

# HP iLO 4 Scripting and Command Line Guide

## Abstract

This document describes the syntax and tools available for use with the HP iLO firmware through the command line or a scripted interface. 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.

Use this guide for HP iLO ProLiant servers and ProLiant BladeSystem server blades. For information about iLO for Integrity servers and server blades, see the HP website at <http://www.hp.com/go/integrityiLO>.



© Copyright 2012, 2014 Hewlett-Packard Development Company, L.P

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

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

#### **Acknowledgments**

Microsoft® and Windows®, are U.S. registered trademarks of Microsoft Corporation.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

Java is a registered trademark of Oracle and/or its affiliates.

#### **Warranty**

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Management products.

# Contents

<b>1</b>	<b>Introduction</b>	<b>13</b>
	Scripting and command line guide overview	13
	Scripting and command line utilities	13
	HPQLOCFG Utility	14
	LOCFG.PL Script	14
	HPONCFG Utility	14
	SMASH CLP	14
	IPMI	15
	New in this version	15
	HP Insight Control server deployment	16
<b>2</b>	<b>HPQLOCFG usage</b>	<b>17</b>
	Configuring for unauthenticated XML queries	17
	Creating a system collection in HP SIM	19
	Launch applications with HP SIM custom tools	19
	Batch processing using HPQLOCFG	19
	HPQLOCFG command line parameters	20
	Using quote characters	20
	Command line switches	21
	Using variables and name value pairs with HPQLOCFG	21
<b>3</b>	<b>LOCFG.PL usage</b>	<b>23</b>
	LOCFG.PL Utility	23
	LOCFG.PL command line switches	23
<b>4</b>	<b>HPONCFG online configuration utility</b>	<b>24</b>
	HPONCFG	24
	HPONCFG supported operating systems	24
	HPONCFG requirements	24
	Installing HPONCFG	24
	Windows server installation	25
	Linux server installation	25
	VMware installation	25
	HPONCFG utility	25
	HPONCFG command line parameters	26
	Using HPONCFG on Windows servers	26
	Using HPONCFG on Linux servers	27
	Obtaining the basic configuration	27
	Obtaining a specific configuration	28
	Setting a configuration	29
	Using variable substitution	29
	Capturing and restoring a configuration	30
<b>5</b>	<b>SMASH CLP usage</b>	<b>32</b>
	SMASH CLP	32
<b>6</b>	<b>IPMI usage</b>	<b>33</b>
	The IPMI utility	33
	Basic IPMI tool usage	33
	Advanced IPMI tool usage on Linux	33
	Advanced IPMIutil usage on Windows	34
<b>7</b>	<b>SMASH CLP Scripting Language</b>	<b>35</b>
	SMASH CLP command line overview	35

SMASH CLP command line access.....	35
Using the command line.....	35
Escape commands.....	36
Base commands.....	37
Specific commands.....	38
User commands.....	38
HP SSO settings.....	39
Network commands.....	41
iLO 4 settings.....	44
iLO 4 embedded health settings.....	45
SNMP settings.....	47
License commands.....	49
Directory commands.....	49
Virtual Media commands.....	51
Start and Reset commands.....	53
Firmware commands.....	54
Non-iLO firmware commands.....	55
Eventlog commands.....	55
Blade commands.....	56
Boot commands.....	56
LED commands.....	59
System properties and targets.....	60
Other commands.....	63
<b>8 RIBCL XML Scripting Language.....</b>	<b>64</b>
Overview of the RIBCL.....	64
XML headers.....	64
Data types.....	65
String.....	65
Specific string.....	66
Boolean string.....	66
Response definitions.....	66
RIBCL.....	66
RIBCL parameters.....	66
RIBCL runtime errors.....	67
Combining multiple commands in one RIBCL script.....	67
LOGIN.....	68
LOGIN parameters.....	69
LOGIN runtime errors.....	69
USER_INFO.....	69
ADD_USER.....	69
ADD_USER parameters.....	70
ADD_USER runtime errors.....	70
DELETE_USER.....	71
DELETE_USER parameter.....	71
DELETE_USER runtime errors.....	71
DEL_USERS_SSH_KEY.....	71
DEL_SSH_KEY parameters.....	72
DEL_SSH_KEY runtime errors.....	72
GET_USER.....	72
GET_USER parameter.....	72
GET_USER runtime errors.....	72
GET_USER return messages.....	72
MOD_USER.....	73
MOD_USER parameters.....	73

MOD_USER runtime errors.....	74
GET_ALL_USERS.....	74
GET_ALL_USERS parameters.....	75
GET_ALL_USERS runtime errors.....	75
GET_ALL_USERS return messages.....	75
GET_ALL_USER_INFO.....	75
GET_ALL_USER_INFO parameters.....	75
GET_ALL_USER_INFO runtime errors.....	76
GET_ALL_USER_INFO return messages.....	76
RIB_INFO.....	76
RESET_RIB.....	77
RESET_RIB parameters.....	77
RESET_RIB runtime errors.....	77
GET_EVENT_LOG.....	77
GET_EVENT_LOG parameters.....	77
GET_EVENT_LOG runtime errors.....	78
GET_EVENT_LOG return messages.....	78
GET_FEDERATION_MULTICAST.....	79
GET_FEDERATION_MULTICAST parameters.....	79
GET_FEDERATION_MULTICAST runtime errors.....	79
GET_FEDERATION_MULTICAST return messages.....	79
SET_FEDERATION_MULTICAST.....	79
SET_FEDERATION_MULTICAST parameters.....	80
SET_FEDERATION_MULTICAST runtime errors.....	80
GET_FEDERATION_ALL_GROUPS.....	80
GET_FEDERATION_ALL_GROUPS parameters.....	80
GET_FEDERATION_ALL_GROUPS runtime errors.....	80
GET_FEDERATION_ALL_GROUPS return messages.....	81
GET_FEDERATION_ALL_GROUPS_INFO.....	81
GET_FEDERATION_ALL_GROUPS_INFO parameters.....	81
GET_FEDERATION_ALL_GROUPS_INFO runtime errors.....	81
GET_FEDERATION_ALL_GROUPS_INFO return messages.....	81
GET_FEDERATION_GROUP.....	82
GET_FEDERATION_GROUP parameters.....	82
GET_FEDERATION_GROUP runtime errors.....	82
GET_FEDERATION_GROUP return messages.....	83
ADD_FEDERATION_GROUP.....	83
ADD_FEDERATION_GROUP parameters.....	83
ADD_FEDERATION_GROUP runtime errors.....	84
MOD_FEDERATION_GROUP.....	84
MOD_FEDERATION_GROUP parameters.....	84
MOD_FEDERATION_GROUP runtime errors.....	85
DELETE_FEDERATION_GROUP.....	85
DELETE_FEDERATION_GROUP parameters.....	85
DELETE_FEDERATION_GROUP runtime errors.....	85
CLEAR_EVENTLOG.....	86
CLEAR_EVENTLOG parameters.....	86
CLEAR_EVENTLOG runtime errors.....	86
COMPUTER_LOCK_CONFIG.....	86
COMPUTER_LOCK_CONFIG parameters.....	87
COMPUTER_LOCK_CONFIG runtime errors.....	87
GET_NETWORK_SETTINGS.....	87
GET_NETWORK_SETTINGS parameters.....	87
GET_NETWORK_SETTINGS runtime errors.....	87
GET_NETWORK_SETTINGS return messages.....	88

MOD_NETWORK_SETTINGS.....	89
MOD_NETWORK_SETTINGS runtime errors.....	92
MOD_NETWORK_SETTINGS parameters.....	92
GET_GLOBAL_SETTINGS.....	96
GET_GLOBAL_SETTINGS parameters.....	96
GET_GLOBAL_SETTINGS runtime errors.....	96
GET_GLOBAL_SETTINGS return messages.....	96
MOD_GLOBAL_SETTINGS.....	97
MOD_GLOBAL_SETTINGS parameters.....	98
MOD_GLOBAL_SETTINGS runtime errors.....	100
BROWNOUT_RECOVERY.....	101
BROWNOUT_RECOVERY parameters.....	101
BROWNOUT_RECOVERY runtime errors.....	101
GET_SNMP_IM_SETTINGS.....	101
GET_SNMP_IM_SETTINGS parameters.....	101
GET_SNMP_IM_SETTINGS runtime errors.....	101
GET_SNMP_IM_SETTINGS return messages.....	102
MOD_SNMP_IM_SETTINGS.....	102
MOD_SNMP_IM_SETTINGS parameters.....	104
MOD_SNMP_IM_SETTINGS runtime errors.....	105
MOD_ENCRYPT_SETTINGS.....	105
MOD_ENCRYPT_SETTINGS parameters.....	106
MOD_ENCRYPT_SETTINGS runtime errors.....	106
GET_ENCRYPT_SETTINGS.....	107
GET_ENCRYPT_SETTINGS parameters.....	107
GET_ENCRYPT_SETTINGS runtime errors.....	107
GET_ENCRYPT_SETTINGS return messages.....	107
UPDATE_RIB_FIRMWARE and UPDATE_FIRMWARE.....	107
UPDATE_FIRMWARE parameters.....	108
UPDATE_FIRMWARE runtime errors.....	108
UPDATE_LANG_PACK.....	109
UPDATE_LANG_PACK parameters.....	109
UPDATE_LANG_PACK runtime errors.....	109
GET_FW_VERSION.....	109
GET_FW_VERSION parameters.....	109
GET_FW_VERSION runtime errors.....	110
GET_FW_VERSION return messages.....	110
LICENSE.....	110
LICENSE parameters.....	110
LICENSE runtime errors.....	110
INSERT_VIRTUAL_MEDIA.....	111
INSERT_VIRTUAL_MEDIA parameters.....	111
INSERT_VIRTUAL_MEDIA runtime errors.....	112
EJECT_VIRTUAL_MEDIA.....	112
EJECT_VIRTUAL_MEDIA parameters.....	112
EJECT_VIRTUAL_MEDIA runtime errors.....	112
GET_VM_STATUS.....	112
GET_VM_STATUS parameters.....	113
GET_VM_STATUS runtime errors.....	113
GET_VM_STATUS return messages.....	113
SET_VM_STATUS.....	113
SET_VM_STATUS parameters.....	114
SET_VM_STATUS runtime errors.....	115
CERTIFICATE_SIGNING_REQUEST.....	115
CERTIFICATE_SIGNING_REQUEST parameters (for custom CSR).....	116

CERTIFICATE_SIGNING_REQUEST errors.....	116
IMPORT_CERTIFICATE.....	116
IMPORT_CERTIFICATE parameters.....	117
IMPORT_CERTIFICATE errors.....	117
AHS_CLEAR_DATA.....	117
AHS_CLEAR_DATA parameters.....	117
AHS_CLEAR_DATA runtime errors.....	117
GET_AHS_STATUS.....	117
GET_AHS_STATUS parameters.....	118
GET_AHS_STATUS runtime errors.....	118
SET_AHS_STATUS.....	118
SET_AHS_STATUS parameters.....	118
SET_AHS_STATUS runtime errors.....	118
ERS_AHS_Submit.xml (TRIGGER_BB_DATA).....	118
ERS_AHS_Submit.xml (TRIGGER_BB_DATA) parameters.....	119
ERS_AHS_Submit.xml (TRIGGER_BB_DATA) runtime errors.....	119
DISABLE_ERS.....	119
DISABLE_ERS parameters.....	119
DISABLE_ERS runtime errors.....	119
GET_ERS_SETTINGS.....	119
GET_ERS_SETTINGS parameters.....	119
GET_ERS_SETTINGS runtime errors.....	119
SET_ERS_IRS_CONNECT.....	120
SET_ERS_IRS_CONNECT parameters.....	120
SET_ERS_IRS_CONNECT runtime errors.....	120
TRIGGER_L2_COLLECTION.....	120
TRIGGER_L2_COLLECTION parameters.....	120
TRIGGER_L2_COLLECTION runtime errors.....	120
TRIGGER_TEST_EVENT.....	120
TRIGGER_TEST_EVENT parameters.....	121
TRIGGER_TEST_EVENT runtime errors.....	121
SET_ERS_DIRECT_CONNECT.....	121
SET_ERS_DIRECT_CONNECT parameters.....	121
SET_ERS_DIRECT_CONNECT runtime errors.....	121
DC_REGISTRATION_COMPLETE.....	122
DC_REGISTRATION_COMPLETE parameters.....	122
DC_REGISTRATION_COMPLETE runtime errors.....	122
SET_ERS_WEB_PROXY.....	122
SET_ERS_WEB_PROXY parameters.....	123
SET_ERS_WEB_PROXY runtime errors.....	123
SET_LANGUAGE.....	123
SET_LANGUAGE parameters.....	123
SET_LANGUAGE runtime errors.....	123
GET_LANGUAGE.....	123
GET_LANGUAGE parameters.....	124
GET_LANGUAGE runtime errors.....	124
GET_ALL_LANGUAGES.....	124
GET_ALL_LANGUAGES parameters.....	124
GET_ALL_LANGUAGES runtime errors.....	124
GET_ASSET_TAG.....	124
GET_ASSET_TAG parameters.....	124
GET_ASSET_TAG runtime errors.....	124
SET_ASSET_TAG.....	124
SET_ASSET_TAG parameters.....	125
SET_ASSET_TAG runtime errors.....	125

GET_SECURITY_MSG.....	125
GET_SECURITY_MSG parameters.....	125
GET_SECURITY_MSG return messages.....	126
GET_SECURITY_MSG runtime errors.....	126
SET_SECURITY_MSG.....	126
SET_SECURITY_MSG parameters.....	126
SET_SECURITY_MSG runtime errors.....	126
GET_SPATIAL.....	126
GET_SPATIAL parameters.....	127
GET_SPATIAL return messages.....	127
GET_SPATIAL runtime errors.....	128
HOTKEY_CONFIG.....	128
HOTKEY_CONFIG parameters.....	128
HOTKEY_CONFIG runtime errors.....	129
GET_HOTKEY_CONFIG.....	129
GET_HOTKEY_CONFIG parameters.....	130
GET_HOTKEY_CONFIG runtime errors.....	130
GET_HOTKEY_CONFIG return messages.....	130
PROFILE_APPLY.....	130
PROFILE_APPLY parameters.....	130
PROFILE_APPLY runtime errors.....	130
PROFILE_APPLY_GET_RESULTS.....	131
PROFILE_APPLY_GET_RESULTS parameters.....	131
PROFILE_APPLY_GET_RESULTS runtime errors.....	132
PROFILE_DELETE.....	132
PROFILE_DELETE parameters.....	132
PROFILE_DELETE runtime errors.....	132
PROFILE_LIST.....	133
PROFILE_LIST parameters.....	133
PROFILE_LIST runtime errors.....	133
PROFILE_DESC_DOWNLOAD.....	134
PROFILE_DESC_DOWNLOAD parameters.....	134
PROFILE_DESC_DOWNLOAD runtime errors.....	134
FIPS_ENABLE.....	135
FIPS_ENABLE parameters.....	135
FIPS_ENABLE runtime errors.....	136
GET_FIPS_STATUS.....	136
GET_FIPS_STATUS parameters.....	136
GET_FIPS_STATUS runtime errors.....	136
GET_FIPS_STATUS return messages.....	136
GET_ALL_LICENSES.....	136
GET_ALL_LICENSES parameters.....	136
GET_ALL_LICENSES runtime errors.....	136
GET_ALL_LICENSES return messages.....	136
FACTORY_DEFAULTS.....	137
FACTORY_DEFAULTS parameters.....	137
FACTORY_DEFAULTS runtime errors.....	137
IMPORT_SSH_KEY.....	137
IMPORT_SSH_KEY parameters.....	138
IMPORT_SSH_KEY runtime errors.....	138
DIR_INFO.....	138
GET_DIR_CONFIG.....	138
GET_DIR_CONFIG parameters.....	139
GET_DIR_CONFIG runtime errors.....	139
GET_DIR_CONFIG return messages.....	139

MOD_DIR_CONFIG.....	141
MOD_DIR_CONFIG parameters.....	143
MOD_DIR_CONFIG runtime errors.....	145
MOD_KERBEROS.....	145
RACK_INFO.....	145
GET_RACK_SETTINGS.....	146
GET_RACK_SETTINGS parameters.....	146
GET_RACK_SETTINGS runtime errors.....	146
GET_RACK_SETTINGS return messages.....	146
BLADESYSTEM_INFO.....	146
GET_OA_INFO.....	147
GET_OA_INFO parameters.....	147
GET_OA_INFO runtime errors.....	147
GET_OA_INFO return messages.....	147
SERVER_INFO.....	147
GET_TPM_STATUS.....	148
GET_TPM_STATUS parameters.....	148
GET_TPM_STATUS runtime errors.....	148
GET_TPM_STATUS return messages.....	148
GET_CURRENT_BOOT_MODE.....	149
GET_CURRENT_BOOT_MODE parameters.....	149
GET_CURRENT_BOOT_MODE runtime errors.....	149
GET_CURRENT_BOOT_MODE return messages.....	149
GET_PENDING_BOOT_MODE.....	149
GET_PENDING_BOOT_MODE parameters.....	150
GET_PENDING_BOOT_MODE runtime errors.....	150
GET_PENDING_BOOT_MODE return messages.....	150
SET_PENDING_BOOT_MODE.....	150
SET_PENDING_BOOT_MODE parameters.....	150
SET_PENDING_BOOT_MODE runtime errors.....	150
GET_PERSISTENT_BOOT.....	150
GET_PERSISTENT_BOOT return messages.....	151
SET_PERSISTENT_BOOT (Legacy).....	151
SET_PERSISTENT_BOOT parameters.....	152
SET_PERSISTENT_BOOT runtime errors.....	152
SET_PERSISTENT_BOOT (UEFI).....	152
SET_PERSISTENT_BOOT parameters.....	153
SET_PERSISTENT_BOOT runtime errors.....	153
GET_ONE_TIME_BOOT.....	153
GET_ONE_TIME_BOOT return messages.....	154
SET_ONE_TIME_BOOT.....	154
SET_ONE_TIME_BOOT parameters.....	155
SET_ONE_TIME_BOOT runtime errors.....	155
GET_SUPPORTED_BOOT_MODE.....	156
GET_SUPPORTED_BOOT_MODE return messages.....	156
GET_SUPPORTED_BOOT_MODE runtime errors.....	156
GET_SERVER_NAME.....	156
GET_SERVER_NAME return message.....	157
GET_SERVER_NAME runtime errors.....	157
SERVER_NAME.....	157
SERVER_NAME parameters.....	157
SERVER_NAME return message.....	157
SERVER_NAME runtime errors.....	157
GET_SERVER_FQDN/GET_SMH_FQDN.....	157
GET_SERVER_FQDN/GET_SMH_FQDN parameters.....	158

GET_SERVER_FQDN/GET_SMH_FQDN return messages.....	158
SERVER_FQDN/SMH_FQDN.....	158
SERVER_FQDN/SMH_FQDN parameters.....	158
SERVER_FQDN/SMH_FQDN return messages.....	158
SERVER_FQDN/SMH_FQDN runtime errors.....	159
GET_PRODUCT_NAME.....	159
GET_PRODUCT_NAME parameters.....	159
GET_PRODUCT_NAME runtime errors.....	159
GET_PRODUCT_NAME return messages.....	159
GET_EMBEDDED_HEALTH.....	159
GET_EMBEDDED_HEALTH parameters.....	160
GET_EMBEDDED_HEALTH return messages.....	160
GET_POWER_READINGS.....	168
GET_POWER_READINGS parameters.....	168
GET_POWER_READINGS return messages.....	169
GET_PWREG.....	169
GET_PWREG parameters.....	169
GET_PWREG return messages.....	169
GET_PWREG runtime errors.....	170
SET_PWREG.....	170
SET_PWREG parameters.....	170
SET_PWREG runtime errors.....	171
GET_POWER_CAP.....	171
GET_POWER_CAP parameters.....	171
GET_POWER_CAP return messages.....	171
SET_POWER_CAP.....	171
SET_POWER_CAP parameters.....	172
SET_POWER_CAP runtime errors.....	172
GET_HOST_POWER_SAVER_STATUS.....	172
GET_HOST_POWER_SAVER_STATUS parameters.....	172
GET_HOST_POWER_SAVER_STATUS runtime errors.....	172
GET_HOST_POWER_SAVER_STATUS return messages.....	172
SET_HOST_POWER_SAVER.....	173
SET_HOST_POWER_SAVER parameters.....	173
SET_HOST_POWER_SAVER runtime errors.....	173
GET_HOST_POWER_STATUS.....	173
GET_HOST_POWER_STATUS parameters.....	173
GET_HOST_POWER_STATUS runtime errors.....	174
GET_HOST_POWER_STATUS Return Messages.....	174
SET_HOST_POWER.....	174
SET_HOST_POWER Parameters.....	174
SET_HOST_POWER Runtime Errors.....	174
GET_HOST_PWR_MICRO_VER.....	174
GET_HOST_PWR_MICRO_VER parameters.....	175
GET_HOST_PWR_MICRO_VER runtime errors.....	175
GET_HOST_PWR_MICRO_VER return messages.....	175
RESET_SERVER.....	175
RESET_SERVER error messages.....	176
RESET_SERVER parameters.....	176
PRESS_PWR_BTN.....	176
PRESS_PWR_BTN parameters.....	176
PRESS_PWR_BTN runtime errors.....	176
HOLD_PWR_BTN.....	176
HOLD_PWR_BTN parameters.....	177
HOLD_PWR_BTN runtime errors.....	177

COLD_BOOT_SERVER.....	177
COLD_BOOT_SERVER parameters.....	177
COLD_BOOT_SERVER runtime errors.....	177
WARM_BOOT_SERVER.....	177
WARM_BOOT_SERVER parameters.....	178
WARM_BOOT_SERVER runtime errors.....	178
SERVER_AUTO_PWR.....	178
SERVER_AUTO_PWR parameters.....	178
SERVER_AUTO_PWR runtime errors.....	179
GET_SERVER_AUTO_PWR.....	179
GET_SERVER_AUTO_PWR parameters.....	179
GET_SERVER_AUTO_PWR return message.....	179
GET_UID_STATUS.....	179
GET_UID_STATUS parameters.....	180
GET_UID_STATUS response.....	180
UID_CONTROL.....	180
UID_CONTROL parameters.....	180
UID_CONTROL errors.....	180
SET_PERS_MOUSE_KEYBOARD_ENABLED.....	180
SET_PERS_MOUSE_KEYBOARD_ENABLED parameters.....	181
SET_PERS_MOUSE_KEYBOARD_ENABLED runtime errors.....	181
GET_PERS_MOUSE_KEYBOARD_ENABLED.....	181
GET_PERS_MOUSE_KEYBOARD_ENABLED parameters.....	181
GET_PERS_MOUSE_KEYBOARD_ENABLED return messages.....	181
GET_SERVER_POWER_ON_TIME.....	181
GET_SERVER_POWER_ON_TIME parameters.....	182
GET_SERVER_POWER_ON_TIME return message.....	182
CLEAR_SERVER_POWER_ON_TIME.....	182
CLEAR_SERVER_POWER_ON_TIME parameters.....	182
CLEAR_SERVER_POWER_ON_TIME return message.....	182
SSO_INFO.....	182
GET_SSO_SETTINGS.....	183
GET_SSO_SETTINGS parameters.....	183
GET_SSO_SETTINGS return messages.....	183
MOD_SSO_SETTINGS.....	184
MOD_SSO_SETTINGS parameters.....	184
MOD_SSO_SETTINGS runtime errors.....	185
SSO_SERVER.....	185
SSO_SERVER parameters.....	186
SSO_SERVER runtime errors.....	187
DELETE_SERVER.....	187
DELETE_SERVER parameters.....	187
DELETE_SERVER runtime errors.....	187
<b>9 Secure Shell.....</b>	<b>188</b>
SSH overview.....	188
Supported SSH features.....	188
Using Secure Shell.....	188
SSH key authorization.....	189
Tool definition files.....	189
Mxagentconfig utility.....	189
Importing SSH keys from PuTTY.....	190
Importing SSH keys generated using ssh-keygen.....	192
<b>10 PERL scripting.....</b>	<b>193</b>
Using PERL with the XML scripting interface.....	193

XML enhancements.....	193
Opening an SSL connection.....	193
Sending the XML header and script body.....	194
<b>11 iLO 4 ports.....</b>	<b>196</b>
Enabling the Shared Network Port feature through XML scripting.....	196
Re-enabling the dedicated NIC management port.....	196
<b>12 Support and other resources.....</b>	<b>198</b>
Information to collect before contacting HP.....	198
How to contact HP.....	198
Security bulletin and alert policy for non-HP owned software components.....	198
Subscription service.....	198
Registering for software technical support and update service.....	198
How to use your software technical support and update service.....	199
HP authorized resellers.....	199
Related information.....	199
<b>13 Documentation feedback.....</b>	<b>201</b>
<b>A Sample script and command reference.....</b>	<b>202</b>
<b>Glossary.....</b>	<b>206</b>
<b>Index.....</b>	<b>208</b>

---

# 1 Introduction

## Scripting and command line guide overview

HP iLO 4 provides multiple ways to configure, update, and operate HP ProLiant servers remotely. The *HP iLO User Guide* describes each feature and explains how to use these features with the browser-based interface and RBSU. For more information, see the *HP iLO User Guide* on the HP website at <http://www.hp.com/go/ilo/docs>.

The *HP iLO Scripting and Command Line Guide* describes the syntax and tools available to use iLO 4 through a command line or scripted interface.

