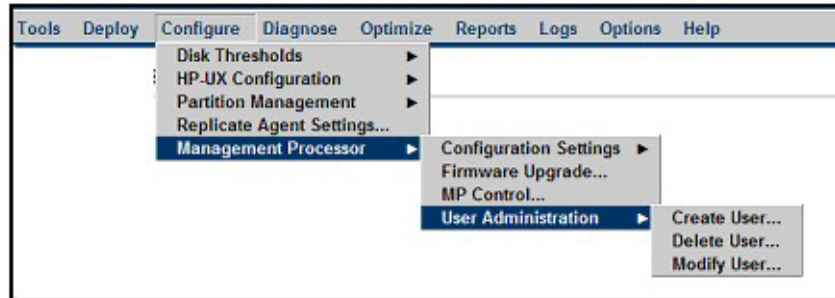
SSH key-based authentication enables HP SIM to connect to LOM devices through SSH and be authenticated and authorized to perform administrative-level tasks. The CLP is utilized to perform tasks. HP SIM can perform these tasks on multiple LOM devices nearly simultaneously, at scheduled times. HP SIM provides a menu-driven interface to manage and configure multiple targets. Enhancements to HP SIM are provided by tool definition files.

HP SIM can perform actions on target devices utilizing an SSH interface that requires private key-based authentication. If HP SIM is enabled to integrate more fully with LOM devices, SSH key-based authentication is implemented in iLO.

An HP SIM instance will be established as a trusted SSH client by installing its public key in iLO. This is completed either manually through a web-based UI, or automatically with the mxagentconfig utility.

Tool definition files

TDEF files extend the menu system of HP SIM to provide the CLP commands that HPSIM will transmit to iLO through an SSH connection.



Mxagentconfig

Mxagentconfig is a utility used to export and install HP SIM public SSH keys into other systems. This utility simplifies the process and can install the public key on many systems simultaneously. Mxagentconfig will make an SSH connection to iLO, authenticate with a user name and password, and transmit the necessary public key. iLO stores this key as a trusted SSH client key.

Importing SSH keys from PuTTY

The public key file format generated by PuTTY is not compatible with iLO. For example, a PuTTY generated public key file looks like this:

```

---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1yc2EAAAABJQAAAIB0x0wVO9itQB11o+tHnY3VvmsGgwh
CyLOVzJl
3A9F5yzKj+RXJVPxOGusAhmJwF8PBQ9wV5E0Rumm6gNOaPyvAMJCG/10
PW7Fhacl
VLt8i5F3Lossw+/LWa+6H0da13TF2vq3ZoYFUT4esC6YbAACM7kLuGwx
F5XMNR2E
Foup3w==
---- END SSH2 PUBLIC KEY ----

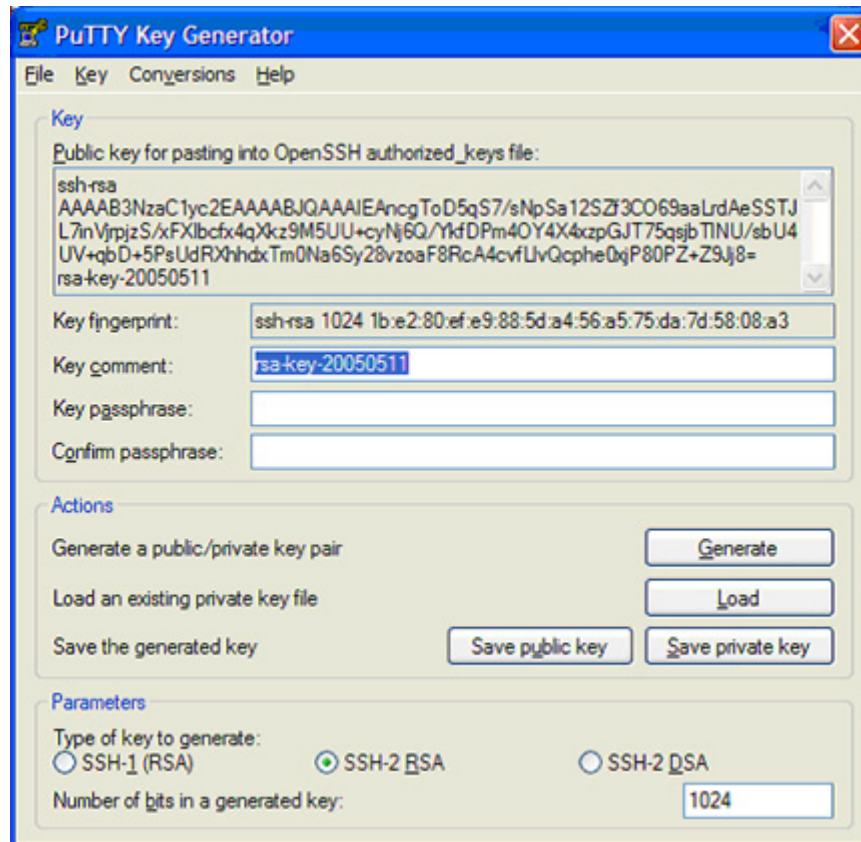
```


PuTTY generated public key files are not compatible with iLO. iLO expects public key file information on a single line. You must use the PuTTY Key Generator (puttygen.exe) utility to import a correctly formatted SSH key for use with iLO.

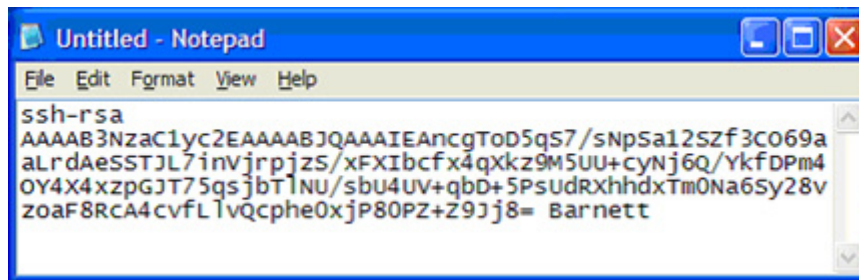
To import SSH keys to iLO from PuTTY:

1. Double-click the PuTTY Key Generator icon to launch the utility.
2. Select **SSH-2 RSA**, and click **Generate**.

On the key area, move the mouse around to generate the key. You must keep moving the mouse until the key generation process is complete.

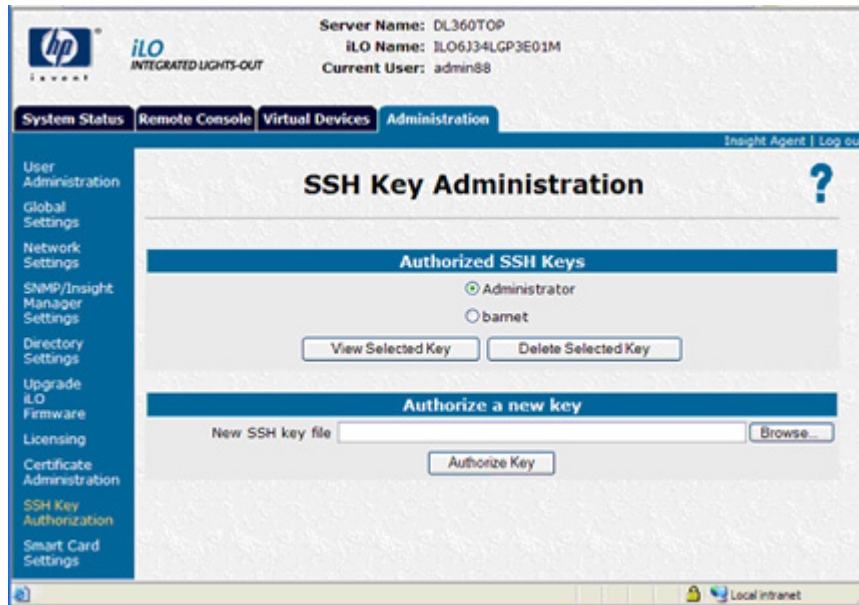


3. After the key is generated, replace the key comment with your iLO user name. (The user name is case-sensitive and must match the case of your iLO user name.)
4. Select all the text in the public key area. Copy the key and paste it into a Notepad session.
5. Return to the PuTTY Key Generator utility.
6. Click **Save private key** to save and enter a file name when prompted, for example, c:\bchan.ppk.
7. Return to Notepad.
8. Save the public key file. Click **File>Save As**, and enter a file name when prompted, for example, c:\bchan.pub.



9. Log into iLO (if not already open).
10. On the iLO SSH Key Administration page, click **Browse**, and locate the public key file.