Sample XML scripts downloaded from the HP website contain commands for all iLO firmware. Unless otherwise specified, the examples in this guide are for iLO 4 firmware version 1.40 and later. Before using the sample scripts, review the firmware support information in each script to tailor the script for the intended firmware and version. Download the sample scripts from the HP website at <http://www.hp.com/go/ilo>. Click **iLO Sample Scripts for Windows** or **Lights-Out XML scripting sample for Linux** on the **Resources** tab, under **Support**.

Throughout this manual, iLO 4 is referred to as iLO.

In addition to the GUI, the iLO firmware provides multiple ways to configure and control iLO and the server using scripts and command line instructions.

The scripting tools provide a method to configure multiple iLO systems, to incorporate a standard configuration into the deployment process, and to control servers and subsystems. Using the scripting tools enables you to:

- Change the Administrator password on all your iLO systems
- Configure LDAP directory service settings
- Control the server power state
- Attach a virtual media CD/DVD to the host server
- Update the iLO firmware
- Retrieve power consumption data
- Issue various configuration and control commands

The command line tools provide quick and easy methods to send commands to the iLO firmware and host servers.

## Scripting and command line utilities

This section describes the following scripting and command line tools:

- HPQLOCFG.EXE
- LOCFG.PL
- HPONCFG.EXE
- SMASH CLP
- IPMI

The current version of iLO introduces RIBCL headers that offer expanded script functionality. Upgrade any of the utilities you use to the versions listed below to take advantage of the expanded functionality.

The current version of iLO 4 requires upgrades to the following utilities:

**Table 1 HP iLO 4 1.40 scripting and command line utilities required versions**

Utility	Version	Version notes for iLO 4 1.40
HPQLOCFG	1.1	HP Lights-Out Configuration Utility. This replaces the CPQLOCFG utility.
HPONCFG	4.3.0	To use this version of the HP Lights-Out Online Configuration Utility you must also upgrade your Channel Interface Driver (CHIF) to version 3.9.0.0.
LOCFG.PL	4.30	This utility is available in the HP Lights-Out XML Scripting Sample 4.2.0 bundle.
HPLOMIG	4.30	Update to this version of HPLOMIG before installing the iLO 4 1.40 update.

**NOTE:** Upgrades are required only for the utilities you use. Continuing to use utilities without the update will cause the following inform message to appear:

Scripting utility should be updated to the latest version.

## HPQLOCFG Utility

The HP Lights-Out Configuration Utility (HPQLOCFG.EXE) utility replaces the previously used CPQLOCFG.EXE utility. HPQLOCFG is a Windows command line utility that sends XML configuration and control scripts over the network to iLO. Run this utility manually from a Windows command prompt, or create a batch file to run the same script to many iLO devices.

The tool accepts properly formatted XML scripts containing commands and values; see the XML scripts in the *iLO Sample Scripts for Windows* or the *HP Lights-Out XML Scripting Sample for Linux* for examples of proper formatting. All available commands are detailed later in this guide. HPQLOCFG also integrates with HP SIM for easy launching of the same script on multiple devices.

## LOCFG.PL Script

The LOCFG.PL scripting utility is a PERL script that provides similar functionality as the HPQLOCFG utility. Run this tool on any client that has a compatible PERL environment (including OpenSSL) installed. This tool uses the same XML scripts as HPQLOCFG input files.

## HPONCFG Utility

Use the HPONCFG.EXE utility to send XML configuration and control scripts (the same scripts as HPQLOCFG) from the server host operating system to iLO. HPONCFG has both Windows and Linux versions. One common usage is to run an HPONCFG script to configure iLO to a standard configuration at the end of your server deployment process. HPONCFG integrates with HP RDP and also runs at the end of an unattended OS installation.

When you run HPONCFG from the host operating system, you must be logged in to the host server using an Administrator or root level user account. An iLO user ID and password is not required.

Windows server operating systems also have the HPONCFG\_GUI.EXE utility. This utility provides the same basic configuration capabilities as the iLO F8 ROM-RBSU during the server boot-up process.

## SMASH CLP

SMASH CLP is the DMTF suite of specifications that deliver industry-standard protocols and profiles to unify the management of the data center. The SMASH CLP specification enables simple and intuitive management of heterogeneous servers in a data center.

SMASH CLP provides a standardized set of commands for configuration and control of management processors (called Management Access Points) and host systems. On iLO, access SMASH CLP through the SSH port.

## IPMI

The IPMI specification is a standard that defines a set of common interfaces to a computer system. System administrators can use IPMI to monitor system health and manage the system. IPMI 2.0 defines a mandatory system interface, and an optional LAN interface. The iLO processor supports both interfaces.

The IPMI specification defines a standardized interface for platform management. The IPMI specification defines the following types of platform management:

- Monitors the status of system information, such as fans, temperatures, and power supplies
- Recovery capabilities, such as system resets and power on/off operations
- Logging capabilities for abnormal events, such as over-temperature readings or fan failures
- Inventory capabilities, such as identifying failed hardware components

IPMI commands are sent to iLO using a third-party or open source utility, such as IPMITOOL, IPMIUTIL, OpenIPMI or FreeIPMI.

You must be familiar with IPMI specifications when issuing raw commands. For additional information, see the IPMI specification on the Intel website at <http://www.intel.com/design/servers/ipmi/tools.htm>.

## New in this version

This guide reflects changes in the iLO 4 firmware. This guide covers iLO 4 firmware version 1.40 and later.

The following updates or additions were made:

- iLO Federation Management

---

**NOTE:** iLO Federation Management is supported on IPv4 and IPv6 networks on the iLO Dedicated Network Port. It is not supported on iLO Shared Network Port. If you receive a data inconsistency error when using iLO Federation Management, refer to the multisystem map page for troubleshooting. HP ProLiant Blade servers must have Onboard Administrator v4.11 installed before using iLO Federation Management.

---

- Insight Remote Support Direct Connect configuration
- HP Enterprise Secure Key Manager ESKM 3.1 and later, which can be used in conjunction with HP Secure Encryption.
- Improved Java Integrated Remote Console (IRC)
- UEFI System Utilities on the HP ProLiant DL580 Gen8 server
- Added the following commands:
  - Federation commands:
    - ADD\_FEDERATION\_GROUP
    - DELETE\_FEDERATION\_GROUP
    - GET\_FEDERATION\_ALL\_GROUPS
    - GET\_FEDERATION\_ALL\_GROUPS\_INFO
    - GET\_FEDERATION\_GROUP
    - GET\_FEDERATION\_MULTICAST

- MOD\_FEDERATION\_GROUP
- SET\_FEDERATION\_MULTICAST
- Insight Remote Support Direct Connect commands:
  - DC\_REGISTRATION\_COMPLETE
  - SET\_ERS\_DIRECT\_CONNECT
  - SET\_ERS\_WEB\_PROXY
- Boot configuration commands:
  - GET\_CURRENT\_BOOT\_MODE
  - GET\_PENDING\_BOOT\_MODE
  - GET\_SUPPORTED\_BOOT\_MODE
  - SET\_PENDING\_BOOT\_MODE
- Encryption commands:
  - GET\_ENCRYPT\_SETTINGS
  - GET\_TPM\_STATUS
  - MOD\_ENCRYPT\_SETTINGS
- Updated the following commands:
  - SET\_ONE\_TIME\_BOOT
  - SET\_PERSISTENT\_BOOT

## HP Insight Control server deployment

HP Insight Control server deployment integrates with iLO to enable the management of remote servers and to monitor the performance of remote console operations, regardless of the state of the operating system or hardware.

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

For more information about the HP Insight Control server deployment, see the documentation that ships on the HP Insight software DVD, or the HP website at <http://www.hp.com/go/insightcontrol>.

---

## 2 HPQLOCFG usage

The HPQLOCFG.EXE utility is a Windows-based utility that connects to iLO using a secure connection over the network. RIBCL scripts are passed to iLO over the secure connection to HPQLOCFG. This utility requires a valid user ID and password with the appropriate privileges. Launch the HPQLOCFG utility from HP SIM for Group Administration, or launch it independently from a command prompt for batch processing.

Download this utility from the HP website at: <http://www.hp.com/support/ilo4>.

Version 1.0 or later of HPQLOCFG is required to support all features of iLO 4 v1.40.

HP SIM discovers iLO devices as management processors. HPQLOCFG sends a RIBCL file to a group of iLO devices to manage the user accounts for those iLO devices. The iLO devices then perform the action designated by the RIBCL file and send a response to the log file.

Use HPQLOCFG to execute RIBCL scripts on iLO. HPQLOCFG must reside on the same server as HP SIM. HPQLOCFG generates two types of error messages; runtime errors, and syntax errors.

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

```
C:\Program Files\HP\System Insight Manager\
```

- Syntax errors occur when an invalid XML tag is encountered. When a syntax error occurs, HPQLOCFG stops running and logs the error in the runtime script and output log file. Syntax errors use the following format:

```
Syntax error: expected X but found Y.
```

For example:

```
Syntax error: expected USER_LOGIN=userlogin  
but found USER_NAME=username
```

### Configuring for unauthenticated XML queries

If configured to do so, the iLO device returns identifying information in response to an unauthenticated XML query. By default, the iLO device is configured to return this information.

To disable this feature, set the `CIM_SECURITY_MASK` in the `MOD_SNMP_IM_SETTINGS` command to disable unauthenticated XML query return information.

You can also disable the unauthenticated XML query information through the iLO web interface:

1. Go to **Administration**→**Management**.  
The **Management** page appears.
2. Under the **Insight Management Integration** heading, click the menu for the **Level of Data Returned** option.  
There are two options in the menu:
  - 1) Enabled (iLO+Server Association Data)
  - 2) Disabled (No Response to Request)
3. Select 2) Disabled (No Response to Request) to disable unauthenticated XML query return information

---

**NOTE:** You must have unauthenticated XML query enabled if you are performing device discoveries with HP SIM.

---

To obtain unauthenticated identifying information, enter the following command to the iLO web server port:

**https://<ioloadaddress>/xmldata?item=all**

Alternatively, you can select option **1) Enabled (iLO+Server Association Data)** from iLO.

A typical response is:

```
<RIMP>
<HSI>
<SBSN>ABC12345678</SBSN>
<SPN>ProLiant BL460c Gen8</SPN>
<UUID>BL4608CN71320ZNN</UUID>
<SP>0</SP>
<cUUID>36344C42-4E43-3830-3731-33305A4E4E32</cUUID>
<VIRTUAL>
<STATE>Inactive</STATE>
<VID>
<BSN/>
<cUUID/>
</VID>
</VIRTUAL>
<PRODUCTID>BL4608-101</PRODUCTID>
<NICS>
<NIC>
<PORT>1</PORT>
<MACADDR>00:17:a4:77:08:02</MACADDR>
</NIC>
<NIC>
<PORT>2</PORT>
<MACADDR>00:17:a4:77:08:04</MACADDR>
</NIC>
<NIC>
<PORT>3</PORT>
<MACADDR>00:17:a4:77:08:00</MACADDR>
</NIC>
<NIC>
<PORT>4</PORT>
<MACADDR>9c:8e:99:13:20:cd</MACADDR>
</NIC>
<NIC>
<PORT>5</PORT>
<MACADDR>9c:8e:99:13:20:ca</MACADDR>
</NIC>
<NIC>
<PORT>6</PORT>
<MACADDR>9c:8e:99:13:20:ce</MACADDR>
</NIC>
<NIC>
<PORT>7</PORT>
<MACADDR>9c:8e:99:13:20:cb</MACADDR>
</NIC>
<NIC>
<PORT>8</PORT>
<MACADDR>9c:8e:99:13:20:cf</MACADDR>
</NIC>
</NICS>
</HSI>
<MP>
<ST>1</ST>
<PN>Integrated Lights-Out 4 (iLO 4)</PN>
<FWRI>1.01</FWRI>
<BBLK>08/30/2011</BBLK>
<HWRI>ASIC: 16</HWRI>
<SN>ILOABC12345678</SN>
<UUID>ILOBL4608ABC12345678</UUID>
<IPM>1</IPM>
```

```

<SSO>0</SSO>
<PWRM>3.0</PWRM>
<ERS>0</ERS>
<EALERT>1</EALERT>
</MP>
<BLADESYSTEM>
<BAY>1</BAY>
<MANAGER>
<TYPE>Onboard Administrator</TYPE>
<MGMTIPADDR>123.456.78.90</MGMTIPADDR>
<RACK>TestRACK</RACK>
<ENCL>TestRACKEnc-C</ENCL>
<ST>2</ST>
</MANAGER>
</BLADESYSTEM>
</RIMP>

```

## Creating a system collection in HP SIM

To quickly see all system management processors, login to SIM and in the **System and Event Collections** panel, scroll down to and select **All Management Processors**. The **All Management Processors** page appears.

To create a custom group of all iLO devices (or by iLO version), create a system collection.

1. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections appear.
3. Click **New**. The New Collection section appears.
4. Select **Choose members by attributes**.
5. In the **Search for** dropdown list, select **systems**.
6. In the **where** dropdown, select **system sub type**, and select **is** from the inclusion/exclusion dropdown.
7. Select an Integrated Lights-Out choice from the system sub type dropdown at the right.
8. Click one of the following:
  - **View** — to run the search and display results immediately.
  - **Save as Collection** — to save the collection.
  - **Cancel** — to close the New Collection section without saving any changes.

## Launch applications with HP SIM custom tools

Use custom tools in HP SIM to combine RIBCL, HPQLOCFG, and system collection to manage Group Administration of iLO devices. Custom tools are executed on the CMS and on target systems. You can create a remote tool that runs on selected target systems, and even schedule its execution.

For more information about custom tools, see the HP SIM help.

## Batch processing using HPQLOCFG

Group Administration is also delivered to iLO through batch processing. The components needed for batch processing are HPQLOCFG, a RIBCL file, and a batch file.

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

```

REM Updating the HP Integrated Lights-Out 3 board
REM Repeat line for each board to be updated
REM

```

```
HPQLOCFG -S RIB1 -F C:\...\SCRIPT.XML -L RIB1LOG.TXT -V
HPQLOCFG -S RIB2 -F C:\...\SCRIPT.XML -L RIB2LOG.TXT -V
HPQLOCFG -S RIB3 -F C:\...\SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...\SCRIPT.XML -L LOGFILE.TXT -V
HPQLOCFG overwrites any existing log files.
```

## HPQLOCFG command line parameters

For information on the syntax of the XML data files, see “RIBCL XML Scripting Language” (page 64). Download sample XML scripts from the HP website at <http://www.hp.com/go/ilo>. Click **iLO Sample Scripts for Windows** or **Lights-Out XML scripting sample for Linux** on the **Resources** tab, under **Support**.

## Using quote characters

The restrictions for using single and double-quote characters are based on whether they are passed to HPQLOCFG inside an XML script or on the command line.

### Quotes inside XML scripts

When using an XML script to enter the user name and password use the double-quote (") as delimiters. However, if you must use " inside the user name or password in the XML file (if the user name or password has double quotes in it), change the outside double-quote delimiters to single quotes (').

For example, consider a username with quotes in it:

```
Sample"simple"name
```

This must be in an XML script as:

```
'Sample"simple"name'
```

---

**NOTE:** Support for Windows-specific smart-quotes (“ ” and ‘ ’) as content delimiters in XML is being phased out. Be sure to replace any smart-quote characters in your script with normal double or single quotes (" and ').

---

### Quotes on the command line

When using HPQLOCFG or LOCFG and entering the password or command on the command line with the `-p` option, you cannot normally use the double-quote special character ("), except when using an ampersand (&) or less-than (<) symbol. To enter a password or command that uses either of these special characters, use double-quotes.

For example:

- "admin&admin"
- "admin<admin"

When using LOCFG and entering the password or command on the command line with the `-i` option, do not include double-quotes around the password.

For example:

```
admin&admin
admin<admin
```

Passwords or commands delimited with double-quotes do not work on the LOCFG command line with the `-i` option.

## Command line switches

The following command line switches are available to be used with HPQLOCFG.EXE:

**Table 2 HPQLOCFG command line switches**

Switch	Effect
-S	Determines the iLO that is to be updated. This switch is followed by either the DNS name or IP address of the target server. When using IPv6 addresses, you can optionally add the port number preceded by a colon (<IPv6_address:port>). <b>NOTE:</b> Do not use this switch if you are launching from HP SIM. HP SIM automatically provides the address of the iLO when you launch HPQLOCFG.
-F	Full path location and name of the RIBCL file that contains the actions to be performed.
-U	User login name. Entering this at the command line overrides the user login name from the script.
-P	Password. Entering this at the command line overrides the password from the script.
-L <sup>1</sup>	Defines the log file name and file location. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch HPQLOCFG. Ensure that HPQLOCFG is in a directory referenced by the PATH environment variable. Any log files generated are placed in the same directory as the HPQLOCFG executable. This switch cannot designate an output log filename. The default filename is based on the DNS name or the IP address. <b>NOTE:</b> Do not use this switch if launching from HP SIM. The output values may need to be modified to match the RIBCL syntax.
-V <sup>1</sup>	Enables verbose message return. The resulting log file contains all commands sent, all responses received, and any errors. By default, only errors and responses from GET commands are logged without this switch.
-t namevaluepairs	The -t namevaluepairs switch substitutes variables (%variable%) in the input file with values specified in name-value pairs. Separate multiple name-value pairs with a comma. See "Using variables and name value pairs with HPQLOCFG" (page 21).

<sup>1</sup> The -L and -V switches might or might not be set depending on the IT administrator preferences.

## Using variables and name value pairs with HPQLOCFG

In [Script prepared for variables](#) you can see a sample script prepared for use with the -t namevaluepairs switch.

### Example 1 Script prepared for variables (Get\_Asset\_Tag.xml)

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="%user%" PASSWORD="%password%">  
    <SERVER_INFO MODE="read">  
      <GET_ASSET_TAG/>  
    </SERVER_INFO>  
  </LOGIN>  
</RIBCL>
```

To execute this script correctly, use the -t namevaluepairs switch on the command line:

```
hpqlocfg -f get_asset_tag.xml -s <serverip> -t user=Admin,password=pass
```

If the parameter contains multiple words, you must enclose the phrase within double quotes (" "). Up to 25 variables are supported in an XML file. The maximum length of a variable name is 48 characters.

## Example 2 Web agent example (Mod\_SNMP\_IM\_Settings.xml):

---

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_SNMP_IM_SETTINGS>
        <WEB_AGENT_IP_ADDRESS value=%WebAgent%/>
      </MOD_SNMP_IM_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

To execute this script correctly, use the `-t namevaluepairs` switch on the command line:

```
hpqlcfg -s <ipV4 addr> -f <filename> -u <username> -p <password> -t
<web_agent_IP_address>
```

---

- For IPv6, without specifying the port number, invoke the script using:

```
hpqlcfg -s [<ipV6 addr>] -f <filename> -u <username> -p <password>
-t <web_agent_IP_address>
```

or

```
hpqlcfg -s <ipV6 addr> -f <filename> -u <username> -p <password>
-t <web_agent_IP_address>
```

- For IPv6, when specifying the port number, invoke the script using the following:

```
hpqlcfg -s [<ipV6 addr>]:<portnumber> -f <filename> -u <username>
-p <password> -t <web_agent_IP_address>
```

When replacing a token that requires double quotes, use single quotes around the token.

## 3 LOCFG.PL usage

### LOCFG.PL Utility

To use the LOCFG.PL utility, you must have the following PERL modules:

- Net::SSL
- IO::Socket::SSL

You must also have a valid iLO user account and password for each XML script to use LOCFG.PL. To process the request, your account must have the appropriate iLO privileges.

The LOCFG.PL script connects to iLO using an SSL connection.

For example:

```
perl locfg.pl -s {servername|ipaddress}[:port] [-l logfile] -f  
input_filename [-u username -p password] [iLO 4]
```

### LOCFG.PL command line switches

The following command line switches are available to be used with LOCFG.PL:

**Table 3 LOCFG.PL command line switches**

Switch	Effect
-s servername	DNS name of target server. Do not use this switch if launching from HP SIM.
-s ipaddress	IP address of the target server. Do not use this switch if launching from HP SIM.
:port	If a port is not specified, the port defaults to :443.
-l logfile	Name of the file to log all output to. A default file with the server name and IP address is created if this option is not specified. Do not use this switch if launching from HP SIM.
-f input_filename	Filename containing the RIB commands.
-u username <sup>1</sup>	Command line user name. Entering this at the command line overrides the user login name from the script.
-p password <sup>1</sup>	Command line password. Entering this at the command line overrides the password from the script.
-t namevaluepairs	The -t namevaluepairs switch substitutes variables (%variable%) in the input file with values specified in name-value pairs. Separate multiple name-value pairs with a comma.
-i	Enables interactive input of username and password.
-v	Enables verbose message mode. The resulting log file contains all commands sent, all responses received, and any errors. By default, only errors and responses from GET commands are logged without this switch.
iLO 4	Specifies the type of targeted management processor. This flag is optional. Without this flag, LOCFG.PL detects the iLO type automatically. The iLO 4 firmware performs better when this flag is present.

<sup>1</sup> Use -u and -p with caution, because command line options are visible on Linux systems.

For more information, see [“RIBCL XML Scripting Language” \(page 64\)](#).

---

# 4 HPONCFG online configuration utility

## HPONCFG

The HPONCFG utility is an online configuration tool used to set up and configure iLO from within Windows and Linux operating systems without requiring a reboot of the server operating system. HPONCFG 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 provides a limited graphical interface for servers that use Windows operating systems.

## HPONCFG supported operating systems

- HPONCFG Windows (32 and 64 bit)
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 Essentials
- HPONCFG Linux (32 and 64 bit)
  - Red Hat Enterprise Linux 5 Server
  - Red Hat Enterprise Linux 6 Server
  - SUSE Linux Enterprise Server 10
  - SUSE Linux Enterprise Server 11
- VMware
  - VMware 5

## HPONCFG requirements

- Windows-based servers—The following channel interface and core driver installations must be loaded on the server:
  - HP ProLiant iLO 3/4 Channel Interface Driver for Windows
  - HP ProLiant iLO 3/4 Management Controller Driver Package for Windows

The management controller driver package provides server monitoring components and event logging. During execution, HPONCFG issues a warning if it cannot locate the channel interface driver. Each Service Pack for ProLiant (SPP) includes the channel interface driver. The downloads are available from the HP website at: <http://www.hp.com/support/ilo4>.
- Linux-based servers—The HP ProLiant iLO Channel Interface (KMOD/KMP) must be loaded on the server, which includes a health driver package. Each SPP includes the necessary interface and health drivers, and the package is also available from the HP website at: <http://www.hp.com/support/ilo4>.

## Installing HPONCFG

The HPONCFG utility is delivered in separate packages for Windows and Linux operating systems. For Windows operating systems, it is included as a smart component. For Linux operating systems,

it is included as an RPM package file. HPONCFG packages are included in the Service Pack for ProLiant (SPP).

## Windows server installation

HPONCFG installs automatically when the Service Pack for ProLiant is installed. To install HPONCFG manually, run the self-extracting executable.

HPONCFG creates a directory at:

```
%Program files%\HP\hponcfg.
```

## Linux server installation

HPONCFG is installed automatically when Service Pack for ProLiant is installed. Download the HPONCFG RPM package for Linux distributions from the HP website. Install the appropriate package using the RPM installation utility.

For example, for a package installation, install the HPONCFG RPM package on Red Hat Enterprise Linux 5 by entering the following command:

```
rpm -ivh hponcfg-4.0.1-2.linux.rpm
```

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

```
rpm -e hponcfg
```

The `hp-ilo` rpm package and the `hp-health` rpm package must be installed on the system before installing the `hponcfg` rpm package.

After installation, the HPONCFG executable is located in the `/sbin` directory. Be sure that the appropriate Management Interface Driver is installed. For details about where to obtain this driver and file, see “[HPONCFG requirements](#)” (page 24).

## VMware installation

HPONCFG is available for VMware (ESXi 5 only). HPONCFG is included with the HP custom VMware ESXi 5 image. If you have the standard VMware ESXi image, HPONCFG can be downloaded from [www.hp.com](http://www.hp.com) and installed as a VIB with the following command:

```
esxcli software vib install -v <path><filename.vib>
```

For VMware, the `hpilo` driver is already included in the image (either HP custom or standard VMware).

## HPONCFG utility

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 at: <http://www.hp.com/go/ilo>.

Click **iLO Sample Scripts for Windows** or **Lights-Out XML scripting sample for Linux** on the **Resources** tab, under **Support**.

Typical usage is to select a script that is similar to the desired functionality and modify it for your exact requirements. Although no authentication to iLO is required, the XML syntax requires that the `USER_LOGIN` and `PASSWORD` tags are present in the `LOGIN` tag, and that these fields contain data. To successfully execute HPONCFG, the utility must be invoked as Administrator on Windows servers and as root on Linux servers. HPONCFG returns an error message if you do not possess sufficient privileges.

## HPONCFG command line parameters

HPONCFG accepts the following command line parameters:

**Table 4 HPONCFG command line parameters**

Parameter	Effect
/help or ?	Displays the help page
/reset	Resets the iLO to factory default values
/f <i>filename</i>	Sets and receives the iLO configuration from the information given in the XML input file that has name <i>filename</i>
/i <i>filename</i>	Sets and receives iLO configuration from XML input received through the standard input stream
/w <i>filename</i>	Writes the iLO configuration obtained from the device to the XML output file named <i>filename</i>
/a or /all	Capture the complete configuration of iLO to a file. Must be used with /w command line parameter.
/l <i>filename</i>	Logs replies to the text log file that has name <i>filename</i>
/v or /xmlverbose	Display all the responses from iLO.
/s <i>namevaluepairs</i> or /substitute <i>namevaluepairs</i>	Substitutes variables present in the input config file with values specified in <i>namevaluepairs</i>
/get_hostinfo	Receives the host information. Returns the server name and server serial number
/m	Indicates 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	Configures the server for optimized mouse handling to improve graphical remote console performance. By default, it optimizes for remote console single cursor mode for the current user. The <code>dualcursor</code> command line option, along with the <code>mouse</code> option, optimizes mouse handling as suited for remote console dual-cursor mode. The <code>allusers</code> command line option optimizes mouse handling for all users on the system. This option is available only for Windows
/display	Configures Windows display parameters to optimize graphical remote console display performance

These parameters must be preceded by a slash (/) for Windows and Linux as specified in the usage string.

For example:

```
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 Windows, `cmd.exe` is available by selecting **Start**→**Run** and entering `cmd`. HPONCFG displays a usage page if HPONCFG is entered with no parameters. HPONCFG accepts a correctly formatted XML script. HPONCFG sample scripts are included in the HPONCFG package.

For more information about formatting XML scripts, see [“RIBCL XML Scripting Language” \(page 64\)](#).

The command line format is:

```
hponcfg [ /help | /? | /m firmwarelevel | /reset [/m firmwarelevel]
        | /f filename [/l filename][/s namevaluepairs]
        | /w filename [/l filename][/s namevaluepairs]
        | /i [/l filename][/s namevaluepairs]
        | /a | /all
        | /l filename
        | /v | /xmlverbose
        | /m firmwarelevel
        | /mouse
        | /display
```

```

        [/xmlverbose or /v][/m firmwarelevel]
| [/a] /w filename [/m firmwarelevel]
| /get_hostinfo [/m firmwarelevel]
| /mouse [/dualcursor][/allusers]
| /display [/allusers]

```

For more information on using these parameters, see [“HPONCFG command line parameters” \(page 26\)](#).

## Using HPONCFG on Linux servers

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

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] [-s namevaluepairs] [-v] [-m minFw]
hponcfg -i [-l filename] [-s namevaluepairs] [-v] [-m minFw]

```

For more information on using these parameters, see [“HPONCFG command line parameters” \(page 26\)](#).

## Obtaining the basic configuration

Use HPONCFG to obtain a basic configuration from iLO 4 by executing the utility from the command line without specifying an input file. You must provide the name of the output file on the command line.

For example:

```
hponcfg /w config.xml
```

In this example, the utility indicates that it obtained the data successfully and wrote the data to the output file.

The following is an example of a typical output file:

```

<!-- HPONCFG VERSION = "4.2.0.0" -->
<!-- Generated 08/20/13 20:14:12 -->
<RIBCL VERSION="2.1">
  <LOGIN_USER_LOGIN="Administrator" PASSWORD="password">
    <DIR_INFO MODE="write">
      <MOD_DIR_CONFIG>
        <DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
        <DIR_LOCAL_USER_ACCT VALUE = "Y"/>
        <DIR_SERVER_ADDRESS VALUE = ""/>
        <DIR_SERVER_PORT VALUE = "636"/>
        <DIR_OBJECT_DN VALUE = ""/>
        <DIR_OBJECT_PASSWORD VALUE = ""/>
        <DIR_USER_CONTEXT_1 VALUE = ""/>
        <DIR_USER_CONTEXT_2 VALUE = ""/>
        <DIR_USER_CONTEXT_3 VALUE = ""/>
      </MOD_DIR_CONFIG>
    </DIR_INFO>
  <RIB_INFO MODE="write">
    <MOD_NETWORK_SETTINGS>
      <SPEED_AUTOSELECT VALUE = "Y"/>
      <NIC_SPEED VALUE = "10"/>
      <FULL_DUPLEX VALUE = "N"/>
    </MOD_NETWORK_SETTINGS>
  </RIB_INFO>
</RIBCL>

```

```

<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 = "192.168.1.3"/>
<SUBNET_MASK VALUE = "255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE = "192.168.1.1"/>
<DNS_NAME VALUE = "ILODNSNAME"/>
<DOMAIN_NAME VALUE = "hp.com"/>
<PRIM_DNS_SERVER value = "192.168.1.2"/>
<SEC_DNS_SERVER value = "0.0.0.0"/>
<TER_DNS_SERVER value = "0.0.0.0"/>
<PRIM_WINS_SERVER value = "0.0.0.0"/>
<SEC_WINS_SERVER value = "0.0.0.0"/>
<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>
</RIB_INFO>
<USER_INFO MODE="write">
<ADD_USER
  USER_NAME = "admin"
  USER_LOGIN = "admin"
  PASSWORD = "%user_password%"
  <ADMIN_PRIV value = "Y"/>
  <REMOTE_CONS_PRIV value = "Y"/>
  <RESET_SERVER_PRIV value = "Y"/>
  <VIRTUAL_MEDIA_PRIV value = "Y"/>
  <CONFIG_ILO_PRIV value = "Y"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

---

**NOTE:** For security reasons, user passwords are not returned.

---

## Obtaining a specific configuration

Obtain a specific configuration using the appropriate XML input file.

For example, the following is 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`.

```

<GET_GLOBAL_SETTINGS>
<!-- A session timeout value of zero means that the timeout is set to infinite. -->
  <SESSION_TIMEOUT VALUE="0"/>

```

```

<F8_PROMPT_ENABLED VALUE="Y"/>
<F8_LOGIN_REQUIRED VALUE="N"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="17990"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<SNMP_ACCESS_ENABLED VALUE="Y"/>
<SNMP_PORT VALUE="161"/>
<SNMP_TRAP_PORT VALUE="162"/>
<SSH_PORT VALUE="22"/>
<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<VSP_LOG_ENABLE VALUE="N"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<RBSU_POST_IP VALUE="Y"/>
<ENFORCE_AES VALUE="N"/>
<IPMI_DCMI_OVER_LAN_ENABLED VALUE="Y"/>
<REMOTE_SYSLOG_ENABLE VALUE="N"/>
<REMOTE_SYSLOG_PORT VALUE="514"/>
<REMOTE_SYSLOG_SERVER_ADDRESS VALUE=""/>
<ALERTMAIL_ENABLE VALUE="N"/>
<ALERTMAIL_EMAIL_ADDRESS VALUE=""/>
<ALERTMAIL_SENDER_DOMAIN VALUE=""/>
<ALERTMAIL_SMTP_PORT VALUE="25"/>
<ALERTMAIL_SMTP_SERVER VALUE=""/>
<PROPAGATE_TIME_TO_HOST VALUE="Y"/>
</GET_GLOBAL_SETTINGS>

```

## Setting a configuration

Set a specific configuration by using the command format:

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

In this example, the input file has contents:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
<ADD_USER
USER_NAME="Landy9"
USER_LOGIN="mandy8"
PASSWORD="floppyshoes">
<ADMIN_PRIV value ="No"/>
<REMOTE_CONS_PRIV value ="Yes"/>
<RESET_SERVER_PRIV value ="No"/>
<VIRTUAL_MEDIA_PRIV value ="No"/>
<CONFIG_ILO_PRIV value="Yes"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

The specified user is added to the device.

## Using variable substitution

HPONCFG enables you to specify variables in the XML RIBCL script and to assign values to those variables when you run HPONCFG. This feature helps to avoid rewriting the XML script file every time with different values. Anything enclosed by two percent sign (%) characters in the XML file is considered a variable.

In this example, %username%, %loginname%, and %password% are variables:

```

<!-- 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="%username%" USER_LOGIN="%loginname%" PASSWORD="%password%">
<RESET_SERVER_PRIV value="Y" />
<ADMIN_PRIV value="Y" />
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

Specify values for the variables when you run HPONCFG by using the substitute option. The argument must be a string or variable name and value pairs must be separated by a comma (,). The variable name and its value must be separated by an equal sign (=). For example:

```
hponcfg /f add_user.xml /s username=testuser,loginname=testlogin,password=testpasswd
```

In this example, %host\_power% is a variable:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<SERVER_INFO MODE="write">
<!-- Modify the HOST_POWER attribute to toggle power on the host server -->
<!-- HOST_POWER="No" (Turns host server power off) -->
<!-- A graceful shutdown will be attempted for ACPI-aware -->
<!-- operating systems configured to support graceful shutdown. -->
<!-- HOST_POWER="Yes" (Turns host server power on) -->
<SET_HOST_POWER HOST_POWER="%host_power%"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>

```

- To power the system on, enter:  
hponcfg /f Set\_Host\_Power.xml /s host\_power=YES
- To power the system off, enter:  
hponcfg /f Set\_Host\_Power.xml /s host\_power=NO

## Capturing and restoring a configuration

Use HPONCFG to capture basic configuration information in an XML readable file format. Use this file to set or restore the iLO configuration. This feature is available with HPONCFG version 1.2 and later. HPONCFG writes the configuration information in the HP RIBCL format.

- To capture a configuration, you must specify the name and location of the output file on the command line. See [“Obtaining the basic configuration” \(page 27\)](#) for details.

For example:

```
hponcfg /w config.xml
```

HPONCFG displays a message when it successfully writes the configuration information to the output file as requested. For security reasons, the default user administrator and user passwords are not captured in the configuration file or returned in the response. A variable is provided in its place to use with the substitute option to provide a default password for all users when restoring a configuration. Manually change the password before using the file to restore the configuration.

- To restore a configuration, the file must be sent to HPONCFG as input using the /f or -f option. Add a default password for all users using the substitute or s option.

For example:

```
hponcfg /f config.xml /s user_password=password
```

---

## 5 SMASH CLP usage

### SMASH CLP

The DMTF SMASH initiative is a suite of specifications that deliver architectural semantics, industry standard protocols and profiles to unify the management of the data center. The SMASH CLP specification enables simple and intuitive management of heterogeneous servers in the data center.

For more information, see [“SMASH CLP Scripting Language” \(page 35\)](#).

---

## 6 IPMI usage

### The IPMI utility

Use the Linux IPMI tool and Windows IPMI util applications to test the IPMI interfaces on server platforms. The Linux IPMI tool is used in environments where scripting is used as the base for platform monitoring.

The Windows IPMI util has a dependency on the IPMI driver if using "in-band" (or from a command prompt). The Windows IPMI driver is delivered in Windows Server 2008 R2. IPMI support might be available in later updates of Windows Server 2003 R2.

The Linux IPMI tool also requires the IPMI drivers (delivered in the distribution) to be enabled if utilized in-band. The IPMI device drivers are not typically enabled to automatically start when the Linux operating system is started. If you are logged on to a Linux console (command prompt) as a root user, use the following command to initiate the IPMI device drivers for Linux:

```
service ipmi start
```

For more information, see the documentation provided by the specific Linux distribution.

The IPMI tool supports remote IPMI protocols that provide the capability to power the server on and off, and to remotely monitor the platform. The iLO firmware supports the IPMI 2.0 RMCP+ protocol for the highest level of authentication, encryption and integrity. The legacy IPMI 1.5 IPMI over LAN protocol is not supported.

### Basic IPMI tool usage

The Linux IPMI tool is fully documented in the Linux MAN page. The `man ipmitool` command provides extended documentation beyond the scope of this guide. To use IPMI tool from the Linux operating system to locally monitor a system, the IPMI drivers must be enabled. Typical in-band commands include the following.

- To retrieve the iLO status, enter:  
`# ipmitool mc info`
- To retrieve the status of iLO monitored sensors, enter:  
`# ipmitool sensor list`
- To retrieve the contents of the IPMI SEL, enter:  
`# ipmitool sel list`

### Advanced IPMI tool usage on Linux

The Linux IPMI tool has the capability to securely communicate with iLO using the IPMI 2.0 RMCP+ protocol. This is the `ipmitool lanplus` protocol feature. For most commands, a valid iLO user name and password is required. Typical out-of-band (or IPMI over LAN) commands include the following.

- To retrieve the general iLO status, enter:  
`# ipmitool -H IP Address or FQDN -I lanplus -U user name mc info`
- To power on the HP ProLiant Server, enter:  
`# ipmitool -H IP Address or FQDN -I lanplus -U user name chassis power on`
- To turn on the HP ProLiant Server UID, enter:  
`# ipmitool -H IP Address or FQDN -I lanplus -U user name chassis identify on`

Most Linux IPMI tool commands can be issued remotely, including retrieving the IML entries and current sensor readings. The following parameter is required to enable the IPMI 2.0 RMCP+ protocol:

```
-l lanplus
```

## Advanced IPMIutil usage on Windows

Use the Windows `IPMIutil.exe` application for remote IPMI access to iLO. The commands, although different, provide similar functionality.

- To retrieve the general status of iLO, enter:

```
C:\> ipmiutil.exe health -N IP Address -J 3 -U user name -P Password
```

- To power the HP ProLiant server on, enter:

```
C:\> ipmiutil.exe reset -u -N IP Address -J 3 -U user name -P Password
```

- To power the HP ProLiant server off, enter:

```
C:\> ipmiutil.exe reset -d -N IP Address -J 3 -U user name -P Password
```

- To turn on the HP ProLiant server UID, enter:

```
C:\> ipmiutil.exe led -i5 -N IP Address -J 3 -U user name -P Password
```

---

**NOTE:** The IPMIutil application only enables turning on the UID for five seconds. To keep the UID light on persistently, script the command in a loop with a four second delay.

---

---

# 7 SMASH CLP Scripting Language

## SMASH CLP command line overview

SMASH CLP provides a standardized set of commands for the configuration and control of management processors (called Management Access Points) and host systems. On iLO, SMASH CLP is accessed through the SSH port.

## SMASH CLP command line access

The iLO 4 firmware features enable you to execute the supported commands from a SMASH CLP command line. Access the command line option from the one of the following interfaces:

- A serial port using one connection
- A network using SSH. This enables three simultaneous connections (an IP address or DNS name, login name, and password are required to start a session using SSH)

Five network connections can be active simultaneously. After the serial CLI is enabled on the Global Settings screen, access the iLO CLI by entering:

```
ESC (
```

The SSH session starts after authentication.

## Using the command line

After initiating a command line session, the iLO CLI prompt appears. Each time you execute a command (or you exit the Remote Console or VSP), you return to the CLI prompt as shown in the following example:

```
hpiLO->
```

Each time a CLI command executes, the returned output follows this general format:

```
hpiLO-> CLI command
status=0
status_tag=COMMAND COMPLETED
... output returned...
hpiLO->
```

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

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

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

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

The privilege level of the logged in user is verified against the privilege required for the command. The command is only executed if the privilege levels match. If the serial command line session

status is set to `Enabled-No Authentication`, then all the commands are executed without verifying the privilege level.

The general syntax of a CLP command is:

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

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

The valid Boolean values for any command are `yes`, `no`, `true`, `false`, `y`, `n`, `t`, `f`, `1`, and `0`.

---

**NOTE:** If a CLP command spans more than one line, you cannot navigate between different lines.

---

In the Windows PuTTY client, map the Backspace key to a value of `0x8` by changing the setting for Terminal Keyboard to **Ctrl+H**.

## Escape commands

The escape key commands are shortcuts to popular tasks.

<code>ESC R</code>	<code>ESC r</code>	<code>ESC R</code>	Resets the system.
<code>ESC ^</code>			Powers on the system.

ESC ESC

Erases the current line.

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

## Base commands

Following are the base commands for use on the command line:

`help` Displays context-sensitive help and all supported commands

`command help/?` Displays the help message specific to that command

`exit` Terminates the CLP session

`cd` The command sets the current default target. The context works like a directory path. The root context for the server is a forward slash (/) and is the starting point for a CLP system. Shorten commands by changing the context.

For example, to find the current iLO firmware version, enter the following command:

```
show /map1/firmware1
```

`show` The command displays values of a property or contents of a collection target.

For example:

```
hpiLO-> show
status=0
status_tag=COMMAND COMPLETED
/
Targets
system1
map1
Properties
Verbs
cd version exit show
```

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

Specify the `show` command with an explicit or implicit context as well as a specific property. For example, an explicit context is `/map1/firmware1` and is not dependent on the current context, while an implicit context assumes that the context specified is a child of the current context. If the current context is `/map1` then a `show firmware` command displays the `/map1/firmware1` data.

If you do not specify a property, then all properties are shown. In the case of the `/map1/firmware1` context, two properties are available: `version`, and `date`. If you execute `show /map1/firmware1 date`, only the date is shown.

`create` Creates a new instance of the MAP in the name space.

`delete` Removes instances of the MAP in the name space.

`load` Moves a binary image from a URL to the MAP.

`reset` Causes a target to cycle from enabled to disabled, and back to enabled.

set	Sets a property or set of properties to a specific value, and resets iLO to implement the changes.
start	Causes a target to change the state to a higher run level.
stop	Causes a target to change the state to a lower run level.
version	The command queries the version of the CLP implementation or other CLP elements. For example:  <pre>hpiLO-&gt; version status=0 status_tag=COMMAND COMPLETED SM-CLP Version 1.0</pre>
oemhp_ping	The command determines if an IP address is reachable from the current iLO session. For example:  <pre>oemhp_ping 192.168.1.1</pre> Where 192.168.1.1 is the IP address you are testing.

## Specific commands

The following sections cover iLO 4-specific commands available when using the command line, including:

- [“User commands” \(page 38\)](#)
- [“HP SSO settings” \(page 39\)](#)
- [“Network commands” \(page 41\)](#)
- [“iLO 4 settings” \(page 44\)](#)
- [“iLO 4 embedded health settings” \(page 45\)](#)
- [“SNMP settings” \(page 47\)](#)
- [“License commands” \(page 49\)](#)
- [“Directory commands” \(page 49\)](#)
- [“Virtual Media commands” \(page 51\)](#)
- [“Start and Reset commands” \(page 53\)](#)
- [“Firmware commands” \(page 54\)](#)
- [“Eventlog commands” \(page 55\)](#)
- [“Blade commands” \(page 56\)](#)
- [“Boot commands” \(page 56\)](#)
- [“LED commands” \(page 59\)](#)
- [“System properties and targets” \(page 60\)](#)
- [“Other commands” \(page 63\)](#)

## User commands

User commands enable you to view and modify user settings. [Table 5 \(page 39\)](#) shows the User Command properties. User settings are located at:

```
/map1/accounts1.
```

## Targets

All local users are valid targets. For example, if three local users have the login names Administrator, admin, and test, then valid targets are:

- Administrator
- admin
- test

**Table 5 User Command Properties**

Property	Access	Description
username	read/write	Corresponds to the iLO 4 login name.
password	read/write	Corresponds to the password for the current user.
name	read/write	Displays the name of the user. If a name is not specified, the parameter uses the same value as the login name (username). This value corresponds to the iLO 4 user name property.
group	read/write	Specifies the privilege level. The valid values are as follows: <ul style="list-style-type: none"><li>• admin</li><li>• config</li><li>• oemhp_power</li><li>• oemhp_rc</li><li>• oemhp_vm</li></ul> If you do not specify a group, no privileges are assigned to the user.

### For example

The current path is:

/map1/accounts1.

- `create username=lname1 password=password`  
In this example, username corresponds to the login name.
- `create /map1/accounts1 username=<lname1> password=<pwd12345> name=<dname1> group=<admin,config,oemhp_vm,oemhp_rc,oemhp_power>`  
In this example, lname1 is the login name of the user.

## HP SSO settings

HP SSO settings commands are accessed using:

/map1/oemhp\_ssocfg1.

You must have the Configure iLO Settings privilege to change these properties. SSO is only supported for browser access from trusted HP SIM servers. SSO is a licensed feature. [Table 6 \(page 40\)](#) shows the HP SSO properties. For more information, see the *HP iLO User Guide* on the HP website at <http://www.hp.com/go/ilo/docs>.

### Targets

None

**Table 6 HP SSO Properties**

Property	Access	Description
oemhp_ssotrust	Read/write	The Single Sign-On required trust level. Valid values are: <ul style="list-style-type: none"> <li>• disabled</li> <li>• all</li> <li>• name</li> <li>• certificate</li> </ul>
oemhp_ssouser	Read/write	The privileges associated with the user role. Valid values are: <ul style="list-style-type: none"> <li>• login</li> <li>• oemhp_rc</li> <li>• oemhp_power</li> <li>• oemhp_vm</li> <li>• config</li> <li>• admin</li> </ul>
oemhp_ssooperator	Read/write	The privileges associated with the operator role. Valid values are: <ul style="list-style-type: none"> <li>• login</li> <li>• oemhp_rc</li> <li>• oemhp_power</li> <li>• oemhp_vm</li> <li>• config</li> <li>• admin</li> </ul>
oemhp_ssoadministrator	Read/write	The privileges associated with the administrator role. Valid values are: <ul style="list-style-type: none"> <li>• login</li> <li>• oemhp_rc</li> <li>• oemhp_power</li> <li>• oemhp_vm</li> <li>• config</li> <li>• admin</li> </ul>
oemhp_ssoserver	Read	Contains 0 or more HP SIM Trusted Server records. Each record contains a server name or a server certificate.

**For example**

- To set the SSO trust level to trust by certificate:

```
</>hpiLO-> set /map1/oemhp_ssocfg1 oemhp_ssotrust=certificate
```
- To assign user roles the Login privilege:

```
</>hpiLO-> set /map1/oemhp_ssocfg1 oemhp_ssouser=login
```
- To assign the operator role Login, Remote Console, Virtual Power and Reset, and Virtual Media privileges:

```
</>hpiLO-> set /map1/oemhp_ssocfg1
oemhp_ssooperator=login,oemhp_rc,oemhp_power,oemhp_vm
```
- To Add an HP SIM Trusted Server name record:

```
</>hpiLO-> cd map1/oemhp_ssocfg1
</map1/oemhp_ssocfg1>hpiLO-> create hpsim1.corp.net
```

- To load an SSO certificate from an HP SIM 7.0 server or later:  

```
</map1/oemhp_ssocfg1>hpiLO-> load http://<HP SIM name or network address>:280/GetCertificate?certtype=sso
```

 Or:  

```
</map1/oemhp_ssocfg1>hpiLO-> load https://<HP SIM name or network address>:50000/GetCertificate?certtype=sso
```
- To delete oemhp\_ssoserver with index 5:  

```
</map1/oemhp_ssocfg1>hpiLO-> delete 5
```
- To display the complete iLO SSO configuration:  

```
</>hpiLO-> cd map1/oemhp_ssocfg1  
</map1/oemhp_ssocfg1>hpiLO->show
```

## Network commands

The network subsystems are located at:

- /map1/enetport1
- /map1/dhccpendpt1
- /map1/dnsendpt1
- /map1/gateway1
- /map1/dnsserver1
- /map1/dnsserver2
- /map1/dnsserver3
- /map1/settings1
- /map1/vlan1

Properties, Targets, and Verbs:

- enetport1
  - Targets
    - lanendpt1
  - Properties
    - EnabledState
    - OtherTypeDescription
    - Autosense
    - PermanentAddress
    - LinkTechnology
    - Speed
    - SystemName
    - Fullduplex

## Verbs

- cd
- version
- exit
- show
- set

### **For example**

```
set /map1/enetport1 Speed=100
```

```
set /map1/enetport1/lanendpt1/ipendpt1 IPv4Address=15.255.102.245  
SubnetMask=255.255.248.0
```

- dhcpendpt1

#### Properties

- EnabledState
- OtherTypeDescription

- dnsendpt1

#### Properties

- EnabledState
- HostName
- DomainName
- OtherTypeDescription

- gateway1

#### Properties

- AccessInfo
- AccessContext

- dnsserver1

#### Properties

- AccessInfo
- AccessContext

## Verbs

- cd
- version
- exit
- show
- set

- dnsserver2
  - Properties
    - AccessInfo
    - AccessContext
- dnsserver3
  - Properties
    - AccessInfo
    - AccessContext
- settings1
  - Targets
    - DNSSettings1
      - Properties
        - DNSServerAddress
        - RegisterThisConnection
        - DomainName
        - DHCPOptionToUse
      - WINSSettingData1
        - Properties
          - WINSServerAddress
          - RegisterThisConnection
          - DHCPOptionToUse
    - Verbs
      - cd
      - version
      - exit
      - show
  - StaticIPSettings1
    - Properties
      - oemhp\_SRoute1Address
      - oemhp\_Mask1Address
      - oemhp\_Gateway1Address
      - oemhp\_SRoute2Address
      - oemhp\_Mask2Address
      - oemhp\_Gateway2Address
      - oemhp\_SRoute3Address
      - oemhp\_Mask3Address

- oemhp\_Gateway3Address
- DHCPOptionToUse

Specify one or more properties on the command line. If multiple properties are on the same command line, they must be separated by a space.

The iLO firmware resets after the network settings have been applied.