11. Click **Authorize**. A new Authorized SSH key will appear in the list.

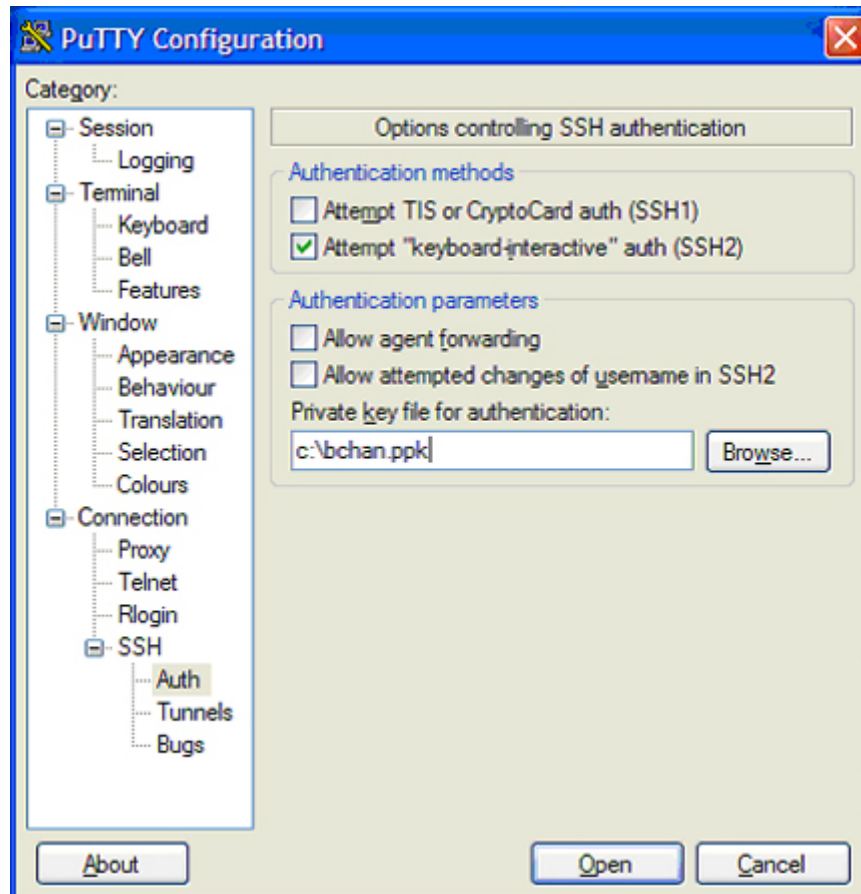


12. Launch PuTTY.

13. Select **SSH>Auth** on the menu.

14. Click **Browse** and locate the public key file.

15. Configure your iLO IP, and click **Open**. iLO will respond and ask for a user name.



16. Enter the logon name associated with the public key. The public key in iLO will handshake with the private key in PuTTY. If the keys match, you are logged into iLO without using a password.

Keys can be created with a key passphrase. If a key passphrase was used to generate the public key, you will be prompted for the key passphrase before you log into iLO.

HPONCFG online configuration utility

In this section

HPONCFG	37
HPONCFG supported operating systems	37
HPONCFG requirements.....	37
Installing HPONCFG	39
Using HPONCFG.....	40

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 using an account with Administrator or root access.

HPONCFG supported operating systems

HPONCFG is supported on:

- 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 server, the server must have the iLO Management Interface Driver loaded. The SmartStart 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 RILOE II-based servers, the server must have the RILOE II Management Interface Driver loaded. 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 sm2user.dll loaded. 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, 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 CP004791.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\
```

Installing HPONCFG

The HPONCFG utility is delivered in separate packages for Windows® and Linux systems. For Windows® systems, it is delivered as a smart component. For Linux systems, it is delivered as an RPM package file. HPONCFG 1.1 is part of SmartStart 7.30.

Windows server installation

HPONCFG will be installed automatically when ProLiant support pack version 7.30 is installed. The individual HPONCFG 1.1 component cp005299.exe can be downloaded from the HP website (<http://h18023.www1.hp.com/support/files/lights-out/us/download/22571.html>).

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. Be sure that the appropriate Management Interface Driver is installed. The sm2user.dll file must also be installed. Refer to the "HPONCFG requirements (on page 37)" for details on where to obtain this driver and file.

Linux server installation

HPONCFG will be installed automatically when ProLiant support pack version 7.30 is installed. The rpm of HPONCFG 1.1 for the respective Linux distributions can be downloaded from the HP website (<http://h18023.www1.hp.com/support/files/lights-out/us/>).

The following is a list of HPONCFG RPMs and the Linux distributions they support:

RPM supported	Distributions
hponcfg-1.1.0-5.rhel21.i386.rpm	Red Hat Enterprise Linux 2.1
hponcfg-1.1.0-5.rhel3.i386.rpm	Red Hat Enterprise Linux 3.0

RPM supported	Distributions
hponcfg-1.1.0-5.sles8.i386.rpm	SUSE Linux Enterprise Server 8 / United Linux 1.0

Install the appropriate package using the RPM installation utility. As an example for package installation, hponcfg RPM on Red Hat Enterprise Linux 3.0 can be installed by:

```
rpm -ivh hponcfg-1.1.0-5.rhel3.i386.rpm
```

If an older version of hponcfg RPM package is already installed on the system, run the following command to remove the older version before installing the new version of HPONCFG:

```
rpm -e hponcfg
```

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

After installation, the HPONCFG executable can be found in the /sbin directory. Be sure that the appropriate Management Interface Driver is installed. Refer to the "HPONCFG requirements (on page 37)" 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 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 [41](#))" section for 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
```

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 47)" 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 [41](#))" section for an explanation of the usage.

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.

Remote Insight command language

In this section

GET_EVENT_LOG	47
GET_NETWORK_SETTINGS.....	50
GET_HOST_POWER_STATUS.....	51
SET_HOST_POWER.....	52
MOD_NETWORK_SETTINGS.....	53
GET_GLOBAL_SETTINGS	58
MOD_GLOBAL_SETTINGS.....	59
GET_DIR_CONFIG.....	63
MOD_DIR_CONFIG.....	65
GET_TWOFACOR_SETTINGS.....	68
MOD_TWOFACOR_SETTINGS	69
GET_HOST_POWER_REG_INFO.....	73

GET_EVENT_LOG

The GET_EVENT_LOG command retrieves the iLO Event Log or the Integrated Management log, depending on the context of the command. For this command to parse correctly, the command must appear within a RIB_INFO or SERVER_INFO command block. To retrieve the iLO Event Log, use the RIB_INFO command block. To retrieve the Integrated Management log use, the SERVER_INFO command block.

Examples:

- iLO Event Log example:


```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="READ">
    <GET_EVENT_LOG />
  </RIB_INFO>
</LOGIN>
</RIBCL>
```

- Integrated Management log example:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="READ">
    <GET_EVENT_LOG />
  </SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_EVENT_LOG parameters

None

GET_EVENT_LOG runtime errors

GET_EVENT_LOG returns a runtime error if it is not called from within the RIB_INFO or SERVER_INFO block. For example:

```
<RIBCL VERSION="2.21">
  <RESPONSE
    STATUS="0x0001"
    MESSAGE='Syntax error: Line #3: syntax error near ">"
    in the line: " GET_EVENT_LOG >"'
  />
</RIBCL>
```

GET_EVENT_LOG return messages

The response includes all of the events recorded, in the order that they occurred. Events are not sorted by severity or other criteria. Each event includes a common set of attributes:

- SEVERITY indicates the importance of the error and how it might impact server or iLO availability.
 - FAILED indicates a problem or component failure that might impact operational time if it is not addressed.
 - CAUTION indicates an event that is not expected during normal system operation. This might not indicate a platform issue.

- REPAIRED indicates that an event or component failure has been addressed.
- INFORMATIONAL indicates that something noteworthy occurred, but operational time is not impacted.
- CLASS indicates the subsystem that generated the event, and can include iLO, environment, power, system error, rack infrastructure, and more.
- LAST_UPDATE indicates the most recent time this event was modified.
- INITIAL_UPDATE indicates when this event first occurred.
- COUNT indicates the number of times a duplicate event happened.
- DESCRIPTION indicates the nature of the event and all recorded details.

The following response is typical of the data returned from the iLO Event Log:

```
<EVENT_LOG DESCRIPTION="iLO Event Log">
  <EVENT
    SEVERITY="Caution"
    CLASS="iLO"
    LAST_UPDATE="04/04/2004 12:34"
    INITIAL_UPDATE="04/04/2004 12:34"
    COUNT="1"
    DESCRIPTION="Server reset."
  />
  ...
</EVENT_LOG>
```

The following response is typical of the data returned from the Integrated Management Log:

```
<EVENT_LOG DESCRIPTION="Integrated Management Log">
  <EVENT
    SEVERITY="Caution"
    CLASS="POST Message"
    LAST_UPDATE="04/04/2004 12:34"
    INITIAL_UPDATE="04/04/2004 12:34"
    COUNT="1"
    DESCRIPTION="POST Error: 1775-Drive Array - ProLiant
    Storage System not Responding"
  />
  ...
</EVENT_LOG>
```

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"/>
  <SHARED_NETWORK_PORT_VLAN VALUE="Yes"/>
  <SHARED_NETWORK_PORT_VLAN_ID VALUE="10"/>
  <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"/>

```

GET_HOST_POWER_STATUS

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

Example:

```

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

```

GET_HOST_POWER_STATUS Parameters

None

GET_HOST_POWER_STATUS Runtime Errors

The possible GET_HOST_POWER_STATUS error messages include:

- Host power is OFF.
- Host power is ON.

GET_HOST_POWER_STATUS Return Messages

The following information is returned within the response:

```
<GET_HOST_POWER
  HOST_POWER="OFF"
/>
```

SET_HOST_POWER

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

Example:

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

SET_HOST_POWER Parameters

HOST_POWER enables or disables the Virtual Power Button. The possible values are "Yes" or "No."

SET_HOST_POWER Runtime Errors

The possible SET_HOST_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Virtual Power Button feature is not supported on this server.
- Host power is already ON.
- Host power is already OFF.
- User does not have correct privilege for action. RESET_SERVER_PRIV required.

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.

The 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 iLO.

The iLO management processor reboots to apply the changes after the script has successfully completed. If connectivity to iLO is lost, 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"/>
    <SHARED_NETWORK_PORT_VLAN VALUE="Yes"/>
    <SHARED_NETWORK_PORT_VLAN_ID VALUE="10"/>
    <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 the following servers:

ProLiant server	Minimum iLO firmware version
DL320 G3	1.64
DL360 G4	1.60
DL380 G4	1.60
DL385 G1	1.64
DL580 G3	1.64
ML370 G4	1.60
ML570 G3	1.64

SHARED_NETWORK_PORT_VLAN VALUE is used to enable iLO Shared Network Port VLAN ID tagging. The possible values are "Yes" or "No."

SHARED_NETWORK_PORT_VLAN_ID VALUE is used to set the VLAN ID value. Values must be between 1 and 4094.

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"/>
```

```

<REMOTE_CONSOLE_ACQUIRE 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"/>
        <REMOTE_CONSOLE_ACQUIRE value="Y"/>
        <PASSTHROUGH_CONFIG value="3"/>
        <HTTPS_PORT value="443"/>
        <HTTP_PORT value="80"/>
        <REMOTE_CONSOLE_PORT value="23"/>
        <TERMINAL_SERVICES_PORT VALUE="3389"/>
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

```
<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>
```

High Performance Mouse example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_GLOBAL_SETTINGS>
      <HIGH_PERFORMANCE_MOUSE VALUE="Yes" />
    </MOD_GLOBAL_SETTINGS >
  </RIB_INFO >
</LOGIN>
</RIBCL>
```

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."

REMOTE_CONSOLE_ACQUIRE determines if the remote console acquire operation will be 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 values 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_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

Starting with iLO 1.80, directory integration can work with HP Lights-Out schema with or without extensions (schema-free). Depending on your directory configuration, the response to GET_DIR_CONFIG contains different data.

Possible GET_DIR_CONFIG return messages are:

- Example of a directory services (with schema extension) return message:

```
<GET_DIR_CONFIG>
  <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
  <DIR_LOCAL_USER_ACCT VALUE="Y"/>
  <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
  <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="" />
  <DIR_ENABLE_GRP_ACCT VALUE="N"/>
</GET_DIR_CONFIG>
```

- Example of a schema-free directory (without schema extension) return message:

```
<GET_DIR_CONFIG>
  <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
  <DIR_LOCAL_USER_ACCT VALUE="Y"/>
  <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
  <DIR_SERVER_PORT VALUE="636"/>
  <DIR_OBJECT_DN VALUE="" />
  <DIR_USER_CONTEXT1 VALUE="CN=Users,DC=demo,DC=com"/>
  <DIR_USER_CONTEXT2 VALUE="" />
  <DIR_USER_CONTEXT3 VALUE="" />
  <DIR_ENABLE_GRP_ACCT VALUE="Y"/>
  <DIR_GRPACCT1_NAME
VALUE="CN=iLOAdmins,CN=Users,DC=demo,DC=com"/>
  <DIR_GRPACCT1_PRIV VALUE="1,2,3,4,5"/>
  <DIR_GRPACCT2_NAME VALUE="" />
  <DIR_GRPACCT2_PRIV VALUE="" />
  <DIR_GRPACCT3_NAME VALUE="" />
```



```

<DIR_GRPACCT3_PRIV VALUE="" />
<DIR_GRPACCT4_NAME VALUE="" />
<DIR_GRPACCT4_PRIV VALUE="" />
<DIR_GRPACCT5_NAME VALUE="" />
<DIR_GRPACCT5_PRIV VALUE="" />
<DIR_GRPACCT6_NAME VALUE="" />
<DIR_GRPACCT6_PRIV VALUE="" />
</GET_DIR_CONFIG><GET_DIR_CONFIG>

```

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.

Examples:

- Extended schema (directory services) configuration 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>

```



NOTE: When using directory integration with schema extension, the following tags must not be used:

- DIR_ENABLE_GRP_ACCT
- DIR_GRPACCT1_NAME
- DIR_GRPACCT1_PRIV
- Schema-free (without extension) configuration example:


```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="admin" PASSWORD="password">
    <DIR_INFO MODE = "write">
      <MOD_DIR_CONFIG>
        <DIR_ENABLE_GRP_ACCT value = "yes"/>
        <DIR_GRPACCT1_NAME value = "test1"/>
        <DIR_GRPACCT1_PRIV value = "1"/>
        <DIR_GRPACCT2_NAME value = "test2"/>
        <DIR_GRPACCT2_PRIV value = "2"/>
      </MOD_DIR_CONFIG>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```



NOTE: When using schema-free directories, the following tags must not be used:

- DIR_OBJECT_DN
- DIR_OBJECT_PASSWORD

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_ENABLE_GRP_ACCT causes iLO to use schema-less directory integration. The possible values are "Yes" and "No."