For example, the following command sets the iLO network port to the shared network port NIC on the server motherboard. This NIC is referred to as the LOM elsewhere in iLO documentation. Not all servers have this hardware.

```
Set /map1/enetport1/lanendpt1 EnabledState=32768
```

The following example sets the iLO network port to the optional shared network port NIC that can be plugged into the server in the FlexibleLOM slot on the server motherboard. This slot is not a standard PCI slot, but is a special horizontal connector in the back right hand corner of the motherboard. Not all servers have this slot, or the NIC that plugs into this slot.

```
Set /map1/enetport1/lanendpt1 EnabledState=32769
```

## iLO 4 settings

The iLO 4 settings commands enable you to view or modify iLO 4 settings. [Table 7 \(page 44\)](#) shows the iLO 4 properties. The iLO 4 settings are located at:

```
/map1/config1
```

### Targets

No targets

### Properties

**Table 7 iLO Properties**

Property	Access	Description
oemhp_mapenable	Read/Write	Enables or disables iLO. Boolean values are accepted.
oemhp_timeout	Read/Write	Sets session timeout in minutes. Valid values are 15, 30, 60, and 120.
oemhp_rbsuenable	Read/Write	Enables or disables RBSU prompt during POST. Boolean values are accepted.
oemhp_rbsulogin	Read/Write	Enables or disables login requirement for accessing RBSU. Boolean values are accepted.
oemhp_rbsushowip	Read/Write	Enables or disables iLO IP address display during POST. Boolean values are accepted.
oemhp_vsp_log_enable	Read/Write	Enables or disables capture of virtual serial port output from the server.
oemhp_rconfig	Read/Write	Sets the Remote Console configuration. Valid values are enabled, disabled, or automatic.
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_sshport	Read/Write	Sets the SSH port value.
oemhp_sshstatus	Read/Write	Enables or disables SSH. Boolean values are accepted.

**Table 7 iLO Properties** *(continued)*

Property	Access	Description
oemhp_serialclistatus	Read/Write	Enables or disables CLP session through serial port. Boolean values are accepted.
oemhp_serialcliauth	Read/Write	Enables or disables authorization requirement for CLP session through serial port. Boolean values are 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_enforce_aes	Read/Write	Enable or disable enforcing AES/3DES encryption. <b>NOTE:</b> When enabling AES/3DES, manually close all other GUI, XML, and CLI connections since remaining sessions may continue to use the non-AES/3DES cipher.
oemhp_authfailurelogging	Read/Write	Sets the logging criteria for failed authentications.
oemhp_computer_lock	Read/Write	Enables or disables the Remote Console Computer Lock.

**Verbs**

- cd
- version
- exit
- show
- set
- oemhp\_loadSSHkey
- oemhp\_resetHotkeys

**For example**

```
set /map1/config1 oemhp_mapenable=yes oemhp_timeout=30
```

Specify one or more properties in the command line. If multiple properties are on the same command line, they must be separated by a space.

For example:

```
set /map1/config1 oemhp_computer_lock=windows
set /map1/config1 oemhp_computer_lock=custom,l_gui,l
set /map1/config1 oemhp_computer_lock=disabled
```

For a complete list of oemhp\_computer\_lock custom keys, see the *HP iLO User Guide* on the HP website at: <http://www.hp.com/go/ilo/docs>. Keys with a space must have the space replaced with an underscore.

For example:

```
set /map1/config1 oemhp_computer_lock=custom,SYS_RQ
```

**iLO 4 embedded health settings**

iLO 4 embedded health commands enable you to display system embedded health information for fans, temperature sensors, voltage sensors, and power supplies. [Table 8 \(page 46\)](#) shows the iLO 4 Embedded Health properties.

The iLO 4 embedded health CLP settings are:

- /system1/fan\*
- /system1/sensor\*
- /system1/powersupply\*

### Targets

- Fan
- Sensor
- Powersupply

**Table 8 Embedded Health Properties**

Property	Access	Description
DeviceID	Read	Displays fan, sensor, or power supply label number
ElementName	Read	Displays fan, sensor, or power supply location
OperationalStatus	Read	Displays fan, sensor, or power supply operational status
VariableSpeed	Read	Displays if fan is operating at variable speed
DesiredSpeed	Read	Displays the current fan speed
HealthState	Read	Displays the health status of the fan, sensor, or power supply
RateUnits	Read	Displays the reading units for temperature and voltage sensors
CurrentReading	Read	Displays the current reading of sensor
SensorType	Read	Displays the sensor type
Oemhp_CautionValue	Read	Displays temperature sensor caution value
Oemhp_CriticalValue	Read	Displays temperature sensor critical value

**NOTE:** All available embedded health properties from all targets are shown in [Table 8 \(page 46\)](#). The actual properties returned depend on the command.

### For example

The following command displays the system fan1 properties:

```
show system1/fan1
```

For example:

```
/system1/fan1
Targets
Properties
DeviceID=Fan 1
ElementName=I/O Board
OperationalStatus=Ok
VariableSpeed=Yes
DesiredSpeed=40
HealthState=Ok
```

VRM power supplies are usually mapped to the sensor targets. The following command displays the VRM 1 properties:

```
show system1/sensor1
```

For example:

```

/system1/sensor1
Targets
Properties
DeviceID=VRM 1
ElementName=CPU 1
OperationalStatus=Ok
RateUnits=Volts
CurrentReading=0
SensorType=Voltage
HealthState=Ok
oemhp_CautionValue=0
oemhp_CriticalValue=0

```

Other sensor targets show system temperatures. The following command displays one of the temperature zone properties:

```
show system1/sensor3
```

For example:

```

/system1/sensor3
Targets
Properties
DeviceID=Temp 1
ElementName=I/O Board Zone
OperationalStatus=Ok
RateUnits=Celsius
CurrentReading=32
SensorType=Temperature
HealthState=Ok
oemhp_CautionValue=68
oemhp_CriticalValue=73

```

## SNMP settings

SNMP settings commands enable you to view and modify SNMP settings. [Table 9 \(page 47\)](#) shows the SNMP command properties. SNMP settings are available at:

```
/map1/snmp1
```

### Targets

None

### Properties

**Table 9 SNMP Command Properties**

Property	Access	Description
accessinfo<n>	Read/Write	Sets the SNMP trap destination address, where <n> is 1, 2, or 3.
readcom<n>	Read/Write	Displays or modifies SNMP read community address for when Agentless Management is enabled, where <n> is 1, 2, or 3.
trapcom<n>	Read/Write	Displays or modifies SNMP trap community address, where <n> is 1, 2, or 3.
oemhp_iloalert	Read/Write	Enables or disables iLO SNMP alerts. Boolean values accepted.
oemhp_agentalert	Read/Write	Enables or disables host agent SNMP alerts. Boolean values accepted.
oemhp_snmpassthru	Read/Write	Enables or disables iLO SNMP pass-through. Boolean values accepted.
oemhp_imagenturl	Read/Write	Sets the Insight Manager Agent URL.

**Table 9 SNMP Command Properties** *(continued)*

Property	Access	Description
oemhp_imdatalevel	Read/Write	Determines if the LOM device responds to anonymous XML queries. Enable or disable valid selections.
oemhp_agentlessenable	Read/Write	Displays or modifies the SNMP Agentless Management. Valid values are 'yes', or 'no'. If Agentless Management is disabled, SNMP passthru will be enabled.
oemhp_systemlocation	Read/Write	Displays or modifies SNMP System Location for when Agentless Management is enabled.
oemhp_systemcontact	Read/Write	Displays or modifies SNMP System Contact for when Agentless Management is enabled.
oemhp_systemrole	Read/Write	Displays or modifies SNMP System Role information for when Agentless Management is enabled.
oemhp_systemroledetail<n>	Read/Write	Displays or modifies SNMP System Role detail for when Agentless Management is enabled, where <n> can be from 1 to 5. The property value is limited to 512 characters total for all five SNMP System Role details. For oemhp_systemroledetail1 to 4, the value is limited to 100 characters, but oemhp_systemroledetail5 is limited to 112 characters. For multi-line values, spaces are added to previous lines to meet the 100 character limit if a subsequent line has information provided.
oemhp_coldstarttrap	Read/Write	Displays or modifies the SNMP Cold Start Trap Broadcast. Valid values are <b>yes</b> , or <b>no</b> .
oemhp_trapsource	Read/Write	Displays or modifies the SNMP trap source setting. Valid values are <b>ilo</b> , or <b>os</b> .

- Verbs
  - cd
  - version
  - exit
  - show
  - set

**For example**

The following commands set various SNMP properties:

- `set /map1/snmp1 accessinfo1=192.168.0.50 oemhp_imdatalevel=Enabled`
- `set readcom1="public1"`
- `set trapcom1="trapcomm1"`
- `set oemhp_systemlocation="HP Data Center, Hockley, TX"`
- `set oemhp_systemcontact="Mr. System Administrator"`
- `set oemhp_systemrole="Brief Role Description [60 characters]"`
- `set oemhp_systemroledetail1="Extended role description [100 characters]"`
- Showing multiple lines for oemhp\_systemroledetail:
  - `set oemhp_systemroledetail2="Extended role description"`
  - `show` - Existing string in detail1 has spaces added to meet 100 char limit.

Specify one or more properties on the command line. If multiple properties are on the same command line, they must be separated by a space.

## License commands

License commands enable you to display and modify the iLO license. [Table 10 \(page 49\)](#) shows the License command properties. License commands are available at:

/map1/

### Targets

None

### Commands

**Table 10 License Commands**

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

### For example

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

## Directory commands

Directory commands enable you to view and modify directory settings. [Table 12 \(page 50\)](#) shows the Directory command properties. Directory command settings are available at:

/map1/oemhp\_dircfg1

### Targets

The Directory Command Targets are shown in [Table 11 \(page 49\)](#).

**Table 11 Directory Command Targets**

Target	Description
/map1/oemhp_dircfg1/ oemhp_keytab1	Contains a load verb used to load the binary keytab file from a given URL. The keytab file may be up to 1024 bytes in length.

### Properties

**Table 12 Directory Command Properties**

Property	Access	Description
oemhp_dirauth	Read/Write	Enables or disables directory authentication. Valid settings are as follows: <ul style="list-style-type: none"> <li>extended_schema Uses HP extended schema</li> <li>default_schema Uses schema-free directories</li> <li>disabled Directory-based authentication is disabled</li> </ul>
oemhp_localacct	Read/Write	Enables or disables local account authentication. This property 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_ldappport	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.
oemhp_usercntxt1, 2 ... (up to 15)	Read/Write	Displays the directory user login search context. This field is not necessary when the schema-free directory configuration is used.
oemhp_group(n)_name where n = 1..6	Read/Write	Displays security group distinguished name. Used within the schema-free directory configuration only.
oemhp_group(n)_priv where n = 1..6	Read/Write	The privileges associated with a group. Valid values are: <ul style="list-style-type: none"> <li>login</li> <li>oemhp_rc</li> <li>oemhp_power</li> <li>oemhp_vm</li> <li>config</li> <li>admin</li> </ul>
oemhp_dir_kerberos_enabled	Read/Write	Enables or disables Kerberos authentication. Boolean values are accepted.
oemhp_dir_kerberos_kdc_port	Read/Write	Specifies the port number used to connect to the domain controller. The Kerberos port number is 88, but the domain controller can be configured for a different port number.
oemhp_dir_kerberos_kdc_address	Read/Write	The location of the domain controller. The domain controller location is specified as an IP address or DNS name.
oemhp_dir_kerberos_realm	Read/Write	Specifies the Kerberos realm for which the domain controller is configured. By convention, the Kerberos realm name for a given domain is the domain name converted to uppercase.

**For example**

- `set /map1/oemhp_dircfg1`
- `set /map1/oemhp_dircfg1 oemhp_dirauth=default_schema  
oemhp_dirsrvaddr=adserv.demo.com`

Define additional groups using additional `set` commands.

Specify one or more properties on the command line. If multiple properties are on the same command line, they must be separated by a space.

## Virtual Media commands

Access to the iLO virtual media is supported through the CLP. [Table 13 \(page 51\)](#) shows the Virtual Media command targets. [Table 14 \(page 51\)](#) shows the Virtual Media command properties. The virtual media subsystem is located at:

```
/map1/oemhp_vm1.
```

For more information, see the *HP iLO User Guide* on the HP website at: <http://www.hp.com/go/ilo/docs>.

### Targets

The virtual media targets are shown in [Table 13 \(page 51\)](#).

**Table 13 Virtual Media Command Targets**

Target	Description
/map1/oemhp_vm1/floppydr1	Virtual floppy or key drive device
/map1/oemhp_vm1/cddr1	Virtual CD-ROM device

**Table 14 Virtual Media Command 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"><li>• Never Do not boot from the device. The value appears as <code>No_Boot</code>.</li><li>• Once Boot from the device only once. The value appears as <code>Once</code>.</li><li>• Always Boot from the device each time the server is rebooted. The value is displayed as <code>Always</code>.</li><li>• Connect Connect the virtual media device. Sets <code>oemhp_connect</code> to <code>Yes</code> and <code>oemhp_boot</code> to <code>Always</code>.</li><li>• Disconnect Disconnects the virtual media device and sets the <code>oemhp_boot</code> to <code>No_Boot</code>.</li></ul>
oemhp_wp	Read/Write	Enables or disables the write-protect flag. Boolean values accepted.
oemhp_vmapplet	Read	Displays if an iLO 4 virtual media device is connected via IRC or Java IRC.

### Image URL

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

URL example:

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

- `protocol`—Mandatory field that must be HTTP or HTTPS
- `username:password`—Optional field

- hostname—Mandatory field
- port—Optional field
- filename—Mandatory field

The CLP performs only a cursory syntax verification of the URL value. You must visually verify that the URL is valid.

### For example

- `set oemhp_image=http://imgserver.company.com/image/dosboot.bin`
- `set oemhp_image=http://john:abc123@imgserver.company.com/VMimage/installDisk.iso`

### Tasks

- To insert a floppy USB key image into the Virtual Floppy/USBKey, enter:

```
cd /map1/oemhp_vm1/floppydr1
show
set oemhp_image=http://my.imageserver.com/floppyimg.bin
set oemhp_boot=connect
show
```

This example executes the following commands:

- Changes the current context to the floppy or key drive
- Shows the current status to verify that the media is not in use
- Inserts the desired image into the drive
- Connects the media. The boot setting always connects automatically
- To eject a floppy or USB key image from the Virtual Floppy/USBKey, enter:

```
cd /map1/oemhp_vm1/floppydr1
set oemhp_boot=disconnect
```

This example executes the following commands:

- Changes the current context to the floppy or key drive
- Issues the disconnect command that disconnects the media and clears the `oemhp_image`
- To insert a CD-ROM image into the virtual CD-ROM, enter:

```
cd /map1/oemhp_vm1/cddr1
show
set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
set oemhp_boot=connect
show
```

This example executes the following commands:

- Changes the current context to the CD-ROM drive
- Shows the current status to verify that the media is not in use
- Inserts the desired image into the drive
- Connects the media. The boot setting always connects automatically

- To eject a CD-ROM image from the Virtual CD-ROM, enter:

```
cd /map1/oemhp_vm1/cddr1
set oemhp_boot=disconnect
```

This example executes the following commands:

- Changes the current context to the CD-ROM drive
  - Issues the disconnect command that disconnects the media and clears the `oemhp_image`
- To insert a CD-ROM image and set for single boot, enter:

```
cd /map1/oemhp_vm1/cddr1
set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
set oemhp_boot=connect
set oemhp_boot=once
show
```

This example executes the following commands:

- Changes the current context to the CD-ROM drive
  - Shows the current status to verify that the media is not in use
  - Inserts the desired image into the drive
  - Connects the media. The boot setting always connects automatically
  - Overrides the boot setting to Once
- To eject a CD-ROM image from the virtual CD-ROM in a single command, enter:  
`set /map1/oemhp_vm1/cddr1 oemhp_boot=disconnect`  
 If you attempt to disconnect when the drive is not connected, you receive an error.

## Start and Reset commands

Start and reset commands enable you to power on and reboot the server containing iLO 4 or iLO 4 itself. [Table 15 \(page 53\)](#) shows the Start and Reset command properties.

**Table 15 Start and Reset Commands**

Command	Description
<code>start</code>	Turns server power on
<code>stop</code>	Turns server power off
<code>reset hard</code>	Power cycles the server
<code>reset soft</code>	Warm boots the server

**Table 16 Manual Reset Command**

Property	Access	Description
<code>manual_iLO_reset</code>	Read/Write	Allows a delay to iLO resets, which is useful when changing multiple properties. Valid values are <b>yes</b> (enabled) or <b>no</b> (disabled). When enabled, the iLO will reset only when a user logs out, is disconnected from iLO, or issues a 'reset/map1' command.

**For example**

The following commands are supported if the current target is:

```
/system1
```

- start
- stop

The following commands are supported if the current target is:

```
/map1
```

- reset

Set the status of the manual\_iLO\_reset property using the following commands:

- set /map1/ manual\_ilo\_reset=yes
- set /map1/ manual\_ilo\_reset=no

## Firmware commands

Firmware commands enable you to display and modify the iLO 4 firmware version. [Table 17 \(page 54\)](#) shows the Firmware Update properties. Firmware settings are available at:

```
/map1/firmware1
```

### Targets

No targets

**Table 17 Firmware Update Properties**

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

### Command format

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

where *URL* is the URL of a firmware update image file on a web server. The URL is limited to 80 characters.

URL example:

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

- protocol—Mandatory field that must be HTTP or HTTPS.
- username:password—Optional field
- hostname—Mandatory field
- port—Optional field
- filename—Mandatory field

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

### For example

```
load -source http://imgserver.company.com/firmware/iloFWimage.bin
```

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

```
load /map1/firmware1 -source  
http://imgserver.company.com/firmware/iloFWimage.bin
```

The [target] field is:

```
/map1/firmware1—This field is optional if it is already the current target.
```

---

**NOTE:** Firmware components loaded will be flashed onto the system, replacing the existing versions. If the firmware flash was successful, then the status\_tag of COMMAND COMPLETED will be shown. If iLO firmware was flashed, then a reset of iLO will occur.

If a Trusted Platform Module (TPM) is installed and enabled the load command must include the '-TPM\_force' option after the URL. Otherwise the command will fail.

---

- ❗ **IMPORTANT:** If a TPM is enabled, then upgrading without performing the proper OS encryption procedure will result in loss of access to your data. If you do not have your recovery key or have not suspended BitLocker do not flash iLO.
- 

## Non-iLO firmware commands

Non-iLO firmware commands support system firmware updates, available at:

```
/system1/swid<N>
```

Where <N> is either a number or a wildcard (\*). Use a wildcard to show every firmware version installed on the system (including iLO) and identify the software ID number of the firmware you want to load.

To display (show) information about the firmware entities installed on the system:

```
</system1>hpiLO-> show swid*
status=0
  status_tag=COMMAND COMPLETED
  Mon Aug 12 16:13:54 2013

  /system1/swid1
    Targets
    Properties
      name=HP ProLiant System ROM
      VersionString=09/01/2013
      oemhp_VersionStrings=09/01/2013
    Verbs
      cd version exit show load
  .
  .
  .
```

When loading non-iLO firmware, the system may need to be manually reset for the changes to be applied.

Follow the command format as explained above. For example:

```
load -source http://192.168.1.1/images/fw/iLO4_100.bin
```

The following types of firmware files are supported:

- HP ProLiant System ROM
- System Programmable Logic Device
- SL Chassis Firmware

Download these server firmware files at:

<http://www.hp.com/support>

## Eventlog commands

Eventlog commands enable you to display or delete the logs of both the system and iLO 4.

Table 18 (page 56) shows the Eventlog command properties. Eventlog settings are available at:

- /system1/log1—IML
- /map1/log1—iLO event log

### Targets

record:1..n

Where  $n$  is the total number of records.

**Table 18 Eventlog Command Properties**

Property	Access	Description
number	read	Displays the record number for the event.
severity	read	Displays the severity of the event. Severity levels are informational, noncritical, critical, or unknown.
date	read	Displays the event date.
time	read	Displays the event time.
description	read	Displays a description of the event.

**For example**

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

## Blade commands

Blade commands enable you to view and modify the values on a c-Class server. [Table 19 \(page 56\)](#) shows the Blade command targets. [Table 20 \(page 56\)](#) shows the Blade command properties. These values are available at:

`/system1/map1/blade1`

**Table 19 Blade Command Targets**

Target	Description
<code>/map1/blade1/rack</code>	Displays and modifies the blade rack settings.
<code>/map1/blade1/rack/enclosure</code>	Displays and modifies the blade enclosure settings.

**Table 20 Blade Command Properties**

Property	Access	Description
bay_number	Read	Displays the blade bay number.
auto_power	Read	Displays and modifies if the blade is enabled to automatically power up.

## Boot commands

Boot commands enable you to modify the boot order of the system. [Table 21 \(page 57\)](#) shows the Boot command properties. Boot settings are available at:

`/system1/bootconfig1`

**Targets**

`bootsource<n>`

Where  $n$  is the total number of boot sources.

The boot source targets and matching boot source values do not change. The values for bootsource are:

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

**Table 21 Boot Command Properties**

Property	Access	Description
bootorder	Read/write	Configures the boot order for a given boot source

### For example

When configuring `bootorder`, first list the current boot order by entering `show -all /system1/bootconfig1`. The example output below shows `bootsource3` (BootfmDrive) is currently configured as the primary boot device, because it has a `bootorder=1`:

```
</system1/bootconfig1/bootsource1>hpiLO-> show -all /system1/bootconfig1
/system1/bootconfig1
Targets
  bootsource1
  bootsource2
  bootsource3
  bootsource4
  bootsource5
Properties
Verbs
  cd version exit show set

/system1/bootconfig1/bootsource1
Targets
Properties
  bootorder=2
Verbs
  cd version exit show set

/system1/bootconfig1/bootsource2
Targets
Properties
  bootorder=3
Verbs
  cd version exit show set

/system1/bootconfig1/bootsource3
Targets
Properties
  bootorder=1
Verbs
  cd version exit show set

/system1/bootconfig1/bootsource4
Targets
Properties
  bootorder=4
Verbs
  cd version exit show set

/system1/bootconfig1/bootsource5
Targets
```

```
Properties
  bootorder=5
Verbs
  cd version exit show set
```

To change the boot order, enter the following command:

```
set /system1/bootconfig1/bootsource<n> bootorder=<num>.
```

For example, to move `bootsource1` (BootFmCd) to be the primary boot device:

```
</system1/bootconfig1>hpiLO-> set bootsource1 bootorder=1
```

Bootorder being set.

```
bootsource1=BootFmCd          bootorder=1
bootsource3=BootFmDisk        bootorder=2
bootsource2=BootFmFloppy      bootorder=3
bootsource4=BootFmUSBKey      bootorder=4
bootsource5=BootFmNetwork     bootorder=5
```

To display the boot order for a specific device, enter the following command:

```
show /system1/bootconfig1/bootsource<n>
```

For example, to display the boot order for `bootsource1`:

```
</system1/bootconfig1>hpiLO-> show /system1/bootconfig1/bootsource1
```

```
/system1/bootconfig1/bootsource1
Targets
Properties
  bootorder=1
Verbs
  cd version exit show set
```

To display the current boot mode, enter the following command:

```
show /system1/bootconfig1/oemhp_bootmode
```

To display the pending boot mode (which will be active on the next boot), enter the following command:

```
show /system1/bootconfig1/oemhp_pendingbootmode
```

## UEFI enabled systems

When configuring the UEFI boot order, first list the current boot order by entering `show -all /system1/bootconfig1`. For systems that support UEFI, the targets are listed in their respective boot order. The example output below shows `oemhp_uefibootsource1` is currently configured as the primary boot device, because it has a `bootorder=1`

```
/system1/bootconfig1
Targets
  oemhp_uefibootsource1
  oemhp_uefibootsource2
Properties
  oemhp_bootmode=UEFI
  oemhp_secureboot=no
  oemhp_pendingbootmode=UEFI
Verbs
  cd version exit show set

/system1/bootconfig1/oemhp_uefibootsource1
Targets
Properties
  bootorder=1
  oemhp_description=Embedded FlexibleLOM 1 Port 1 : HP FlexFabric 10Gb 2-port
534FLB Adapter (IPv4)
Verbs
  cd version exit show set

/system1/bootconfig1/oemhp_uefibootsource2
```

```

Targets
Properties
  bootorder=2
  oemhp_description=Embedded FlexibleLOM 1 Port 1 : HP FlexFabric 10Gb 2-port
534FLB Adapter (IPv6)
Verbs
  cd version exit show set

```

To change the boot order for UEFI enabled systems, enter the following command:

```
set /system1/bootconfig1/oemhp_uefibootsource<n> bootorder=<num>.
```

For example, to move uefibootsource2 to be the primary boot device:

```
</system1/bootconfig1>hpiLO-> set oemhp_uefibootsource2 bootorder=1
Bootorder being set.
```

```
oemhp_uefibootsource2=534FLB Adapter (IPv6)          bootorder=1
oemhp_uefibootsource1=534FLB Adapter (IPv4)          bootorder=2
```

To display the boot order for a specific device, enter the following command:

```
show /system1/bootconfig1/oemhp_uefibootsource<n>/bootorder
```

To display the system secure boot setting for systems with UEFI enabled, enter the following command:

```
show /system1/bootconfig1/oemhp_secureboot
```

## LED commands

LED commands are used to change the state of the UID light on the server. [Table 22 \(page 59\)](#) shows the LED command properties. LED settings are available at:

```
/system1/led1
```

**Table 22 LED Command Properties**

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

### For example

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

### iLO 4 CLI support

Simple UID CLI commands are supported:

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

The CLP format is supported as well:

- `show /system1/led1`—Verifies LED status
- `start /system1/led1`—Turns LED on
- `stop /system1/led1`—Turns LED off

## System properties and targets

The properties and targets described in this section provide information about the server. [Table 23 \(page 60\)](#) shows the System targets. [Table 24 \(page 61\)](#) shows the System properties. System properties settings are available at:

/system1/oemhp\_power1

**Table 23 System Targets**

Target	Description
oemhp_PresentPower	Displays the average power reading from the last sample
oemhp_AvgPower	Displays the average power reading from the past 24 hours
oemhp_MaxPower	Displays the greatest peak power reading from the past 24 hours
oemhp_MinPower	Displays the minimum average power reading from the past 24 hours
warning_type	Displays and modifies the warning type
warning_threshold	Displays and modifies the warning threshold for power consumption
warning_duration	Displays and modifies the duration the power threshold must be exceeded before a warning is generated
oemhp_powerreg	Displays and modifies the Power Regulator for ProLiant state. Valid values are <b>dynamic</b> , <b>max</b> , <b>min</b> , or <b>os</b> .
oemhp_pwracap	Displays and modifies the power cap setting for the server in watts. A wattage of zero indicates that power capping is disabled. The value must be an integer cap value that is greater than or equal to oemhp_serverminpower, and must be less than or equal to oemhp_powersupplycapacity.
oemhp_powersupplycapacity	Displays the power supply's total capacity in Watts.
oemhp_servermaxpower	Displays the server's maximum power capacity in Watts.
oemhp_serverminpower	Displays the server's minimum power capacity in Watts.
oemhp_power_micro_ver	Displays the firmware version number for the Power Micro Controller.
oemhp_auto_pwr	Displays and modifies Server Automatic Power On setting. Valid values are on, 15, 30, 45, 60, random, restore, and off. <b>On</b> turns on automatic power on with minimum delay. Time-delayed automatic power on settings of <b>15</b> , <b>30</b> , <b>45</b> , and <b>60</b> seconds, as well as a <b>random</b> time delay of up to 120 seconds can be enabled (time starts after iLO finishes booting). <b>Restore</b> restores the last power state (except on BL servers). <b>Off</b> turns off automatic power on.