When using schema-free directory integration, iLO supports variable privileges associated with different directory groups. These groups are contained in the directory, and the corresponding member iLO privileges are stored in iLO.

- **DIR_GRPACCT1_NAME** identifies a group container in the directory, such as Administrators, Users, or Power Users.

- `DIR_GRPACCT1_PRIV` numerically identify iLO privileges for members of the group. You can mix and match privileges by including more than one value. These privileges are expressed as a comma separated list of numbers (1,2,3,4,5) which correlate to:

1. Administer Group Accounts
2. Remote Console Access
3. Virtual Power and Reset
4. Virtual Media
5. Configure iLO Settings



NOTE: When using directory integration with schema extension, the following tags must not be used:

- `DIR_ENABLE_GRP_ACCT`
- `DIR_GRPACCT1_NAME`
- `DIR_GRPACCT1_PRIV`



NOTE: When using schema-free directories, the following tags must not be used:

- `DIR_OBJECT_DN`
- `DIR_OBJECT_PASSWORD`

`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.

GET_TWOFACOR_SETTINGS

The GET_TWOFACOR_SETTINGS command requests the respective iLO Two-Factor Authentication settings. For this command to parse correctly, the GET_TWOFACOR_SETTINGS 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_TWOFACOR_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_TWOFACOR_SETTINGS parameters

None

GET_TWOFACOR_SETTINGS runtime errors

None

GET_TWOFACOR_SETTINGS return messages_Checkpoint

Starting with iLO 1.80, users can be authenticated with a digital certificate. Depending on the iLO Two-Factor Authentication settings, the response to GET_TWOFACOR_SETTINGS will contain different data.

Possible GET_TWOFACOR_SETTINGS return messages are:

Example of a Two-Factor Authentication settings return message with default settings:

```
<GET_TWOFACOR_SETTINGS>
  <AUTH_TWOFACOR_ENABLE VALUE="N"/>
  <CERT_REVOCATION_CHECK VALUE="N"/>
  <CERT_OWNER_SUBJECT/>
</GET_TWOFACOR_SETTINGS>
```

Example of a Two-Factor Authentication settings return message when SAN field in the certificate for directory authentication is enabled:

```
<GET_TWOFACOR_SETTINGS>
  <AUTH_TWOFACOR_ENABLE VALUE="Y"/>
  <CERT_REVOCATION_CHECK VALUE="N"/>
  <CERT_OWNER_SAN/>
</GET_TWOFACOR_SETTINGS>
```

MOD_TWOFACOR_SETTINGS

MOD_TWOFACOR_SETTINGS command is used modify the Two-Factor Authentication settings on iLO. For this command to parse correctly, the MOD_TWOFACOR_SETTINGS 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. Changing the value of AUTH_TWOFACOR_ENABLE will cause iLO to reset in order for the new setting to take effect.

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

To provide the necessary security, the following configuration changes are made when Two-Factor Authentication is enabled:

- Remote Console Data Encryption: Yes (This will disable Telnet access)
- Enable Secure Shell (SSH) Access: No
- Serial Command Line Interface Status: Disabled

If Telnet, SSH or Serial CLI access is required, re-enable these settings after Two-Factor Authentication is enabled. However, since these access methods do not provide a means of Two-Factor Authentication, only a single factor is required to access iLO with Telnet, SSH or Serial CLI.

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

- **Example of enabling Two-Factor Authentication:**

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_TWOFACOR_SETTINGS>
        <AUTH_TWOFACOR_ENABLE value="Yes"/>
        <CERT_REVOCATION_CHECK value="No"/>
        <CERT_OWNER_SAN/>
      </MOD_TWOFACOR_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