Verbs:

- cd
- version
- exit
- show
- set

For example:

- show /system1/oemhp\_power1 oemhp\_powerreg
- set /system1/oemhp\_power1 oemhp\_powerreg=<dynamic|max|min/os>
- show /system1/oemhp\_power1 oemhp\_pwracap
- set /system1/oemhp\_power1 oemhp\_pwracap=0
- show /system1/oemhp\_power1 oemhp\_power\_micro\_ver

The following properties are available in:

`/system1`

**Table 24 System Properties**

Property	Access	Description
<code>name</code>	Read	Displays the system name.
<code>number</code>	Read	Displays the system serial number.
<code>oemhp_server_name</code>	Read	Displays the host server name string. This string can be up to 50 characters in length, and requires the Configure iLO Settings privilege to change.
<code>enabledstate</code>	Read	Appears if the server is powered up.
<code>processor_number</code>	Read	Displays the number of logical processors in the system.

**For example**

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

The CPU property is a target of `/system1` and displays information about the system processor. [Table 25 \(page 61\)](#) shows the System CPU properties. The properties are available at:

`/system1/cpun`

Where *n* is the processor number.

**Table 25 System CPU Properties**

Property	Access	Description
<code>name</code>	Read	Displays manufacturer information about the processor.
<code>status</code>	Read	Displays status information.
<code>number_cores</code>	Read	Displays the number of processor cores.
<code>active_cores</code>	Read	Displays the number of active processor cores.
<code>threads</code>	Read	Displays the total number of threads on the active processor cores.
<code>speed</code>	Read	Displays the processor speed.
<code>memory_technology</code>	Read	Displays the bit level technology of the memory.
<code>cachememory1</code>	Read	Displays the size of the processor level-1 cache.
<code>cachememory2</code>	Read	Displays the size of the processor level-2 cache.
<code>cachememory3</code>	Read	Displays the size of the processor level-3 cache.

**For example:**

```
show /system1/cpu1
```

```
/system1/cpu1
Targets
Properties
  name= Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz
  status=OK
  number_cores=8
  active_cores=8
  threads=16
  speed=2600MHz
```

```
memory_technology=64-bit Capable
cachememory1=256KB
cachememory2=2048KB
cachememory3=20480KB
```

The memory property displays information about the system memory.

Table 26 (page 62) shows the System memory properties. The properties are available at:

`/system1/memoryn`

Where *n* is the memory DIMM number.

### Table 26 System Memory Properties

Property	Access	Description
size	Read	Displays the memory size.
speed	Read	Displays the memory speed.
location	Read	Displays the location of the memory.

The Slot property displays information about the system slots.

Table 27 (page 62) shows the System Slot properties. The properties are available at:

`/system1/slotn`

Where *n* is the slot number.

### Table 27 System Slot Properties

Property	Access	Description
type	Read	Displays the slot type.
width	Read	Displays the slot width.

The Firmware property displays information about the system ROM.

Table 28 (page 62) shows the System Firmware properties. The properties are available at:

`/system1/firmware1`

### Table 28 System Firmware Properties

Property	Access	Description
version	Read	Displays the version of the system ROM.
date	Read	Displays the date the system ROM.

#### For example:

- `show /system1/cpu1`—Displays information on one CPU.
- `show /system1/memory1`—Displays information on one memory slot.
- `show /system1/slot1`—Displays information on one slot.
- `show /system1/firmware1`—Displays information about system ROM.

For example:

```
/system1/firmware1
Targets
Properties
version=P56
date=01/05/2010
```

## Other commands

Other commands include the following:

`start /system1/oemhp_vsp1` Starts a virtual serial port session. Press **Esc** ( to return to the CLI session.

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

# 8 RIBCL XML Scripting Language

## Overview of the RIBCL

RIBCL enables you to write XML scripts to configure and manage iLO 4 configuration settings, user accounts, directory settings, server settings, and HP SSO settings. Download the sample scripts from the HP website at <http://www.hp.com/go/ilo>. Click **iLO Sample Scripts for Windows** or **Lights-Out XML scripting sample for Linux** on the **Resources** tab, under **Support**. Before using the XML sample scripts downloaded from the HP website, read the firmware support information in each sample script to tailor the script for the intended firmware and version.

When writing your XML scripts, write comments in the command as needed. If a comment falls in the command line, an error message is generated. Unless otherwise specified, examples in this guide are specifically for iLO 4 firmware version 1.40 and later.

This section describes the XML commands and their parameters common to most LOM products and servers. For more information about the ProLiant BL c-Class server and rack XML commands, see the *HP iLO User Guide* on the HP website at: <http://www.hp.com/go/ilo/docs>.

## XML headers

The following XML header must be present in every script, to ensure the connection is an XML connection, not an HTTP connection:

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

In addition to the header above, with the latest utilities update two other headers can be added in RIBCL scripts:

```
<?ilo entity-processing="standard"?>
```

This header added to a RIBCL script (or in a response) will take five entities in a quoted string and change them to their symbol equivalents:

**Table 29 Accepted script entities**

Entity	Symbol
&lt;	<
&gt;	>
&amp;	&
&apos;	'
&quot;	"

```
<?xmlilo output-format="xml"?>
```

This header will accept five entities (see [Table 29 \(page 64\)](#)) along with changing output to minimum of response.

**Table 30 XMLILO output (GET\_FW\_VERSION)**

Output with header	Output without header
C:\data\ilo\scripts>perl locfg.pl -s servername -f get_fw_version.xml -u admin -p admin123	
<pre>&lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;GET_FW_VERSION   FIRMWARE_VERSION = "1.60"   FIRMWARE_DATE = "Feb 27 2013"   MANAGEMENT_PROCESSOR = "iLO4"   LICENSE_TYPE = "iLO Advanced"</pre>	<pre>&lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt;</pre>

**Table 30 XMLILO output (GET\_FW\_VERSION) (continued)**

Output with header	Output without header
<pre> /&gt; &lt;/RIBCL&gt; </pre>	<pre> &lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt; &lt;/RIBCL&gt;  &lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt; &lt;/RIBCL&gt;  &lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt; &lt;GET_FW_VERSION   FIRMWARE_VERSION = "1.60"   FIRMWARE_DATE = "Feb 27 2013"   MANAGEMENT_PROCESSOR = "iLO4"   LICENSE_TYPE = "iLO Advanced"   /&gt; &lt;/RIBCL&gt;  &lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt; &lt;/RIBCL&gt;  &lt;?xml version="1.0"?&gt; &lt;RIBCL VERSION="2.22"&gt; &lt;RESPONSE   STATUS="0x0000"   MESSAGE='No error'   /&gt; &lt;/RIBCL&gt; </pre>

## Data types

The three data types allowed in the parameter are:

- String
- Specific string
- Boolean string

## String

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

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

---

### Unsupported Microsoft Windows quote characters:

Support for Windows-specific smart-quotes (" " and ' ') as content delimiters in XML is being phased out. Be sure to replace any smart-quote characters in your script with normal double or single quotes (" and ').

---

### Specific string

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

### Boolean string

A Boolean string is a specific string that specifies a *yes* or *no* condition. Acceptable Boolean strings are *yes*, *no*, *true*, *false*, *y*, *n*, *t*, *f*, *1*, and *0*. These strings are not case sensitive.

### Response definitions

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

For example:

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

- **RESPONSE**

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

- **STATUS**

This parameter contains an error number. The number `0x0000` indicates that no error exists.

- **MSG**

This element contains a message describing the error that happened. If there is no error, the `No error` message appears.

### RIBCL

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

For example:

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

### RIBCL parameters

**VERSION** is a string that indicates the version of the RIBCL that the client application is expecting to use. The **VERSION** string is compared to the version of the RIBCL that is expected, and an error message is returned if the first number of the string and the version (major version) do not match. The preferred value for the **VERSION** parameter is 2.X. For example, if the string is 2.20 and the expected major version number is 2, no error message is sent. However, if the **VERSION** string is 1.X and the expected version is 2, then the different versions may introduce compatibility issues. If there is a major version mismatch, the following inform message is sent:

The RIBCL version is incorrect. The correct version is <X.XX> or later. Update the RIBCL script to be compatible with the current RIBCL version.

## RIBCL runtime errors

The possible RIBCL error messages include:

- Version must not be blank.
- The RIBCL version is incorrect. The correct version is X.XX or later.

## Combining multiple commands in one RIBCL script

To combine multiple commands in a single RIBCL script, enclose each command in a top level \*\_INFO tag. One of the following top level tags must enclose each command used, or accidental changes to your configuration can result:

- USER\_INFO
- RIB\_INFO
- DIR\_INFO
- BLADESYSTEM\_INFO
- SERVER\_INFO
- SSO\_INFO

See the examples below for contrasting script samples.

### Example 3 Incorrectly combined script

---

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <MIN_PASSWORD value="5"/>
      </MOD_GLOBAL_SETTINGS>
      <MOD_NETWORK_SETTINGS>
        <DHCP_DNS_SERVER value="No"/>
        <DHCP_WINS_SERVER value="No"/>
        <DHCP_STATIC_ROUTE value="No"/>
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
    <USER_INFO MODE="write">
      <ADD_USER USER_NAME="admin" USER_LOGIN="admin" PASSWORD="admin">
        <ADMIN_PRIV value="Yes" />
        <REMOTE_CONS_PRIV value="Yes" />
        <RESET_SERVER_PRIV value="Yes" />
        <VIRTUAL_MEDIA_PRIV value="Yes" />
        <CONFIG_ILO_PRIV value="Yes" />
      </ADD_USER>
      <DELETE_USER USER_LOGIN="Administrator" />
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

---

### Example 4 Correctly combined script

---

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <MIN_PASSWORD value="5"/>
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
    <RIB_INFO MODE="write">
      <MOD_NETWORK_SETTINGS>
        <DHCP_DNS_SERVER value="No"/>
        <DHCP_WINS_SERVER value="No"/>
        <DHCP_STATIC_ROUTE value="No"/>
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
    <USER_INFO MODE="write">
      <ADD_USER USER_NAME="admin" USER_LOGIN="admin" PASSWORD="admin">
        <ADMIN_PRIV value="Yes" />
        <REMOTE_CONS_PRIV value="Yes" />
        <RESET_SERVER_PRIV value="Yes" />
        <VIRTUAL_MEDIA_PRIV value="Yes" />
        <CONFIG_ILO_PRIV value="Yes" />
      </ADD_USER>
    </USER_INFO>
    <USER_INFO MODE="write">
      <DELETE_USER USER_LOGIN="Administrator" />
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

---

## LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level is used when performing RIBCL actions. The specified user must have a valid iLO account to

execute RIBCL commands. The user privileges are verified against the required privilege for a particular command, and an error is returned if the privilege level does not match.

For example:

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

Alternatively, the HPQLOCFG utility allows you to specify the login information as parameters on the command line using switches:

```
hpqlocfg -u username -p password
```

## LOGIN parameters

USER\_LOGIN is the login name of the user account. This parameter is case sensitive and must not be blank.

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

## LOGIN runtime errors

Possible runtime error messages include:

- User login name was not found.
- Password must not be blank.
- Logged-in user does not have required privilege for this command.

## USER\_INFO

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

USER\_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

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

For example:

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

## ADD\_USER

The ADD\_USER command is used to add a local user account. The USER\_NAME and USER\_LOGIN parameters must not exist in the current user database. Use the MOD\_USER command to change existing user information. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE must be set to write. The user must have the Administer User Accounts privilege.

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

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

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <USER_INFO MODE="write">
    <ADD_USER
      USER_NAME="User"
      USER_LOGIN="username"
      PASSWORD="password">
      <ADMIN_PRIV value ="N"/>
      <REMOTE_CONS_PRIV value ="Y"/>
      <RESET_SERVER_PRIV value ="N"/>
      <VIRTUAL_MEDIA_PRIV value ="N"/>
      <CONFIG_ILO_PRIV value="Y"/>
    </ADD_USER>
  </USER_INFO>
</LOGIN>
</RIBCL>

```

## ADD\_USER parameters

USER\_NAME is the actual name of the user. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is not case sensitive and must not be blank.

USER\_LOGIN is the name used to gain access to the respective iLO. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is not case sensitive and must not be left blank.

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

ADMIN\_PRIV is a Boolean parameter that enables the user to administer user accounts. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. The user can modify account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE\_CONS\_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET\_SERVER\_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL\_MEDIA\_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter denies the user the Virtual Media privilege.

CONFIG\_ILO\_PRIV is a Boolean parameter that enables the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

## ADD\_USER runtime errors

Possible ADD\_USER error messages include:

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

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

## DELETE\_USER

The DELETE\_USER command is used to remove an existing local user account. The USER\_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE must be set to write. The user must have the Administer User Accounts privilege.

For example:

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

### DELETE\_USER parameter

USER\_LOGIN is the login name of the user account. This parameter is case sensitive and must not be blank.

### DELETE\_USER runtime errors

Possible DELETE\_USER errors include:

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

## DEL\_USERS\_SSH\_KEY

Deletes any SSH keys associated with USER\_LOGIN. The DEL\_USERS\_SSH\_KEY command is implemented as a subcommand and must appear within a MOD\_USER command block. This command requires HPQLOCFG.EXE version 1.00 or later.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="admin" PASSWORD="admin123">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="admin">
        <DEL_USERS_SSH_KEY/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

```
        </MOD_USER>
    </USER_INFO>
</LOGIN>
</RIBCL>
```

## DEL\_SSH\_KEY parameters

None

## DEL\_SSH\_KEY runtime errors

Possible DEL\_SSH\_KEY runtime errors include:

- User login name must not be blank
- User does not have correct privilege for action. ADMIN\_PRIV required.
- Unable to clear the SSH key.

## GET\_USER

The GET\_USER command returns local user information, excluding the password. The USER\_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE can be in read or write. The user must have the Administer User Accounts privilege to retrieve other user accounts. Otherwise, the user can only view their individual account information.

For example:

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

## GET\_USER parameter

USER\_LOGIN is the login name of the user account. This parameter is case sensitive and must not be blank.

## GET\_USER runtime errors

Possible GET\_USER error messages include:

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

## GET\_USER return messages

A possible GET\_USER return message includes:

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

## MOD\_USER

The MOD\_USER command is used to modify an existing local user account. The USER\_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE must be set to write. The user must have the Administer User Accounts privilege. Otherwise, the user can only modify their individual account password.

🎥 To see a video demonstration of using the MOD\_USER command to change a user password, see *How to use HP iLO's XML scripting interface, RIBCL, to change an user password.* at <http://www.hp.com/go/ilo/videos>.

For example:

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

Reset administrator password example:

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

Change password example:

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

## MOD\_USER parameters

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

MOD\_USER USER\_LOGIN is the login name of the user to be changed. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is not case sensitive and must not be left blank.

USER\_NAME is the actual name of the user to be modified. This parameter is not case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must not be left blank.

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

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

REMOTE\_CONS\_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET\_SERVER\_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL\_MEDIA\_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter denies the user The Virtual Media privilege.

CONFIG\_ILO\_PRIV is a Boolean parameter that enables the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to `Yes` if the user is allowed this privilege. If this parameter is used, the Boolean string value must not be left blank. Omitting this parameter prevents the user from manipulating the current iLO configuration.

## MOD\_USER runtime errors

Possible MOD\_USER error messages include:

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

## GET\_ALL\_USERS

The GET\_ALL\_USERS command returns all USER\_LOGIN parameters in the user database. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE can be in read or write. The user must have the Administer User Accounts privilege to retrieve all user accounts.

For example:

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

```
<GET_ALL_USERS />
</USER_INFO>
</LOGIN>
</RIBCL>
```

## GET\_ALL\_USERS parameters

None

## GET\_ALL\_USERS runtime errors

The possible GET\_ALL\_USERS error messages include:

- User does not have correct privilege for action. ADMIN\_PRIV required.

## GET\_ALL\_USERS return messages

A possible GET\_ALL\_USERS return message is:

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

A possible unsuccessful request is:

```
<RESPONSE STATUS="0x0023" MESSAGE='User does NOT have correct
privilege for action.
ADMIN_PRIV required.' />
```

## GET\_ALL\_USER\_INFO

The GET\_ALL\_USER\_INFO command returns all local user information in the user database, excluding passwords. For this command to parse correctly, the command must appear within a USER\_INFO command block, and USER\_INFO MODE can be in read or write. The user must have the Administer User Accounts privilege to execute this command.

For example:

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

## GET\_ALL\_USER\_INFO parameters

None

## GET\_ALL\_USER\_INFO runtime errors

The possible GET\_ALL\_USER\_INFO error messages include:

User does not have correct privilege for action. ADMIN\_PRIV required.

## GET\_ALL\_USER\_INFO return messages

A possible GET\_ALL\_USER\_INFO return message is:

```
<GET_ALL_USER_INFO/>
<GET_USER
USER_NAME="Admin"
USER_LOGIN="Admin"
ADMIN_PRIV="Y"
CONFIG_RILO_PRIV="Y"
LOGIN_PRIV="Y"
REMOTE_CONS_PRIV="Y"
RESET_SERVER_PRIV="Y"
VIRTUAL_MEDIA_PRIV="Y"
/> .....
```

The same information will be repeated for all the users.

```
</GET_ALL_USER_INFO>
```

A possible unsuccessful request is:

```
<RESPONSE STATUS="0x0023" MESSAGE='User does NOT have correct
privilege for action.
ADMIN_PRIV required.'/>
```

## RIB\_INFO

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

RIB\_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

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

For example:

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

Clear iLO event log example:

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

## RESET\_RIB

The RESET\_RIB command is used to reset iLO. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE can be set to read or write. The user must have the Configure iLO Settings privilege to execute this command.

For example:

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

### RESET\_RIB parameters

None

### RESET\_RIB runtime errors

The possible RESET\_RIB error message include:

User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.

## GET\_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.

For example:

- iLO Event Log example:

```
<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="READ">
      <GET_EVENT_LOG />
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

- Integrated Management log example:

```
<RIBCL version="2.0">
  <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="2.0">
<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.
  - DEGRADED indicates the device or subsystem is operating at a reduced capacity.
  - 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\_FEDERATION\_MULTICAST

Use the GET\_FEDERATION\_MULTICAST command to retrieve the current federation multicast options. The response includes values for Multicast Discovery, Multicast Announcement Interval, IPv6 Multicast Scope, and Multicast TTL. The command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to read.

For example:

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

### GET\_FEDERATION\_MULTICAST parameters

None

### GET\_FEDERATION\_MULTICAST runtime errors

None

### GET\_FEDERATION\_MULTICAST return messages

The following response is typical of the data returned from the GET\_FEDERATION\_MULTICAST command:

```
<?xml version="1.0"?>  
<RIBCL VERSION="2.23">  
<RESPONSE  
  STATUS="0x0000"  
  MESSAGE='No error'  
  />  
<GET_FEDERATION_MULTICAST>  
  <MULTICAST_DISCOVERY_ENABLED VALUE="Yes"/>  
  <MULTICAST_ANNOUNCEMENT_INTERVAL VALUE="60"/>  
  <IPv6_MULTICAST_SCOPE VALUE="Site"/>  
  <MULTICAST_TTL VALUE="255"/>  
</GET_FEDERATION_MULTICAST>  
</RIBCL>
```

## SET\_FEDERATION\_MULTICAST

Enter the SET\_FEDERATION\_MULTICAST to set federation multicast options, including Multicast Discovery, Multicast Announcement Interval, IPv6 Multicast Scope, and Multicast TTL.

---

**NOTE:** Disabling multicast discovery or announcements disables iLO federation features.

All devices in a federated group must have the same scope and TTL to properly enable peer discovery.

---

For example:

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

```

    <SET_FEDERATION_MULTICAST>
      <MULTICAST_DISCOVERY_ENABLED VALUE="Yes"/>
      <MULTICAST_ANNOUNCEMENT_INTERVAL VALUE="30"/>
      <IPV6_MULTICAST_SCOPE VALUE="Site"/>
      <MULTICAST_TTL VALUE="255"/>
    </SET_FEDERATION_MULTICAST>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

## SET\_FEDERATION\_MULTICAST parameters

**MULTICAST\_DISCOVERY\_ENABLED** enables or disables multicast discovery. Value must be either **Yes** (enabled) or **No** (disabled). When enabled, this parameters makes the iLO discoverable as federated on the network. When disabled, iLO Federation Management features are unavailable.

**MULTICAST\_ANNOUNCEMENT\_INTERVAL** sets the number of seconds between each multicast availability announcement on the network. Valid values are **Disabled**, **30**, **60**, **120**, **300**, **600**, **900**, and **1800** seconds. When disabled, iLO Federation Management features are unavailable.

**IPV6\_MULTICAST\_SCOPE** sets the scope of multicast discovery. Valid values are **Link** (link-local), **site** (site-local), and **organization** (organization-local). All devices in a federated group must have the same scope to properly enable peer discovery.

**MULTICAST\_TTL** sets the time to live, limiting the number of switches that can be traversed before the multicast discovery is stopped. Any value between **1** and **255** can be used. All devices in a federated group must have the same TTL to properly enable peer discovery.

## SET\_FEDERATION\_MULTICAST runtime errors

Some possible SET\_FEDERATION\_MULTICAST error messages include:

- The **MULTICAST\_ANNOUNCEMENT\_INTERVAL VALUE** is invalid.
- The **IPV6\_MULTICAST\_SCOPE VALUE** is invalid.
- The **MULTICAST\_TTL VALUE** is invalid. Valid values are between 1 and 255.
- User does not have correct privilege for action. **CONFIG\_ILO\_PRIV** required.

## GET\_FEDERATION\_ALL\_GROUPS

Use the **GET\_FEDERATION\_ALL\_GROUPS** command to retrieve a list of all iLO 4 Federation group names. The command must appear within a **RIB\_INFO** command block, and **RIB\_INFO MODE** must be set to read.

For example:

```

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

```

## GET\_FEDERATION\_ALL\_GROUPS parameters

None

## GET\_FEDERATION\_ALL\_GROUPS runtime errors

None

## GET\_FEDERATION\_ALL\_GROUPS return messages

The following response is typical of the data returned from the GET\_FEDERATION\_ALL\_GROUPS command:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_FEDERATION_ALL_GROUPS>
  <GROUP_NAME VALUE="Group1"/>
  <GROUP_NAME VALUE="Group2"/>
</GET_FEDERATION_ALL_GROUPS>
</RIBCL>
```

## GET\_FEDERATION\_ALL\_GROUPS\_INFO

Use GET\_FEDERATION\_ALL\_GROUPS\_INFO to retrieve a list of all Federation group names and the associated privileges for each group. To retrieve the privileges of a single specified group, use [GET\\_FEDERATION\\_GROUP](#).

Besides the group name, the returned group privileges include:

- User account administration
- Remote console access
- Virtual power and reset
- Virtual media
- iLO setting configuration
- Login privilege

The command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to read.

For example:

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

## GET\_FEDERATION\_ALL\_GROUPS\_INFO parameters

None

## GET\_FEDERATION\_ALL\_GROUPS\_INFO runtime errors

None

## GET\_FEDERATION\_ALL\_GROUPS\_INFO return messages

The following response is typical of the data returned from the GET\_FEDERATION\_ALL\_GROUPS\_INFO command:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
```

```

<GET_FEDERATION_ALL_GROUPS_INFO>
  <FEDERATION_GROUP>
    <GROUP_NAME VALUE="Group1"/>
    <ADMIN_PRIV VALUE="Yes"/>
    <REMOTE_CONS_PRIV VALUE="Yes"/>
    <RESET_SERVER_PRIV VALUE="Yes"/>
    <VIRTUAL_MEDIA_PRIV VALUE="Yes"/>
    <CONFIG_ILO_PRIV VALUE="Yes"/>
    <LOGIN_PRIV VALUE="Yes"/>
  </FEDERATION_GROUP>
  <FEDERATION_GROUP>
    <GROUP_NAME VALUE="Group2"/>
    <ADMIN_PRIV VALUE="Yes"/>
    <REMOTE_CONS_PRIV VALUE="Yes"/>
    <RESET_SERVER_PRIV VALUE="No"/>
    <VIRTUAL_MEDIA_PRIV VALUE="No"/>
    <CONFIG_ILO_PRIV VALUE="Yes"/>
    <LOGIN_PRIV VALUE="Yes"/>
  </FEDERATION_GROUP>
</GET_FEDERATION_ALL_GROUPS_INFO>
</RIBCL>

```

## GET\_FEDERATION\_GROUP

Use `GET_FEDERATION_GROUP` to retrieve the privileges granted to a specified Federated group. To retrieve the privileges granted to all groups, use [GET\\_FEDERATION\\_ALL\\_GROUPS\\_INFO](#). Besides the group name, the return includes the following group privileges:

- User account administration
- Remote console access
- Virtual power and reset
- Virtual media
- iLO setting configuration
- Login privilege

The command must appear within a `RIB_INFO` command block, and `RIB_INFO MODE` must be set to read.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_FEDERATION_GROUP GROUP_NAME="groupname"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

### GET\_FEDERATION\_GROUP parameters

**GROUP\_NAME**—The name of the group to be displayed. The name must be from 1 to 31 characters long.

### GET\_FEDERATION\_GROUP runtime errors

`GET_FEDERATION_GROUP` returns the following message if the value specified for `GROUP_NAME` does not match any existing groups:

Group name not found.