- **Importing a CA and a user certificate example:**

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

```

    <MOD_TWOFACOR_SETTINGS>
      <CERT_OWNER_SAN/>
      <IMPORT_CA_CERTIFICATE>
-----BEGIN CERTIFICATE-----
MIIETzCCA5+gAwIBAgIQBGg9C0d7B5pF/l4bVA44hjANBgkqhkiG9w0B
AQUFADBM
MRMwEQYKCZImiZPyLQGGRYDTEFCMRUwEwYKCZImiZPyLQGGRYFSkpS
SUIxHjAc
...
9gVCPSoQUgMMZUeNYOBkTE0e+MrPGL+TqQEYIakF3rjA2PbL1uSY6d4d
lCx7izkO
buEpHTPDqs9gZ3U5ht9bjES93UHnDENLopkZ2JgGwH8Y50eBnjq4xml9
psbYZn5Y
yWpONE/IjIjJyww=
-----END CERTIFICATE-----
      </IMPORT_CA_CERTIFICATE>
      <IMPORT_USER_CERTIFICATE USER_LOGIN="apollo">
-----BEGIN CERTIFICATE-----
CZImiZPyLQGGRYDTEFCMRUwEwYKCZImiZPyLQGGRYFSkpSSUIxHjAc
BgNVBAMT
ODU5NDRaMFYxEzARBgoJkiaJk
...
sjbbpNGpxGsK9Gzi5j6UeOYklePyau0TJ3KIm2RPlR2C6XAGz2PTWgsx
GLUP91NH
bfz0+TD0JsschjqK23/vr2GxQ9C/835zRxdu5Dn8JGm3/dFHR2VxgCet
IxyR9TQC
ZKTfvIa8N9KvMLZdclSj94jUyMZjYYmCWULW8WySMV70nclvrsI2hi3n
wMtt2Zvj
WnbeZujBX9LGz3HdmghgUw4GTwy13ZG88snuTyXlilPFXYXvNAhGeWq
Xtrh7A90
3NprjG7DM1uw
-----END CERTIFICATE-----
      </IMPORT_USER_CERTIFICATE>
    </MOD_TWOFACOR_SETTINGS>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

MOD_TWOFACOR_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.

AUTH_TWOFACOR_ENABLE enables or disables Two-Factor authentication. The possible values are "Yes" and "No."

CERT_REVOCATION_CHECK causes iLO to use the CRL distribution point attribute of the client certificate, to download the CRL and check against revocation. The possible values are "Yes" and "No." If this setting is set to Yes, and the CRL cannot be downloaded for any reason, authentication will be denied.

CERT_OWNER_SAN causes iLO to extract the User Principle Name from the Subject Alternative Name, and use that for authentication with the directory, for example: username@domain.extension.

CERT_OWNER_SUBJECT causes iLO to derive the user's distinguished name from the subject name. For example if the subject name is "/DC=com/DC=domain/OU=organization/CN=user", iLO will derive: "CN=user,OU=organization,DC=domain,DC=com".

The CERT_OWNER_SAN and CERT_OWNER_SUBJECT settings are only used if directory authentication is enabled.

IMPORT_CA_CERTIFICATE imports the certificate into iLO as the trusted Certificate Authority. iLO will only allow client certificates that are issued by this CA. A Trusted CA certificate must be configured in iLO in order for Two-Factor authentication to function.

IMPORT_USER_CERTIFICATE imports the certificate into iLO and maps it to the specified local user. Any client that authenticates with this certificate will authenticate as the local user to which it is mapped. The SHA1 hash of this certificate will be displayed on the Modify User web page for the user to whom it is mapped. If iLO is using directory authentication, client certificate mapping to local user accounts is optional and only necessary if authentication with local accounts is desired.

The IMPORT_CA_CERTIFICATE and IMPORT_USER_CERTIFICATE settings require that base64 encoded certificate data be included between the begin and end tags.

MOD_TWOFACOR_SETTINGS runtime errors

The possible MOD_TWOFACOR_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- This setting cannot be changed while Shared Network port is enabled.
iLO has been configured to use shared network port, which will not function if Two-factor authentication is enabled
- This setting cannot be enabled unless a trusted CA certificate has been imported.
A CA certificate must be imported before enabling Two-factor authentication.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_HOST_POWER_REG_INFO

The GET_HOST_POWER_REG_INFO command requests iLO power regulator information. For this command to parse correctly, the GET_HOST_POWER_REG_INFO command must appear within a SERVER_INFO command block, and SERVER_INFO_MODE must be set to read.

Example:

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

GET_HOST_POWER_REG_INFO parameters

None

GET_HOST_POWER_REG_INFO runtime errors

GET_HOST_POWER_REG_INFO returns a runtime error if an iLO Advanced License is not found. For example:

```
<RIBCL VERSION="2.22">
  <RESPONSE
    STATUS="0x0043"
    MESSAGE='This feature requires an advanced license'
  />
</RIBCL>
```

GET_HOST_POWER_REG_INFO return messages

The GET_HOST_POWER_REG_INFO command returns all data available at the time of the request. If the request occurs within the first five minutes of a system or iLO reset or power cycle, only a limited amount of data is available.

A possible GET_HOST_POWER_REG_INFO return message within the five minutes of a system or iLO reset or power cycle is:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>0</NumberProcessors>
<NumberPstates>0</NumberPstates>
</GET_HOST_POWER_REG_INFO>
```

A possible GET_HOST_POWER_REG_INFO return message when all data is available is:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>2</NumberProcessors>
<NumberPstates>3</NumberPstates>
<Processor0>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
```

```
<TotalAverage>0</TotalAverage>
</Pstate3>
.....
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor0>

<Processor1>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
.....
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor1>
</GET_HOST_POWER_REG_INFO>
```


HPQLOMGC command language

In this section

Using HPQLOMGC	77
ILO_CONFIG.....	78

Using HPQLOMGC

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.

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\ilol140.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" />
  </MOD_DIR_CONFIG>
</RIBCL>
```

```
<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\Admin1" />
<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
- MOD_DIR_CONFIG

iLO parameters

In this section

Network Settings parameters	79
Directory settings parameters	82

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.
Duplex	N/A (autoselect)	Use this setting to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.


Parameter	Default value	Definition
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: <ul style="list-style-type: none"> • 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.
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.

Parameter	Default value	Definition
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	iLOXXXXXXXXX XXXX, where the 12 Xs 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.
<i>Blade server parameters</i>		
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.

Parameter	Default value	Definition
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.

Directory settings parameters

Parameter	Default value	Definition
Disable 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.
Schema-free directory	Yes	This parameter enables or disables the use of schema-free directories.
Use HP extended schema	No	This parameter enables or disables the use of extended schema directories.
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.

Parameter	Default value	Definition
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.
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."

Technical support

In this section

HP contact information.....	85
Before you contact HP.....	85

HP contact information

For the name of the nearest HP authorized reseller:

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

For HP technical support:

- In North America:
 - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
 - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (<http://www.hp.com>).
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to the HP website (<http://www.hp.com>).

Before you contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)

- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

Acronyms and abbreviations

ACPI

Advanced Configuration and Power Interface

ARP

Address Resolution Protocol

ASCII

American Standard Code for Information Interchange

ASM

Advanced Server Management

ASR

Automatic Server Recovery

CA

certificate authority

CGI

Common Gateway Interface

CLI

Command Line Interface

CLP

command line protocol

CR

Certificate Request

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

SMASH

System Management Architecture for Server Hardware

SNMP

Simple Network Management Protocol

SSH

Secure Shell

SSL

Secure Sockets Layer

TCP

Transmission Control Protocol

UART

universal asynchronous receiver-transmitter

UID

unit identification

USB

universal serial bus

VM

Virtual Machine

VPN

virtual private networking

WINS

Windows® Internet Naming Service

XML

extensible markup language

Index

A

additional information 85
 ASR (Automatic Server Recovery) 87
 authorized reseller 85
 Automatic Server Recovery (ASR) 87

C

CGI, software components 27
 command syntax 50, 51, 52, 53, 58, 59, 63, 65
 commands 9, 15, 17, 50, 51, 53, 58, 59, 63, 65
 configuration parameters 79, 82
 configuration procedures 43, 44, 45
 configuration utilities 37
 contacting HP 85

D

data types 47
 DHCP (Dynamic Host Configuration Protocol) 88
 Directory Services 82
 Directory settings 82

E

error messages 47, 50, 53, 58, 63, 68

F

features 7

G

GET_DIR_CONFIG 63
 GET_GLOBAL_SETTINGS 58
 GET_HOST_POWER_REG_INFO 73
 GET_HOST_POWER_STATUS 51

GET_NETWORK_SETTINGS 50
 GET_TWOFACITOR_SETTINGS 68

H

help resources 85
 HP Technical Support 85
 HPONCFG (HP Lights-Out Configuration),
 installation 39
 HPONCFG (HP Lights-Out Online
 Configuration) 37
 HPONCFG (HP Lights-Out Online
 Configuration), commands 41
 HPONCFG (HP Lights-Out Online
 Configuration), requirements 37
 HPONCFG (HP Lights-Out Online
 Configuration), using 39, 42
 HPQLOMGC 77

I

iLO settings 11

L

LAN 90

M

MOD_DIR_CONFIG 65
 MOD_GLOBAL_SETTINGS 59
 MOD_NETWORK_SETTINGS 53
 MOD_TWOFACITOR_SETTINGS 69
 Mxagentoconfig 32

N

network settings 79
 NIC (network interface controller) 91

P

parameters 41, 50, 52, 53, 55, 58, 60, 63, 66,
 68, 79, 82

phone numbers 85

R

required information 85

return messages 50, 52, 58, 64, 69, 74

RIBCL 47

runtime errors 48, 50, 52, 53, 58, 63, 69, 74

S

scripts 27, 37

SNMP settings 15

SSH Key authorization 31

SSH key authorization, tool definition files 32

SSH keys, importing 32

support 85

supported operating systems 37

U

user account, adding 47

V

Virtual Media 17

virtual media image files 27

W

website, HP 85