## GET\_FEDERATION\_GROUP return messages

The following response is typical of the data returned from the GET\_FEDERATION\_GROUP command:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_FEDERATION_GROUP>
  <FEDERATION_GROUP>
    <GROUP_NAME VALUE="Group2"/>
    <ADMIN_PRIV VALUE="Yes"/>
    <REMOTE_CONS_PRIV VALUE="Yes"/>
    <RESET_SERVER_PRIV VALUE="No"/>
    <VIRTUAL_MEDIA_PRIV VALUE="No"/>
    <CONFIG_ILO_PRIV VALUE="Yes"/>
    <LOGIN_PRIV VALUE="Yes"/>
  </FEDERATION_GROUP>
</GET_FEDERATION_GROUP>
</RIBCL>
```

## ADD\_FEDERATION\_GROUP

Use ADD\_FEDERATION\_GROUP to add a new Federation group membership and associated privileges. The command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <ADD_FEDERATION_GROUP
        GROUP_NAME="groupname"
        GROUP_KEY="groupkey">
          <ADMIN_PRIV VALUE="Yes"/>
          <REMOTE_CONS_PRIV VALUE="Yes"/>
          <RESET_SERVER_PRIV VALUE="Yes"/>
          <VIRTUAL_MEDIA_PRIV VALUE="Yes"/>
          <CONFIG_ILO_PRIV VALUE="Yes"/>
          <LOGIN_PRIV VALUE="Yes"/>
        </ADD_FEDERATION_GROUP>
      </RIB_INFO>
    </LOGIN>
  </RIBCL>
```

---

**NOTE:** HP iLO 4 supports a maximum of 10 Federation groups. To remove a Federation group, use [DELETE\\_FEDERATION\\_GROUP](#).

---

## ADD\_FEDERATION\_GROUP parameters

**GROUP\_NAME**—The name of the group to be added. The name must be from 1 to 31 characters long.

**GROUP\_KEY**—The password to set for the group to be added. The password must be 1 to 31 characters long.

**ADMIN\_PRIV**—Administer User Accounts—Enables members of a group to add, edit, and delete iLO user accounts.

**REMOTE\_CONS\_PRIV**—Remote Console Access—Enables members of a group to remotely access the host system Remote Console, including video, keyboard, and mouse control.

RESET\_SERVER\_PRIV—Virtual Power and Reset—Enables members of a group to power-cycle or reset the local iLO system.

VIRTUAL\_MEDIA\_PRIV—Virtual Media—Enables members of a group to use scripted Virtual Media with the local iLO system.

CONFIG\_ILO\_PRIV—Configure iLO Settings—Enables members of a group to configure most iLO settings, including security settings, and to remotely update firmware.

LOGIN\_PRIV—Login—Enables members of a group to log in to iLO.

## ADD\_FEDERATION\_GROUP runtime errors

- The GROUP\_NAME must not be left blank.
- The GROUP\_NAME is too long.
- The GROUP\_KEY must not be left blank.
- The GROUP\_KEY is too long.
- Group membership already exists.
- Cannot add group membership. Maximum number of memberships reached: 10.

## MOD\_FEDERATION\_GROUP

Use MOD\_FEDERATION\_GROUP to modify an existing Federation group membership and associated privileges. The command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write.

---

**NOTE:** All parameters are optional. Any Federation property not explicitly modified retains its old value.

---

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_FEDERATION_GROUP GROUP_NAME="groupname">
        <GROUP_NAME VALUE="newgroupname"/>
        <GROUP_KEY VALUE="newgroupkey"/>
        <ADMIN_PRIV VALUE="Yes"/>
        <REMOTE_CONS_PRIV VALUE="Yes"/>
        <RESET_SERVER_PRIV VALUE="Yes"/>
        <VIRTUAL_MEDIA_PRIV VALUE="Yes"/>
        <CONFIG_ILO_PRIV VALUE="Yes"/>
        <LOGIN_PRIV VALUE="Yes"/>
      </MOD_FEDERATION_GROUP>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## MOD\_FEDERATION\_GROUP parameters

GROUP\_NAME—The name of the group to be changed, or the new name to be given to the specified Federation group, depending on the parameters' location. The name must be from 1 to 31 characters long.

GROUP\_KEY—The new password to set for the group. The password must be 1 to 31 characters long.

ADMIN\_PRIV—Administer User Accounts—Enables members of a group to add, edit, and delete iLO user accounts.

REMOTE\_CONS\_PRIV—Remote Console Access—Enables members of a group to remotely access the host system Remote Console, including video, keyboard, and mouse control.

RESET\_SERVER\_PRIV—Virtual Power and Reset—Enables members of a group to power-cycle or reset the local iLO system.

VIRTUAL\_MEDIA\_PRIV—Virtual Media—Enables members of a group to use scripted Virtual Media with the local iLO system.

CONFIG\_ILO\_PRIV—Configure iLO Settings—Enables members of a group to configure most iLO settings, including security settings, and to remotely update firmware.

LOGIN\_PRIV—Login—Enables members of a group to log in to iLO.

## MOD\_FEDERATION\_GROUP runtime errors

Some possible MOD\_FEDERATION\_GROUP error messages include:

- The GROUP\_NAME must not be left blank.

---

**NOTE:** This error only appears if the value in the <MOD\_FEDERATION\_GROUP GROUP\_NAME="groupname"> command is left blank. This error does not appear if *newgroupname* in the parameter setting <GROUP\_NAME VALUE="newgroupname"/> is left blank or the line is omitted. In that case, the original group name is retained.

---

- Group name not found.
- The GROUP\_NAME is too long.
- The GROUP\_KEY must not be left blank.
- The GROUP\_KEY is too long.
- Group membership already exists.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.

## DELETE\_FEDERATION\_GROUP

Use DELETE\_FEDERATION\_GROUP to remove the iLO from a Federation group membership. The command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write.

For example:

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

## DELETE\_FEDERATION\_GROUP parameters

GROUP\_NAME—The name of the Federation group to be deleted. The name must be from 1 to 31 characters long and must already exist as a membership group.

## DELETE\_FEDERATION\_GROUP runtime errors

Possible runtime errors returned by DELETE\_FEDERATION\_GROUP include:

- If the value specified for GROUP\_NAME does not match any existing groups: Group name not found.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.

## CLEAR\_EVENTLOG

The CLEAR\_EVENTLOG command clears the iLO Event Log. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write. The user must have the Configure iLO Settings privilege to execute this command.

For example:

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

## CLEAR\_EVENTLOG parameters

None

## CLEAR\_EVENTLOG runtime errors

The possible CLEAR\_EVENTLOG error messages are:

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

## COMPUTER\_LOCK\_CONFIG

The COMPUTER\_LOCK\_CONFIG command is used to configure the Remote Console Computer Lock feature. 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 Settings privilege to execute this command.

Uppercase letters are not supported, and are converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. For a complete list of the supported custom keys, see the *HP iLO User Guide* on the HP website at: <http://www.hp.com/go/ilo/docs>.

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

        <!-- To set default Windows Computer Lock keys combination:      -->
        <COMPUTER_LOCK value="windows"/>

        <!-- To configure custom Computer Lock keys combination:      -->
        <!--
        <COMPUTER_LOCK value="custom"/>
        <COMPUTER_LOCK_KEY value="L_GUI,1"/>
        -->

        <!-- To disable Computer Lock feature:                          -->
        <!--
        <COMPUTER_LOCK value="disabled"/>
        -->

      </COMPUTER_LOCK_CONFIG>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## COMPUTER\_LOCK\_CONFIG parameters

COMPUTER\_LOCK value— You can customize Windows, Linux and other operating systems by setting the value:

- windows—Sets the command to define the computer lock for a Windows based operating system. The computer lock on Windows based operating systems defaults to the **Windows logo + L** keys.
- custom—Sets the command to define the computer lock for a non-Windows based operating system.
- disabled—Disables the computer lock feature.

COMPUTER\_LOCK key—Sets the key combination to lock an operating system.

For example:

```
<COMPUTER_LOCK key="l_gui,l"/>
```

## COMPUTER\_LOCK\_CONFIG runtime errors

Possible COMPUTER\_LOCK\_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Invalid number of parameters. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.
- Invalid COMPUTER\_LOCK option; value must be windows, custom, or disabled.
- COMPUTER\_LOCK value must be set to custom to use the COMPUTER\_LOCK\_KEY tag.
- The COMPUTER\_LOCK key command was used without a preceding COMPUTER\_LOCK value command equal to custom.
- The key parameter specified is not valid.

## 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.

For 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>
  <ENABLE_NIC VALUE="Y"/>
  <SHARED_NETWORK_PORT VALUE="N"/>
  <VLAN_ENABLED VALUE="N"/>
  <VLAN_ID VALUE="4"/>
  <SPEED_AUTOSELECT VALUE="Y"/>
  <NIC_SPEED VALUE="Automatic"/>
  <FULL_DUPLEX VALUE="Automatic"/>
  <DHCP_ENABLE VALUE="Y"/>
  <DHCP_GATEWAY VALUE="Y"/>
  <DHCP_DNS_SERVER VALUE="Y"/>
  <DHCP_WINS_SERVER VALUE="Y"/>
  <DHCP_STATIC_ROUTE VALUE="Y"/>
  <DHCP_DOMAIN_NAME VALUE="N"/>
  <DHCP_SNTP_SETTINGS VALUE="N"/>
  <REG_WINS_SERVER VALUE="Y"/>
  <REG_DDNS_SERVER VALUE="Y"/>
  <PING_GATEWAY VALUE="Y"/>
  <MAC_ADDRESS VALUE="9c:8e:99:30:a5:50"/>
  <IP_ADDRESS VALUE="192.168.1.3"/>
  <SUBNET_MASK VALUE="255.255.252.0"/>
  <GATEWAY_IP_ADDRESS VALUE="192.168.1.1"/>
  <DNS_NAME VALUE="ILODNSNAME"/>
  <DOMAIN_NAME VALUE="hp.com"/>
  <PRIM_DNS_SERVER VALUE="192.168.1.2"/>
  <SEC_DNS_SERVER VALUE="0.0.0.0"/>
  <TER_DNS_SERVER VALUE="0.0.0.0"/>
  <PRIM_WINS_SERVER VALUE="0.0.0.0"/>
  <SEC_WINS_SERVER VALUE="0.0.0.0"/>
  <SNTP_SERVER1 VALUE=""/>
  <SNTP_SERVER2 VALUE=""/>
  <TIMEZONE VALUE="Atlantic/Reykjavik"/>
  <STATIC_ROUTE_1 DEST="0.0.0.0"
    MASK="0.0.0.0"
    GATEWAY="0.0.0.0"/>
  <STATIC_ROUTE_2 DEST="0.0.0.0"
    MASK="0.0.0.0"
    GATEWAY="0.0.0.0"/>
  <STATIC_ROUTE_3 DEST="0.0.0.0"
    MASK="0.0.0.0"
    GATEWAY="0.0.0.0"/>
  <IPV6_ADDRESS VALUE="fe80::9e8e:99ff:fe30:a550"
    PREFIXLEN="64"
    ADDR_SOURCE="SLAAC"
    ADDR_STATUS="ACTIVE"/>
  <IPV6_ADDRESS VALUE="fd0e:2d:ba9:221a:9e8e:99ff:fe30:a550"
    PREFIXLEN="64"
    ADDR_SOURCE="SLAAC"
    ADDR_STATUS="ACTIVE"/>
  <IPV6_STATIC_ROUTE_1
    IPV6_DEST="::"
    PREFIXLEN="0"
    IPV6_GATEWAY="::"
    ADDR_STATUS="INACTIVE"/>
  <IPV6_STATIC_ROUTE_2
    IPV6_DEST="::"
    PREFIXLEN="0"
    IPV6_GATEWAY="::"
    ADDR_STATUS="INACTIVE"/>
  <IPV6_STATIC_ROUTE_3
    IPV6_DEST="::"
    PREFIXLEN="0"
```

```

        IPV6_GATEWAY="::"
        ADDR_STATUS="INACTIVE"/>
<IPV6_PRIM_DNS_SERVER VALUE="::"/>
<IPV6_SEC_DNS_SERVER VALUE="::"/>
<IPV6_TER_DNS_SERVER VALUE="::"/>
<IPV6_DEFAULT_GATEWAY VALUE="::"/>
<IPV6_PREFERRED_PROTOCOL VALUE="Y"/>
<IPV6_ADDR_AUTOCFG VALUE="Y"/>
<IPV6_REG_DDNS_SERVER VALUE="Y"/>
<DHCPV6_STATELESS_ENABLE VALUE="Y"/>
<DHCPV6_STATEFUL_ENABLE VALUE="Y"/>
<DHCPV6_RAPID_COMMIT VALUE="N"/>
<DHCPV6_SNTP_SETTINGS VALUE="N"/>
<DHCPV6_DNS_SERVER VALUE="Y"/>
</GET_NETWORK_SETTINGS>

```

If the request is unsuccessful, you might receive the following message:

```

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

```

- For IPV6\_ADDRESS the ADDR\_STATUS="string", will report status of "Pending", "Active", or "Failed" for each address. Pending indicates the Duplicate Address Detection (DAD) test is still in progress, Failed indicates that a duplicate address was found on the network and the address is not currently in use by iLO, and Active indicates that DAD passed and the address is in use by iLO.
- For IPV6\_ADDRESS the ADDR\_SOURCE="string" will report status of "Static" or "SLAAC" indicating the configuration source for that address. SLAAC indicates RFC 4862 Stateless Address Auto Configuration.
- For IPV6\_STATIC\_ROUTE\_[1:3] the ADDR\_STATUS="string" will report status of "Active" or "Failed" for each static route configured. Active indicates the route was accepted by the networking stack and is in use. Failed indicates the route was rejected by the networking stack, typically this is due to a "No route to source" error for the specified gateway. In this case, iLO will periodically retry setting the static route as long as it remains configured (a route to the gateway may be discovered in the future through router advertisements or further iLO address configuration.)

## MOD\_NETWORK\_SETTINGS

Use MOD\_NETWORK\_SETTINGS 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 Settings 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.

Once the script has successfully completed, the iLO management processor reboots to apply the changes. If connectivity to iLO is lost, use the RBSU to reconfigure the network settings to values that are compatible with the network environment.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">

```

```

<RIB_INFO MODE="write">
  <MOD_NETWORK_SETTINGS>
    <ENABLE_NIC value="Yes"/>
    <REG_DDNS_SERVER value="Yes"/>
    <PING_GATEWAY value="No"/>
    <DHCP_DOMAIN_NAME value="Yes"/>
    <SPEED_AUTOSELECT value="YES"/>
    <NIC_SPEED value="100"/>
    <FULL_DUPLEX value="Yes"/>
    <DHCP_ENABLE value="No"/>
    <IP_ADDRESS value="172.20.60.152"/>
    <SUBNET_MASK value="255.255.255.0"/>
    <GATEWAY_IP_ADDRESS value="172.20.60.1"/>
    <DNS_NAME value="demoilo"/>
    <DOMAIN_NAME value="internal.com"/>
    <DHCP_GATEWAY value="Yes"/>
    <DHCP_DNS_SERVER value="Yes"/>
    <DHCP_WINS_SERVER value="Yes"/>
    <DHCP_STATIC_ROUTE value="Yes"/>
    <REG_WINS_SERVER value="Yes"/>
    <PRIM_DNS_SERVER value="0.0.0.0"/>
    <SEC_DNS_SERVER value="0.0.0.0"/>
    <TER_DNS_SERVER value="0.0.0.0"/>
    <PRIM_WINS_SERVER value="0.0.0.0"/>
    <SEC_WINS_SERVER value="0.0.0.0"/>
    <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"/>
    <DHCP_SNTP_SETTINGS value="Yes"/>
    <SNTP_SERVER1 value="0.0.0.0"/>
    <SNTP_SERVER2 value="0.0.0.0"/>
    <TIMEZONE value="America/Anchorage"/>
    <!-- This tag can be used on an iLO blade server to force iLO -->
    <!-- to attempt to get an IP address from the signal backplane -->
    <!-- in a server enclosure. The IP address must be set prior -->
    <!-- with Mod_Enc_Bay_IP_Settings.xml -->
    <!-- <ENCLOSURE_IP_ENABLE VALUE="Yes"/> -->
  </MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

Modify VLAN for the embedded LOM example:

```

<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="WRITE" >
      <MOD_NETWORK_SETTINGS>
        <ENABLE_NIC value="Yes"/>
        <SHARED_NETWORK_PORT VALUE="Yes"/>
        <VLAN_ENABLED VALUE="Yes" />
        <VLAN_ID VALUE="1"/>
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

Modify VLAN for the FlexibleLOM example:

```

<RIBCL version="2.21">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="WRITE" >
      <MOD_NETWORK_SETTINGS>
        <ENABLE_NIC value="Yes"/>
        <SHARED_NETWORK_PORT VALUE="FlexibleLOM"/>
        <VLAN_ENABLED VALUE="Yes" />
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

```

    <VLAN_ID VALUE="1" />
  </MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

RBSU POST IP example:

```

<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write" >
      <MOD_GLOBAL_SETTINGS>
        <RBSU_POST_IP VALUE="Y"/>
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

Shared network port example:

```

<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="WRITE" >
      <MOD_NETWORK_SETTINGS>
        <SHARED_NETWORK_PORT VALUE="N"/>
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## IPv6\_ADDRESS support

MOD\_NETWORK\_SETTINGS supports IPv6. This section of the sample script (shown below) is commented out by default. Uncomment the parameters as needed to enable them, and disable (comment out) the equivalent IPv4 parameters. See [IPv6 MOD\\_NETWORK\\_SETTINGS parameters](#) for information on the parameters and their values.

```

<IPV6_ADDRESS VALUE="2001:DB8:2:1::15" PREFIXLEN="64"/>
<IPV6_ADDRESS VALUE="2001:DB8:2:2::15" PREFIXLEN="64"/>
<IPV6_ADDRESS VALUE="FC00:DB8:2:3::15" PREFIXLEN="64"/>
<IPV6_ADDRESS VALUE="FC00:DB8:2:2::15"
  PREFIXLEN="64"
  ADDR_SOURCE="STATIC"
  ADDR_STATUS="ACTIVE"/>
<IPV6_STATIC_ROUTE_1
  IPV6_DEST="::"
  PREFIXLEN="0"
  IPV6_GATEWAY="::"
  ADDR_STATUS="INACTIVE"/>
<IPV6_STATIC_ROUTE_2
  IPV6_DEST="::"
  PREFIXLEN="0"
  IPV6_GATEWAY="::"
  ADDR_STATUS="INACTIVE"/>
<IPV6_STATIC_ROUTE_3
  IPV6_DEST="2001:DB8:2002:3003::"
  PREFIXLEN="64"
  IPV6_GATEWAY="2001:DB8:1::40"
  ADDR_STATUS="ACTIVE"/>
<IPV6_PRIM_DNS_SERVER VALUE="2001:DB8:2:1::13"/>
<IPV6_SEC_DNS_SERVER VALUE="::"/>
<IPV6_TER_DNS_SERVER VALUE="::"/>
<IPV6_DEFAULT_GATEWAY VALUE="::"/>
<IPV6_PREFERRED_PROTOCOL VALUE="Y"/>
<IPV6_ADDR_AUTOCFG VALUE="Y"/>

```

```

<IPV6_REG_DDNS_SERVER VALUE="Y"/>
<SNTP_SERVER1 VALUE="2001:DB8:2:1::13"/>
<SNTP_SERVER2 VALUE="2001:DB8:1:1::13"/>
<!--      Support for the following 5 tags:      -->
<!--      iLO 4 - Version 1.30 and later.      -->
<!--      iLO 3 - Version 1.60 and later.      -->
<!--      iLO 2 - None                          -->
<DHCPV6_STATELESS_ENABLE VALUE="Y"/>
<DHCPV6_STATEFUL_ENABLE VALUE="Y"/>
<DHCPV6_RAPID_COMMIT VALUE="N"/>
<DHCPV6_SNTP_SETTINGS VALUE="N"/>
<DHCPV6_DNS_SERVER VALUE="Y"/>

```

## MOD\_NETWORK\_SETTINGS runtime errors

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.
- iLO may not be disabled on this server. This message is sent if ENABLE\_NIC is set to No and the system is a blade.

## 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 sets the Shared Network Port value. The values are LOM, FlexibleLOM, Yes, or No. The Shared Network Port feature is only available on servers with hardware, NIC firmware, and iLO firmware that supports this feature. This command is supported on all 300, 500, 700 and 900 ML/DL servers, though not all values, (LOM or FlexibleLOM), are supported on all servers.

- No—Enables a NIC with a jack on the back of the server (a dedicated network port).
- Yes—Enables a NIC that is built into the server (a shared network port). The NIC handles server network traffic and can, if ILO is configured to do so, handle iLO traffic at the same time.
- LOM—Enables a NIC that is built into the server (a shared network port). The NIC handles server network traffic and can, if ILO is configured to do so, handle iLO traffic at the same time. Not all servers support a LOM.
- FlexibleLOM—Enables an optional NIC that plugs into a special slot on the server. The NIC handles server network traffic and can, if iLO is configured to do so, handle iLO traffic at the same time. Not all servers support a FlexibleLOM.

When using the iLO Shared Network Port, flashing the iLO firmware through the XML interface takes approximately 7 minutes to complete. Flashing the firmware using Shared Network Port with iLO does not take any longer to complete than using the dedicated iLO management port.

REG\_DDNS\_SERVER VALUE instructs iLO to register the management port with a DDNS server. The possible values are Yes or No.

SPEED\_AUTOSELECT is a Boolean parameter to enable or disable the iLO transceiver to auto-detect the speed (NIC\_SPEED) and duplex (FULL\_DUPLEX) of the network. This parameter is optional, and the Boolean string must be set to Yes to enable the speed auto-detect. If this parameter is used, the Boolean string value must not be left blank. The possible values are Yes or No. The parameter value is case insensitive.

NIC\_SPEED is used to set the transceiver speed if SPEED\_AUTOSELECT is set to No. The possible values are 10, 100, or Automatic. If SPEED\_AUTOSELECT is set to N, and NIC\_SPEED is set to Automatic, the current value is retained. In other words, if SPEED\_AUTOSELECT is set to N, then Automatic is not an applicable value for NIC\_SPEED.

FULL\_DUPLEX is used to decide if 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, No, or Automatic. If SPEED\_AUTOSELECT is set to N, and FULL\_DUPLEX is set to Automatic, the current value is retained. In other words, if SPEED\_AUTOSELECT is set to N, then Automatic is not an applicable value for FULL\_DUPLEX. The parameter value is case insensitive.

DHCP\_ENABLE is used to enable DHCP. The possible values are Yes or No. The parameter value is case insensitive.

IP\_ADDRESS is used to select the IP address for 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 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 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 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 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. The parameter value 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. The parameter value 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. The parameter value 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. The parameter value is case sensitive. This selection is only valid if DHCP is enabled.

REG\_WINS\_SERVER specifies if iLO must be registered with the WINS server. The possible values are Yes or No. The parameter value 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.

DHCP\_SNTP\_SETTINGS is used to determine whether iLO is to get the SNTP time servers and timezone from the DHCP server or whether the user enters that information manually.

SNTP\_SERVER1 specifies the IP address of an IPv4 or IPv6 SNTP server or the FQDN of an SNTP server. The FQDN must adhere to the DNS standard, for example time.nist.gov. The iLO firmware contacts this server for the UTC time. If iLO is unable to contact this server, it attempts to contact the Secondary Time Server. This parameter is only relevant if DHCP\_SNTP\_SETTINGS is set to No. If an empty string is entered, the current value is deleted.

SNTP\_SERVER2 specifies the IP address of an IPv4 or IPv6 SNTP server or the FQDN of an SNTP server. The FQDN must adhere to the DNS standard, for example time.nist.gov. The iLO firmware contacts this server for the UTC time. If iLO cannot contact the Primary Time Server, it contacts this server. This parameter is only relevant if DHCP\_SNTP\_SETTINGS is set to No. If an empty string is entered, the current value is deleted.

TIMEZONE specifies the current time zone from the Olson database. Using a web browser, in iLO 4, go to **Administration**→**Network**→**SNTP Settings** and select the correct time zone from the Timezone list box. The text of the time zone name must be entered exactly as it appears in the SNTP Settings time zone list box, (minus the GMT offset). **America/Anchorage** or **Europe/Zurich** are two examples of a valid time zone.

### IPv6 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.

IPV6\_ADDRESS is used to configure a static IPv6 address on iLO. When IPV6\_ADDRESS entries are included in a script, all previously configured IPv6 static addresses are deleted. Only the addresses specified in the script will be in use by iLO after the script successfully completes. All static address entries on iLO can be cleared by specifying a single blank IPV6\_ADDRESS entry.

- ADDR\_SOURCE may be included for ease in turning around GET\_NETWORK\_SETTINGS output as input to MOD\_NETWORK\_SETTINGS. However, if the value is not **STATIC** the entire entry is ignored.
- ADDR\_STATUS may be included for ease in turning using GET\_NETWORK\_SETTINGS output as input to MOD\_NETWORK\_SETTINGS. The value is always ignored as input.

IPV6\_STATIC\_ROUTE\_[1:3] is used to configure static routes for IPv6 on iLO.

- IPV6\_DEST specifies the destination address prefix, limited by PREFIXLEN. Must be a valid literal IPv6 address in string form.
- IPV6\_GATEWAY specifies the IPv6 address to which the prefixes should be routed. Must be a valid literal IPv6 address in string form.
- ADDR\_STATUS is used for ease in turning GET\_NETWORK\_SETTINGS output around as input to MOD\_NETWORK\_SETTINGS, but is always ignored as input.

---

**NOTE:** To clear a single static route, enter blank addresses ("::") for IPV6\_DEST and IPV6\_GATEWAY, with "0" (zero) PREFIXLEN.

---

IPV6\_PRIM\_DNS\_SERVER, IPV6\_SEC\_DNS\_SERVER, and IPV6\_TER\_DNS\_SERVER are used to specify primary, secondary, and tertiary IPv6 DNS server addresses. Values must be valid literal IPv6 addresses in string form. These addresses are used in addition to the IPv4 DNS server addresses. Clear address entries by specifying blank IPv6 addresses ("::"). When iLO Client applications are configured to prefer IPv6 (see IPV6\_PREFERRED\_PROTOCOL) the order of use will be:

1. IPV6\_PRIM\_DNS\_SERVER
2. PRIM\_DNS\_SERVER
3. IPV6\_SEC\_DNS\_SERVER
4. SEC\_DNS\_SERVER
5. IPV6\_TER\_DNS\_SERVER
6. TER\_DNS\_SERVER

When IPv4 protocol is preferred by iLO clients, the order of IPv6 and IPv4 is reversed for each of primary, secondary, and then tertiary settings respectively.

IPV6\_DEFAULT\_GATEWAY allows you to add an IPv6 address to the default gateway address list maintained by the ILO network stack. This is primarily for environments when no RA (router advertised) messages are present on the network. The value must be a valid literal IPv6 address in string form. Clear address entry by specifying a blank IPv6 address ("::").

IPV6\_ADDR\_AUTOCFG enables or disables RFC 4862 SLAAC (Stateless Address Auto Configuration). Value must be either **Y** (enabled) or **N** (disabled). When enabled, iLO creates IPv6 addresses for itself from RA prefixes as appropriate. When disabled, only the link-local address is automatically configured. Router advertisements are still monitored but not used for SLAAC address creation.

IPV6\_REG\_DDNS\_SERVER enables or disables automatic DNS server IPv6 address registration. Value must be either **Y** (enabled) or **N** (disabled). When enabled, iLO attempts to register AAAA and PTR records for its IPv6 addresses with the DNS server.

IPV6\_PREFERRED\_PROTOCOL enables or disables using IPv6 addresses as preferred. Value must be either **Y** (enabled) or **N** (disabled). When enabled, iLO client applications use IPv6 service addresses before IPv4 service addresses when both are configured. Client applications affected by this setting currently are the DNS name resolver and SNTP. In SNTP, if FQDNs are configured, and the DNS name resolver returns both A (IPv4) and AAAA (IPv6) records, the addresses are tried in order specified by this setting. For the DNS name resolver, if both IPv4 and IPv6 DNS addresses are configured, this setting determines the order of use for the primary addresses, then the secondary addresses, and finally the tertiary addresses.

DHCPV6\_STATELESS\_ENABLE and DHCPV6\_STATEFUL\_ENABLE modifies the operational mode of DHCPv6. The values for both of these parameters can be either **Y** (enabled) or **N** (disabled).

- DHCPV6\_STATEFUL\_ENABLE is analogous to DHCPv4, and enables the configuration of a node address and additional parameters such as NTP server location and time zone.
- DHCPV6\_STATELESS\_ENABLE enables the configuration of parameters such as NTP server location but does not provide for the configuration of a node address. This mode may be used with IPv6 Stateless Address Auto-Configuration (SLAAC) to provide configuration data that cannot otherwise be provided.

DHCPV6\_STATELESS\_ENABLE and DHCPV6\_STATEFUL\_ENABLE work together in a DHCPv6 environment. In most environments, if DHCPV6\_STATEFUL\_ENABLE is enabled (which provides a subset of information available via DHCPV6\_STATEFUL\_ENABLE) this implies that DHCPV6\_STATELESS\_ENABLE should also be enabled. Value must be either **Y** (enabled) or **N** (disabled).

DHCPV6\_RAPID\_COMMIT is used when DHCPV6\_STATEFUL\_ENABLE is enabled. It provides a reduction in the amount of DHCPv6 network traffic needed to assign addresses, but should not be used if more than one DHCPv6 server is present in the network for the purpose of assigning

addresses. DHCPv6 database errors may result if more than one server can assign iLO an IPv6 address and Rapid Commit mode is enabled. Value must be either **Y** (enabled) or **N** (disabled).

DHCPV6\_SNTP\_SETTINGS specifies whether DHCPv6 Stateless-assigned NTP server addresses are used or whether the user enters that information manually. Value must be either **Y** (enabled) or **N** (disabled).

DHCPV6\_DNS\_SERVER specifies whether the DHCPv6 Stateless-assigned DNS server addresses are used. Value must be either **Y** (enabled) or **N** (disabled).

## 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`.

For example:

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

### GET\_GLOBAL\_SETTINGS parameters

None

### GET\_GLOBAL\_SETTINGS runtime errors

None

### GET\_GLOBAL\_SETTINGS return messages

A possible GET\_GLOBAL\_SETTINGS return message is as follows:

```
<GET_GLOBAL_SETTINGS>
  <SESSION_TIMEOUT VALUE="30"/>
  <F8_PROMPT_ENABLED VALUE="Y"/>
  <F8_LOGIN_REQUIRED VALUE="N"/>
  <HTTPS_PORT VALUE="443"/>
  <HTTP_PORT VALUE="80"/>
  <REMOTE_CONSOLE_PORT VALUE="17990"/>
  <VIRTUAL_MEDIA_PORT VALUE="17988"/>
  <SNMP_ACCESS_ENABLED VALUE="Y"/>
  <SNMP_PORT VALUE="161"/>
  <SNMP_TRAP_PORT VALUE="162"/>
  <SSH_PORT VALUE="22"/>
  <SSH_STATUS VALUE="Y"/>
  <SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
  <SERIAL_CLI_SPEED VALUE="9600"/>
  <VSP_LOG_ENABLE VALUE="N"/>
  <MIN_PASSWORD VALUE="8"/>
  <AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
  <RBSU_POST_IP VALUE="Y"/>
  <ENFORCE_AES VALUE="N"/>
</GET_GLOBAL_SETTINGS>
```

## MOD\_GLOBAL\_SETTINGS

The MOD\_GLOBAL\_SETTINGS command modifies 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 Settings privilege to execute this command.

The iLO device (not the server) resets automatically to make changes to port settings effective. Setting the ILO\_FUNCT\_ENABLED to No disables the iLO management functions. If disabled, you must use the iLO Security Override Switch on the server system board and the iLO RBSU (F8 key) to re-enable iLO.

Example 1: Use HPQLOCFG.EXE version 1.00 or later with the following scripts.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <SESSION_TIMEOUT value="0"/>
        <F8_PROMPT_ENABLED value="Yes"/>
        <HTTP_PORT value="80"/>
        <HTTPS_PORT value="443"/>
        <REMOTE_CONSOLE_PORT value="17990"/>
        <MIN_PASSWORD value="8"/>
        <ILO_FUNCT_ENABLED value="Yes"/>
        <VIRTUAL_MEDIA_PORT value="17988"/>
        <F8_LOGIN_REQUIRED value="No"/>
        <SSH_PORT value="22"/>
        <SSH_STATUS value="Yes"/>
        <SERIAL_CLI_STATUS value="3"/>
        <SERIAL_CLI_SPEED value="1"/>
        <RBSU_POST_IP value="Y"/>
        <ENFORCE_AES value="N"/>
        <AUTHENTICATION_FAILURE_LOGGING value="3"/>
        <!-- Firmware support information for next 3 tags: -->
        <!-- iLO 4 - 1.10 or later. -->
        <!-- iLO 3 - None. -->
        <!-- iLO 2 - None. -->
        <SNMP_ACCESS_ENABLED value="N"/>
        <SNMP_PORT value="161"/>
        <SNMP_TRAP_PORT value="162"/>
        <!-- Firmware support information for next 7 tags: -->
        <!-- iLO 4 - 1.20 or later. -->
        <!-- iLO 3 - None. -->
        <!-- iLO 2 - None. -->
        <REMOTE_SYSLOG_ENABLE VALUE="Yes"/>
        <REMOTE_SYSLOG_PORT VALUE="514"/>
        <REMOTE_SYSLOG_SERVER_ADDRESS VALUE="" />
        <ALERTMAIL_ENABLE VALUE="Y"/>
        <ALERTMAIL_EMAIL_ADDRESS VALUE="user@domain.com"/>
        <ALERTMAIL_SENDER_DOMAIN VALUE="domain.com"/>
        <ALERTMAIL_SMTP_SERVER VALUE="smtp.domain.com" />
        <!-- Firmware support information for next tag: -->
        <!-- iLO 4 - 1.30 or later. -->
        <!-- iLO 3 - None. -->
        <!-- iLO 2 - None. -->
        <ALERTMAIL_SMTP_PORT VALUE="25"/>
        <!-- Firmware support information for next tag: -->
        <!-- iLO 4 - 1.20 or later. -->
        <!-- iLO 3 - 1.55 or later. -->
        <!-- iLO 2 - None. -->
        <IPMI_DCMI_OVER_LAN_ENABLED value="y"/>
        <!-- Firmware support information for next tag: -->
        <!-- iLO 4 - 1.20 or later. -->
        <!-- iLO 3 - None. -->
        <!-- iLO 2 - 2.09 or later. -->
        <VSP_LOG_ENABLE VALUE="Y" />
        <!-- Firmware support information for next tag: -->
        <!-- iLO 4 - 1.30 or later. -->
```

```

        <!--      iLO 3 - 1.60 or later.          -->
        <!--      iLO 2 - None.                  -->
        <PROPAGATE_TIME_TO_HOST VALUE="Y" />
    </MOD_GLOBAL_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

As of release iLO 4 version 1.01, the Virtual Serial Port supports automatically enabling and disabling software flow control. By default, this behavior is disabled. You can enable this configuration option using the RIBCL only. To enable this option, execute the following script:

Example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_GLOBAL_SETTINGS>
        <VSP_SOFTWARE_FLOW_CONTROL value="Yes"/>
      </MOD_GLOBAL_SETTINGS>
      <RESET_RIB />
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## MOD\_GLOBAL\_SETTINGS parameters

The following parameters are optional. If you do not specify a parameter, then the parameter value for the specified setting is preserved.

---

**NOTE:** If any port changes are detected, iLO reboots to apply the changes after the script has completed successfully.

---

**SESSION\_TIMEOUT**—Determines the maximum session timeout value in minutes. The accepted values are 0, 15, 30, 60, and 120. A value of 0 specifies infinite timeout.

**F8\_PROMPT\_ENABLED**—Determines if the F8 prompt for ROM-based configuration appears during POST. The possible values are *Yes* or *No*.

**HTTP\_PORT**—Specifies the HTTP port number.

**HTTPS\_PORT**—Specifies the HTTPS (SSL) port number.

**REMOTE\_CONSOLE\_PORT**—Specifies the port used for remote console.

**MIN\_PASSWORD**—Specifies how many characters are required in all user passwords. The value can be from zero to 39 characters.

**ILO\_FUNCT\_ENABLED**—Determines if the Lights-Out functionality is enabled or disabled for iLO. The possible values are *Yes* or *No*. This parameter is case insensitive.

**VIRTUAL\_MEDIA\_PORT**—Specifies the port used for virtual media.

**F8\_LOGIN\_REQUIRED**—Determines if login credentials are required to access the RBSU for iLO. The possible values are *Yes* or *No*.

**ENFORCE\_AES**—Determines if iLO enforces the use of AES/3DES encryption ciphers over the iLO interface, SSH, and XML connections. The possible values are *Yes* or *No*.

---

**NOTE:** When enabling AES/3DES, manually close all other GUI, XML, and CLI connections since remaining sessions may continue to use the non-AES/3DES cipher.

---

**AUTHENTICATION\_FAILURE\_LOGGING**—Specifies logging criteria for failed authentications.

Possible values include:

- **0**—Disabled
- **1**—Enabled (records every authentication failure)
- **2**—Enabled (records every second authentication failure)
- **3**—Enabled (records every third authentication failure: this is the default value.)
- **5**—Enabled (records every fifth authentication failure)

**SSH\_STATUS**—Determines if SSH is enabled. The valid values are **Yes** or **No**, which enable or disable SSH functionality.

**SSH\_PORT**—Specifies the port used for SSH connection on iLO 4. The processor must be reset if this value is changed.

**SERIAL\_CLI\_STATUS**—Specifies the status of the CLI. The possible values include:

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

**SERIAL\_CLI\_SPEED**—Specifies the CLI port speed.

---

**NOTE:** The serial port speed set using this parameter must match the speed of the serial port set in the RBSU.

---

The possible values include:

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

**RBSU\_POST\_IP**—Determines whether the iLO 4 IP address is displayed during server POST process. The valid values are **Y** (enabled) or **N** (disabled).

**SNMP\_ACCESS\_ENABLED**—Determines whether iLO should respond to external SNMP requests. Valid values are **Y** (enabled) or **N** (disabled). If disabled, the iLO Management Engine continues to operate and the information displayed in the iLO web interface is updated, but no alerts are generated and SNMP access is not permitted.

**SNMP\_PORT**—Sets the port used for SNMP communications. The industry standard (default) SNMP port is 161 for SNMP access. Value must be a valid port.

**SNMP\_TRAP\_PORT**—Sets the port to which SNMP traps (alerts) are sent. The industry standard (default) SNMP trap port is 162. Value must be a valid port.

**REMOTE\_SYSLOG\_ENABLE**—Determines whether iLO should send event notification messages to a Syslog server. Valid values are **Y** (enabled) or **N** (disabled)

**REMOTE\_SYSLOG\_PORT**—Sets the port number through which the Syslog server listens.

**REMOTE\_SYSLOG\_SERVER\_ADDRESS**—Sets the IP address, FQDN, IPv6 name, or short name of the server running the Syslog service.

**ALERTMAIL\_ENABLE**—Determines whether iLO should send alert conditions detected independently of the host operating system via email. The valid values are **Y** (enabled) or **N** (disabled).

`ALERTMAIL_EMAIL_ADDRESS`—Sets the destination email address for iLO email alerts. Value must be a single email address no longer than 63 characters, and must be in standard email address format.

`ALERTMAIL_SENDER_DOMAIN`—Sets the domain name to be used in the sender (From) email address. Value is formed by using the iLO name as the hostname and the subject string as the domain name. If this value is left blank or not specified, the iLO domain name is used (which may not be accepted by all SMTP servers.) The maximum string length is 63 characters.

`ALERTMAIL_SMTP_SERVER`—Sets the IP address or DNS name of the SMTP server or the MSA. This server cooperates with the MTA to deliver the email. The maximum string length is 63 characters. Note that the SMTP server specified must support unauthenticated SMTP connections on port 25.

`ALERTMAIL_SMTP_PORT`—Sets the port that the SMTP server uses for unauthenticated SMTP connections. The default value is 25.

`IPMI_DCMI_OVER_LAN_ENABLED`—Determines whether you can send industry-standard IPMI and DCMI commands over the LAN using a client-side application. Server-side IPMI/DCMI applications are still functional even when this setting is disabled. The valid values are `Y` (enabled) or `N` (disabled).

`VSP_LOG_ENABLE`—Determines whether the virtual serial port output from the server is captured. Valid values are `Y` (enabled) or `N` (disabled). The parameter is not case sensitive.

`PROPAGATE_TIME_TO_HOST`—Determines whether iLO sets the system host time to match the iLO time. Valid values are `Y` (enabled) or `N` (disabled). If enabled, the propagation time set occurs whenever the iLO is cold-booted. The parameter is not case sensitive.

## MOD\_GLOBAL\_SETTINGS runtime errors

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.
- The `SNMP_PORT` value specified is invalid. Values supported are between 1 and 65535.
- The `SNMP_PORT` value specified is invalid. This port number cannot be used.
- The `SNMP_PORT` value must not be left blank.
- The `SNMP_TRAP_PORT` value specified is invalid. Values supported are between 1 and 65535.
- The `SNMP_TRAP_PORT` value specified is invalid. This port number cannot be used.
- The `SNMP_TRAP_PORT` value must not be left blank.
- Error while reading or writing SNMP data.
- iLO may not be disabled on this server. This message is sent if `ILO_FUNCT_ENABLED` is set to No and the system is a blade.

Possible MOD\_GLOBAL\_SETTINGS warning messages include:

- SNMP\_ACCESS is disabled, SNMP\_PORT and SNMP\_TRAP\_PORT will not be changed.
- SNMP\_ACCESS is being disabled, SNMP\_PORT and SNMP\_TRAP\_PORT will not be changed.
- SNMP\_ACCESS is disabled, SNMP\_PORT and SNMP\_TRAP\_PORT will not be changed.

## BROWNOUT\_RECOVERY

The BROWNOUT\_RECOVERY command turns the brownout recovery feature on or off. For this command to parse correctly, it must appear within a RIB\_INFO command block, and must appear within a MOD\_GLOBAL\_SETTINGS command block. RIB\_INFO MODE must be set to write. This command requires HPQLOCFG.EXE version 1.00 or later. The user must have the Configure iLO Settings privilege to execute this command.

For example:

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

### BROWNOUT\_RECOVERY parameters

<BROWNOUT\_RECOVERY VALUE="No" />—Disables brownout recovery  
<BROWNOUT\_RECOVERY VALUE="Yes" />—Enables brownout recovery

### BROWNOUT\_RECOVERY runtime errors

None

## GET\_SNMP\_IM\_SETTINGS

The GET\_SNMP\_IM\_SETTINGS command requests the respective iLO SNMP IM settings. For this command to parse correctly, the GET\_SNMP\_IM\_SETTINGS command must appear within a RIB\_INFO command block, and RIB\_INFO MODE can be set to read or write.

For example:

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

### GET\_SNMP\_IM\_SETTINGS parameters

None

### GET\_SNMP\_IM\_SETTINGS runtime errors

None

## GET\_SNMP\_IM\_SETTINGS return messages

A possible GET\_SNMP\_IM\_SETTINGS return message is:

```
<GET_SNMP_IM_SETTINGS>
  <SNMP_ACCESS VALUE="Enable"/>
  <SNMP_ADDRESS_1 VALUE=""/>
  <SNMP_ADDRESS_1_ROCOMMUNITY VALUE=""/>
  <SNMP_ADDRESS_1_TRAPCOMMUNITY_VERSION="" VALUE=""/>
  <SNMP_ADDRESS_2 VALUE=""/>
  <SNMP_ADDRESS_2_ROCOMMUNITY VALUE=""/>
  <SNMP_ADDRESS_2_TRAPCOMMUNITY_VERSION="" VALUE=""/>
  <SNMP_ADDRESS_3 VALUE=""/>
  <SNMP_ADDRESS_3_ROCOMMUNITY VALUE=""/>
  <SNMP_ADDRESS_3_TRAPCOMMUNITY_VERSION="" VALUE=""/>
  <SNMP_V3_ENGINE_ID VALUE=""/>
  <SNMP_PORT VALUE="161"/>
  <SNMP_TRAP_PORT VALUE="162"/>
  <TRAP_SOURCE_IDENTIFIER VALUE="iLO Hostname"/>
  <RIB_TRAPS VALUE="Y"/>
  <OS_TRAPS VALUE="Y"/>
  <COLD_START_TRAP_BROADCAST VALUE="Y"/>
  <SNMP_V1_TRAPS VALUE="Y"/>
  <SNMP_PASSTHROUGH_STATUS VALUE="N"/>
  <WEB_AGENT_IP_ADDRESS VALUE="WIN-DPOHJLI9DO8"/>
  <CIM_SECURITY_MASK VALUE="3"/>
  <SNMP_SYS_CONTACT VALUE=""/>
  <SNMP_SYS_LOCATION VALUE=""/>
  <AGENTLESS_MANAGEMENT_ENABLE VALUE="Y"/>
  <SNMP_SYSTEM_ROLE VALUE=""/>
  <SNMP_SYSTEM_ROLE_DETAIL VALUE=""/>
  <SNMP_USER_PROFILE INDEX="1">
    <SECURITY_NAME VALUE=""/>
    <AUTHN_PROTOCOL VALUE="0"/>
    <AUTHN_PASSPHRASE VALUE=""/>
    <PRIVACY_PROTOCOL VALUE="0"/>
    <PRIVACY_PASSPHRASE VALUE=""/>
  </SNMP_USER_PROFILE>
  <SNMP_USER_PROFILE INDEX="2">
    <SECURITY_NAME VALUE=""/>
    <AUTHN_PROTOCOL VALUE="0"/>
    <AUTHN_PASSPHRASE VALUE=""/>
    <PRIVACY_PROTOCOL VALUE="0"/>
    <PRIVACY_PASSPHRASE VALUE=""/>
  </SNMP_USER_PROFILE>
  <SNMP_USER_PROFILE INDEX="3">
    <SECURITY_NAME VALUE=""/>
    <AUTHN_PROTOCOL VALUE="0"/>
    <AUTHN_PASSPHRASE VALUE=""/>
    <PRIVACY_PROTOCOL VALUE="0"/>
    <PRIVACY_PASSPHRASE VALUE=""/>
  </SNMP_USER_PROFILE>
</GET_SNMP_IM_SETTINGS>
```

## MOD\_SNMP\_IM\_SETTINGS

MOD\_SNMP\_IM\_SETTINGS is used to modify SNMP and Insight Manager settings. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write. The user must have the Configure iLO Settings privilege to execute this command.

For example:

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

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_SNMP_IM_SETTINGS>
      <WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
      <SNMP_ADDRESS_1 value="192.168.125.121"/>
      <SNMP_ADDRESS_2 value="192.168.125.122"/>
      <SNMP_ADDRESS_3 value="192.168.125.123"/>
      <OS_TRAPS value="Yes"/>
      <SNMP_PASSTHROUGH_STATUS value="Yes"/>
      <RIB_TRAPS value="No"/>
      <CIM_SECURITY_MASK value="3"/>
      <!-- Firmware support information for the below tags: -->
      <!-- iLO 4 - All versions. -->
      <!-- iLO 3 - None. -->
      <!-- iLO 2 - None. -->
      <SNMP_ADDRESS_1_ROCOMMUNITY VALUE="public1"/>
      <SNMP_ADDRESS_1_TRAPCOMMUNITY VERSION="v1" VALUE="trapcomm1"/>
      <SNMP_ADDRESS_2_ROCOMMUNITY VALUE="public2"/>
      <SNMP_ADDRESS_2_TRAPCOMMUNITY VERSION="v2c" VALUE="trapcomm2"/>
      <SNMP_ADDRESS_3_ROCOMMUNITY VALUE="public3"/>
      <SNMP_ADDRESS_3_TRAPCOMMUNITY VERSION="1" VALUE="trapcomm3"/>
      <AGENTLESS_MANAGEMENT_ENABLE value="Yes"/>
      <SNMP_SYS_CONTACT VALUE="Mr. System Administrator"/>
      <SNMP_SYS_LOCATION VALUE="HP Data Center, Hockley, TX"/>
      <SNMP_SYSTEM_ROLE VALUE="Brief Role Description [60 characters]"/>
      <SNMP_SYSTEM_ROLE_DETAIL VALUE="Extended role description [500 characters]"/>
      <COLD_START_TRAP_BROADCAST value="No"/>
      <!-- Firmware support information for next tag: -->
      <!-- iLO 4 - 1.10 or later. -->
      <!-- iLO 3 - None. -->
      <!-- iLO 2 - None. -->
      <!-- Acceptable values for TRAP_SOURCE_IDENTIFIER: -->
      <!-- iLO Hostname, OS Hostname -->
      <TRAP_SOURCE_IDENTIFIER value = "iLO Hostname"/>
      <!-- Firmware support information for next tags: -->
      <!-- iLO 4 - 1.20 or later. -->
      <!-- iLO 3 - None. -->
      <!-- iLO 2 - None. -->
      <!-- Acceptable values for AUTHN_PROTOCOL: 0 or 1 -->
      <!-- 0 is for MD5, 1 is for SHA -->
      <!-- Acceptable values for PRIVACY_PROTOCOL: 0 or 1 -->
      <!-- 0 is for DES, 1 is for AES -->
      <SNMP_ACCESS_ENABLED value = "Y"/>
      <SNMP_PORT value="161"/>
      <SNMP_TRAP_PORT value="162"/>
      <SNMP_V1_TRAPS VALUE="Yes"/>
      <SNMP_V3_ENGINE_ID VALUE="0x12345678"/>
      <SNMP_USER_PROFILE INDEX = "1">
        <SECURITY_NAME VALUE="Security Name 1"/>
        <AUTHN_PROTOCOL VALUE="0"/>
        <AUTHN_PASSPHRASE VALUE="Authentication Pass Phrase 1"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="Privacy Pass Phrase 1"/>
      </SNMP_USER_PROFILE>
      <SNMP_USER_PROFILE INDEX = "2">
        <SECURITY_NAME VALUE="Security Name 2"/>
        <AUTHN_PROTOCOL VALUE="0"/>
        <AUTHN_PASSPHRASE VALUE="Authentication Pass Phrase 2"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="Privacy Pass Phrase 20"/>
      </SNMP_USER_PROFILE>
      <SNMP_USER_PROFILE INDEX = "3">
        <SECURITY_NAME VALUE="Security Name 3"/>
        <AUTHN_PROTOCOL VALUE="0"/>
        <AUTHN_PASSPHRASE VALUE="Authentication Pass Phrase 3"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="Privacy Pass Phrase 3"/>
      </SNMP_USER_PROFILE>
    </MOD_SNMP_IM_SETTINGS>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

## MOD\_SNMP\_IM\_SETTINGS parameters

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

SNMP\_ADDRESS\_1, SNMP\_ADDRESS\_2, and SNMP\_ADDRESS\_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address.

SNMP\_ADDRESS\_1\_ROCOMMUNITY, SNMP\_ADDRESS\_2\_ROCOMMUNITY, and SNMP\_ADDRESS\_3\_ROCOMMUNITY configure the SNMP read-only community string. Values can include a community string, optionally followed by an IP address or FQDN.

SNMP\_ADDRESS\_1\_TRAPCOMMUNITY, SNMP\_ADDRESS\_2\_TRAPCOMMUNITY, and SNMP\_ADDRESS\_3\_TRAPCOMMUNITY configures the SNMP trap community string.

OS\_TRAPS determines if the user is allowed to receive SNMP traps that are generated by the operating system. The possible values are `Yes` and `No`. By default, the value is set to `No`.

RIB\_TRAPS determines if the user is allowed to receive SNMP traps that are generated by the RIB. The possible values are `Yes` and `No`. By default, the value is set to `No`.

AGENTLESS\_MANAGEMENT\_ENABLE enables or disables agentless management. Valid values are **Yes** or **No**.

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

SNMP\_PASSTHROUGH\_STATUS determines if iLO can receive and send SNMP requests to and from the host OS. By default, the value is set to `Yes`.

SNMP\_SYS\_CONTACT specifies the system administrator or server owner. The string can be a maximum of 49 characters long, and can include information such as a name, email address, or phone number.

SNMP\_SYS\_LOCATION specifies the physical location of the server. The string can be a maximum of 49 characters long.

SNMP\_SYSTEM\_ROLE describes the server role or function, and can be a maximum of 64 characters long.

SNMP\_SYSTEM\_ROLE\_DETAIL describes specific tasks the server might perform, and can be a maximum of 512 characters long.

CIM\_SECURITY\_MASK accepts the integers 0, 1, or 3. The possible values are:

- **0**—No change
- **1**—None (no data is returned)
- **3**—Enabled

COLD\_START\_TRAP\_BROADCAST specifies whether to broadcast to the subnet broadcast IP address if there are no trap destinations configured for SNMP\_ADDRESS\_1, SNMP\_ADDRESS\_2, or SNMP\_ADDRESS\_3. Valid values are **Yes** or **No**.

TRAP\_SOURCE\_IDENTIFIER allows the substitution of the OS Hostname for the sysName when SNMP traps are generated from iLO. Value must be a valid iLO hostname or OS hostname.

SNMP\_ACCESS\_ENABLED enables SNMP access. Valid values are `Y` (enabled) and `N` (disabled).

SNMP\_PORT sets the port on which SNMP should communicate.

SNMP\_TRAP\_PORT sets the port on which SNMP traps are sent.

SNMP\_V1\_TRAPS sets whether SNMPv1 traps are sent. Valid values are `Y` and `N`.

SNMP\_V3\_ENGINE\_ID sets the unique identifier of an SNMP engine belonging to a SNMP agent entity. Value must be hexadecimal string, between 6 and 32 characters long (for example, 0x01020304abcdef). The value must be an even length, excluding the preceding "0x."

SNMP\_USER\_PROFILE INDEX sets the number (1, 2, or 3) for one of three available user profiles for SNMPv3 authentication, and includes the following:

- SECURITY\_NAME sets the user profile name. Value must be 1 to 32 alphanumeric characters long.
- AUTHN\_PROTOCOL sets the message digest algorithm to use for encoding the authorization passphrase. The message digest is calculated over an appropriate portion of an SNMP message and included as part of the message sent to the recipient. Valid values are 0 (for MD5) or 1 (for SHA).
- AUTHN\_PASSPHRASE sets the passphrase to be used for sign operations. Value must be 8 to 49 characters long.
- PRIVACY\_PROTOCOL sets the encryption algorithm to be used for encoding the privacy passphrase. A portion of an SNMP message is encrypted before transmission. Valid values are 0 (for DES) or 1 (for AES).
- PRIVACY\_PASSPHRASE sets the passphrase used for encrypt operations. Value must be 8 to 49 characters long. If this value is omitted, the value for AUTHN\_PASSPHRASE is used.

## MOD\_SNMP\_IM\_SETTINGS runtime errors

Possible MOD\_SNMP\_IM\_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.
- The TRAP\_SOURCE\_IDENTIFIER value must not be left blank.
- TRAP\_SOURCE\_IDENTIFIER VALUE is too long.
- The value specified is invalid.
- SNMP V1 Traps can not be disabled in SNMP Pass-thru mode.
- SNMP\_V3\_ENGINE VALUE is too long.
- SECURITY\_NAME VALUE is too long.
- AUTHN\_PROTOCOL valid values are 0:MD5 or 1:SHA.
- AUTHN\_PROTOCOL can not be left blank.
- AUTHN\_PASSPHRASE VALUE is too long.
- PRIVACY\_PROTOCOL valid values are 0:DES or 1:AES.
- PRIVACY\_PROTOCOL can not be left blank.
- PRIVACY\_PASSPHRASE VALUE is too long.
- PRIVACY\_PASSPHRASE VALUE needs a minimum of 8 characters.
- INDEX can not be left blank.

## MOD\_ENCRYPT\_SETTINGS

The MOD\_ENCRYPT\_SETTINGS command is used to set the communication settings for the Enterprise Secure Key Manager (ESKM). 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 Settings privilege to execute this command. For example:

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

```

<MOD_ENCRYPT_SETTINGS>
  <ESKM_USER_LOGIN VALUE="username"/>
  <ESKM_PASSWORD VALUE="password"/>
  <ILO_GROUP_NAME VALUE="groupname"/>
  <ESKM_CERT_NAME VALUE="certname"/>
  <ENABLE_REDUNDANCY VALUE = "Y"/>
  <ESKM_PRIMARY_SERVER_ADDRESS VALUE="0.0.0.0"/>
  <ESKM_PRIMARY_SERVER_PORT VALUE="0"/>
  <!-- Secondary Server Address & Port values are optional -->
  <ESKM_SECONDARY_SERVER_ADDRESS VALUE=""/>
  <ESKM_SECONDARY_SERVER_PORT VALUE=""/>
</MOD_ENCRYPT_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

- 
- ❗ **IMPORTANT:** Incorrect or mismatched port settings can disable the ability to connect to the iLO. Verify the values before executing this command.
- 

## MOD\_ENCRYPT\_SETTINGS parameters

ESKM\_USER\_LOGIN is the Local User name with administrator permissions that is configured on the ESKM. This is the ESKM *deployment user*. This parameter is case sensitive and must not be blank.

ESKM\_PASSWORD is the password for the Local User name with administrator permissions that is configured on the ESKM. This parameter is case sensitive and can be a combination of any printable characters.

ESKM\_CERT\_NAME is the name of the local certificate authority certificate in ESKM. It is typically named `Local CA`. HP iLO will retrieve the certificate and use it to authenticate the ESKM server(s) for all transactions going forward.

ILO\_GROUP\_NAME is the Local Group created on the ESKM for use with iLO user accounts and the keys iLO imports into the ESKM. When keys are imported, they are automatically accessible to all devices assigned to the same group.

ENABLE\_REDUNDANCY determines whether redundancy is enabled. Valid values are `Y` (enabled) or `N` (disabled).

ESKM\_PRIMARY\_SERVER\_ADDRESS is the IP address of the main ESKM server. The value must be a valid IP address and must not be blank.

ESKM\_PRIMARY\_SERVER\_PORT is the port on which to communicate with the main ESKM server. The value must be a valid port number from 1 to 65535, and must not be blank.

ESKM\_SECONDARY\_SERVER\_ADDRESS is the IP address of a secondary (backup) ESKM server. The value must be valid IP address, however if this parameter is not used it can be left blank.

ESKM\_SECONDARY\_SERVER\_PORT is the port on which to communicate with the secondary ESKM server. The value must be a valid port number from 1 to 65535, however if this parameter is not used it can be left blank.

## MOD\_ENCRYPT\_SETTINGS runtime errors

Possible MOD\_ENCRYPT\_SETTINGS error messages include:

- The ESKM\_USER\_LOGIN VALUE is too long.
- The ESKM\_USER\_LOGIN VALUE must not be left blank.
- The ESKM\_PASSWORD VALUE is too long.
- The ESKM\_PASSWORD VALUE must not be left blank.
- The ILO\_GROUP\_NAME VALUE is too long.
- The ILO\_GROUP\_NAME VALUE must not be left blank.

- The `ESKM_PRIMARY_SERVER_ADDRESS VALUE` is too long.
- The `ESKM_PRIMARY_SERVER_ADDRESS VALUE` must not be left blank.
- The `ESKM_PRIMARY_SERVER_PORT VALUE` specified is invalid. Values supported are between 1 and 65535.
- The `ESKM_PRIMARY_SERVER_PORT VALUE` must not be left blank.
- The `ESKM_SECONDARY_SERVER_ADDRESS VALUE` is too long.
- The `ESKM_SECONDARY_SERVER_PORT VALUE` specified is invalid. Values supported are between 1 and 65535.

## GET\_ENCRYPT\_SETTINGS

Use the `GET_ENCRYPT_SETTINGS` command to display the current encryption settings for a Lights-out device. For this command to parse correctly, the command must appear within a `RIB_INFO` command block, and `RIB_INFO MODE` must be set to read. For example:

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

### GET\_ENCRYPT\_SETTINGS parameters

None

### GET\_ENCRYPT\_SETTINGS runtime errors

None

### GET\_ENCRYPT\_SETTINGS return messages

Possible `GET_ENCRYPT_SETTINGS` return messages includes:

```
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_ENCRYPT_SETTINGS>
  <ENABLE_REDUNDANCY VALUE="N"/>
  <ESKM_CERT_NAME VALUE=""/>
  <ESKM_PRIMARY_SERVER_ADDRESS VALUE=""/>
  <ESKM_PRIMARY_SERVER_PORT VALUE="0"/>
  <ESKM_SECONDARY_SERVER_ADDRESS VALUE=""/>
  <ESKM_SECONDARY_SERVER_PORT VALUE="0"/>
</GET_ENCRYPT_SETTINGS>
</RIBCL>
```

## UPDATE\_RIB\_FIRMWARE and UPDATE\_FIRMWARE

The `UPDATE_FIRMWARE` or `UPDATE_RIB_FIRMWARE` command copies a specified file to iLO, starts the upgrade process, and reboots the board after the image has been successfully flashed.

Note that the two commands are used to update different components:

- `UPDATE_RIB_FIRMWARE` flashes the iLO firmware.
- `UPDATE_FIRMWARE` flashes the CPLD, Power PIC, and ROM.

---

**NOTE:** Do not use both the UPDATE\_RIB\_FIRMWARE and the UPDATE\_FIRMWARE commands in the same script.

---

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 Settings privilege to execute this command.

Example 1:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Firmware support information for next tag: -->
      <!-- iLO 4 - All versions. For servers with TPM enabled. -->
      <!-- iLO 3 - All versions. For servers with TPM enabled. -->
      <!-- iLO 2 - 1.70 and later. For servers with TPM enabled. -->
      <TPM_ENABLED VALUE="Yes"/>
      <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\x1170\ilo4_100_p90_checked.bin"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

When you send an XML script to update firmware, it verifies the trusted platform module (TPM) configuration status of option ROM measuring. If it is enabled, the iLO firmware returns the same warning message as stated in the web interface. You can add the TPM\_ENABLE command to the script file. HP recommends using XML script syntax to execute firmware updates. To enable the firmware update to continue, you must set TPM\_ENABLE to a value of Y or Yes.

Example 2:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <RIB_INFO MODE="write">
      <TPM_ENABLE ="Yes"/>
      <UPDATE_FIRMWARE IMAGE_LOCATION="<path>\<firmware filename>"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## UPDATE\_FIRMWARE parameters

IMAGE\_LOCATION is the full path file name of the firmware upgrade file.

TPM\_ENABLE enables the firmware to continue updating when the option ROM measuring is enabled. To enable the firmware update to continue, you must set TPM\_ENABLE to a value of Y or Yes.

## UPDATE\_FIRMWARE runtime errors

Possible UPDATE\_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.

- IMAGE\_LOCATION must not be blank.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.

## UPDATE\_LANG\_PACK

The UPDATE\_LANG\_PACK command updates the language of an iLO device with a specified language pack file. Replace USER\_LOGIN and PASSWORD with values appropriate for your environment. 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 Settings privilege to execute this command. For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Firmware support information for next tag:          -->
      <!-- iLO 4 - All versions. For servers with TPM enabled. -->
      <TPM_ENABLED VALUE="Yes"/>
      <UPDATE_LANG_PACK IMAGE_LOCATION="C:\lang_ja_120_p01.lpk"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### UPDATE\_LANG\_PACK parameters

IMAGE\_LOCATION is the full path and file name of the language pack upgrade file.

TPM\_ENABLED enables the language pack to continue updating when the option ROM measuring is enabled. To enable the language update to continue, you must set TPM\_ENABLE to a value of **Y** or **Yes**.

### UPDATE\_LANG\_PACK runtime errors

Possible UPDATE\_LANG\_PACK error messages include:

- IMAGE\_LOCATION cannot be longer than 255 characters.
- The firmware image file is not valid.
- Open flash part failed.
- Flash failed.
- Image is not available or not valid.

## GET\_FW\_VERSION

The GET\_FW\_VERSION command requests the respective iLO firmware information. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to read. The user must have the Configure iLO Settings privilege to execute this command.

For example:

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

### GET\_FW\_VERSION parameters

None

## GET\_FW\_VERSION runtime errors

None

## GET\_FW\_VERSION return messages

The following information is returned within the response:

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

## LICENSE

The LICENSE command activates or deactivates iLO advanced features. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write. The user must have the Configure iLO Settings privilege to execute this command.

📺 To see a video demonstration of LICENSE command, see *Installing an iLO License Key through scripting* at:

<http://www.hp.com/go/ilo/videos>

You do not have to use a licensing key on a ProLiant BL Class server. Advanced features are automatically activated.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <LICENSE>
        <ACTIVATE="1111122222333334444455555"/>
      </LICENSE>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## LICENSE parameters

ACTIVATE followed by a valid KEY value signals the activation of the iLO 4 advanced pack licensing.

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

## LICENSE runtime errors

Possible LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.

## INSERT\_VIRTUAL\_MEDIA

This command notifies iLO of the location of a diskette image. The INSERT\_VIRTUAL\_MEDIA command must display within a RIB\_INFO element, and RIB\_INFO must be in write mode. You must purchase the iLO Advanced license to enable this feature.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!--      Firmware support information for next tag:      -->
      <!--          iLO 4 - All versions.                        -->
      <!--          iLO 3 - All versions.                        -->
      <!--          iLO 2 - All versions.                        -->
      <INSERT_VIRTUAL_MEDIA DEVICE="FLOPPY" IMAGE_URL="http://188.188.188.33/
        images/Floppy/dos.bin" />
      <!--      Firmware support information for next tag:      -->
      <!--          iLO 4 - All versions.                        -->
      <!--          iLO 3 - None.                                -->
      <!--          iLO 2 - None.                                -->
      <!--      <INSERT_VIRTUAL_FLOPPY IMAGE_LOCATION = "c:\tools\test.img"/>
      -->
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### INSERT\_VIRTUAL\_MEDIA parameters

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

IMAGE\_URL specifies the URL for the diskette image. The URL format is as follows:

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

- protocol is mandatory and must be either http or https.
- username:password is optional.
- hostname is mandatory.
- port is optional.
- filename is mandatory.
- cgi-helper is optional. This enables the virtual floppy to be writable.

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

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

For example:

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

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

This command specifies only the location of the image to be used. For the image to be connected to the server, the appropriate BOOT\_OPTION must be specified using the SET\_VM\_STATUS command. If BOOT\_OPTION is set to BOOT\_ONCE and the server is rebooted, any subsequent server reboots eject the image.

## INSERT\_VIRTUAL\_MEDIA runtime errors

The possible INSERT\_VIRTUAL\_MEDIA error messages include:

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

## EJECT\_VIRTUAL\_MEDIA

EJECT\_VIRTUAL\_MEDIA ejects the Virtual Media image if one is inserted. The EJECT\_VIRTUAL\_MEDIA command must display within a RIB\_INFO element and RIB\_INFO must be in write mode. You must purchase the iLO Advanced license to enable this feature.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!--          Firmware support information for next tag:          -->
      <!--          iLO 4 - All versions.                                -->
      <!--          iLO 3 - All versions.                                -->
      <!--          iLO 2 - All versions.                                -->
      <EJECT_VIRTUAL_MEDIA DEVICE="FLOPPY"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## EJECT\_VIRTUAL\_MEDIA parameters

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

## EJECT\_VIRTUAL\_MEDIA runtime errors

Possible EJECT\_VIRTUAL\_MEDIA errors are:

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

## GET\_VM\_STATUS

GET\_VM\_STATUS returns the Virtual Media drive status. This command must display within a RIB\_INFO element.

For example:

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

```

        <!--      Firmware support information for next tag:      -->
        <!--      iLO 4 - All versions.      -->
        <!--      iLO 3 - All versions.      -->
        <!--      iLO 2 - All versions.      -->
        <GET_VM_STATUS DEVICE="FLOPPY"/>
    </RIB_INFO>
</LOGIN>
</RIBCL>

```

## GET\_VM\_STATUS parameters

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

## GET\_VM\_STATUS runtime errors

The possible GET\_VM\_STATUS error is:

An invalid Virtual Media option has been given.

## GET\_VM\_STATUS return messages

The return message displays the current state of the Virtual Media. The VM\_APPLET parameter shows if a virtual media device is already connected through the Integrated Remote Console, Java Integrated Remote Console, or the iLO 4 graphical interface. If the VM\_APPLET = CONNECTED, then the (non-URL based) Virtual Media is already in use and cannot be connected through scriptable Virtual Media or Virtual Media XML commands.

---

**NOTE:** Only URL-based Virtual Media can be connected through scriptable Virtual Media or Virtual Media XML. However, URL-based Virtual Media will display as DISCONNECTED through VM\_APPLET even if an URL-based VM is configured via the iLO, Integrated Remote Console, Java Integrated Remote Console, CLI, or RIBCL.

---

The DEVICE parameter tells which device this return message is for. The BOOT\_OPTION shows the current setting; BOOT\_ALWAYS means that the server always use the Virtual Media device for booting, BOOT\_ONCE means that the server boots to the Virtual Device once and then disconnects the Virtual Media on the subsequent server reboot, and NO\_BOOT means that the Virtual Media does not connect during a server reboot. The WRITE\_PROTECT\_FLAG parameter shows if the Virtual Media image can be written to. The IMAGE\_INSERTED parameter tells if the Virtual Media device is connected via the scriptable Virtual Media or the Virtual Media XML command.

A possible GET\_VM\_STATUS return message is:

```

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

```

---

**NOTE:** If the BOOT\_ONCE boot option is selected, all scriptable virtual media parameters are reset to default settings after the server boots. Specifically BOOT\_OPTION = NO\_BOOT, WRITE\_PROTECT = NO, and IMAGE\_INSERTED = NO.

---

## SET\_VM\_STATUS

The SET\_VM\_STATUS command sets the Virtual Media drive status. This command must appear within a RIB\_INFO element, and RIB\_INFO must be set to write. All the parameters in the command are optional. You must purchase the iLO Advanced license to enable this feature.

For example:

```

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

```

```

<!--      Firmware support information for next tag:      -->
<!--      iLO 4 - All versions.                          -->
<!--      iLO 3 - All versions.                          -->
<!--      iLO 2 - All versions.                          -->
<SET_VM_STATUS DEVICE="FLOPPY">
  <VM_BOOT_OPTION VALUE="BOOT_ONCE"/>
  <VM_WRITE_PROTECT VALUE="YES" />
</SET_VM_STATUS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

## SET\_VM\_STATUS parameters

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

VM\_BOOT\_OPTION specifies the boot option parameter for the Virtual Media. The possible values are BOOT\_ALWAYS, BOOT\_ONCE, or NO\_BOOT. These values control how the Virtual Media device behaves during the boot phase of the server. Setting these values does not affect the current state of the Virtual Media device. These settings only take effect if the Virtual Media device is connected at server boot.

- BOOT\_ALWAYS sets the VM\_BOOT\_OPTION to BOOT\_ALWAYS. The Virtual Media device is always connected during server boot. The Virtual Media device is not connected immediately when the VM\_BOOT\_OPTION is set. The Virtual Media device is connected on the next server boot after setting of the VM\_BOOT\_OPTION.
- BOOT\_ONCE sets the VM\_BOOT\_OPTION to BOOT\_ONCE. The Virtual Media device is connected during the next server boot, but on any subsequent server boots, it does not connect. The BOOT\_ONCE option is intended to boot one time to the Virtual Media device, use that device while the server is running, and then not have the Virtual Media device available on subsequent server reboots. The Virtual Media device is not connected immediately when the VM\_BOOT\_OPTION is set. The Virtual Media device is connected on the next server boot following the setting of the VM\_BOOT\_OPTION. After the server has booted once with the Virtual Media device connected, on the subsequent server reboot, the Virtual Media device does not connect and the following Virtual Media device settings reset to their default values:
  - BOOT\_OPTION=NO\_BOOT
  - IMAGE\_INSERTED = NO
- NO\_BOOT sets the VM\_BOOT\_OPTION to NO\_BOOT. The Virtual Media device is not connected during the next server boot. The Virtual Media device is not disconnected immediately when the VM\_BOOT\_OPTION is set. The Virtual Media device is disconnected on the next server boot following the setting of the VM\_BOOT\_OPTION. After the server has booted, the Virtual Media device does not connect and the following Virtual Media device settings reset to their default values:
  - BOOT\_OPTION = NO\_BOOT
  - IMAGE\_INSERTED = NO

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

- CONNECT sets the VM\_BOOT\_OPTION to CONNECT. The Virtual Media device is immediately connected to the server. Setting the VM\_BOOT\_OPTION to CONNECT is equivalent to clicking the device **Connect** button on the Virtual Media Applet. After setting the

VM\_BOOT\_OPTION to `CONNECT`, the `VM_GET_STATUS` command shows the `VM_BOOT_OPTION` as `BOOT_ALWAYS`. This is by design and shows that the Virtual Media device is connected like the Virtual Media device in the applet which is always connected during all server boots.

- `DISCONNECT` sets the `VM_BOOT_OPTION` to `DISCONNECT`. The Virtual Media device is immediately disconnected from the server. Setting the `VM_BOOT_OPTION` to `DISCONNECT` is equivalent to clicking the device **Disconnect** button on the Virtual Media Applet. Additionally, setting the `VM_BOOT_OPTION` to `DISCONNECT` is equivalent to issuing the `EJECT_VIRTUAL_MEDIA` command. When the `VM_BOOT_OPTION` is set to `DISCONNECT`, the Virtual Media device does not connect and the following Virtual Media device settings are reset to their default values:
  - `BOOT_OPTION = NO_BOOT`
  - `IMAGE_INSERTED = NO`

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

## SET\_VM\_STATUS runtime errors

The possible runtime errors are:

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

## CERTIFICATE\_SIGNING\_REQUEST

This command requests a certificate from iLO. When this command is received, iLO generates a certificate signing request. The request is returned to the user enclosed in a `CERTIFICATE_SIGNING_REQUEST` tag. This command requires `HPQLOCFG.EXE` version 1.00 or later.

You can choose the default, or custom script.

The default response is:

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

The custom response is:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Default -->
      <!-- <CERTIFICATE_SIGNING_REQUEST/> -->
      <!-- Custom CSR -->
      <CERTIFICATE_SIGNING_REQUEST>
        <CSR_STATE VALUE = ""/>
        <CSR_COUNTRY VALUE = "US"/>
        <CSR_LOCALITY VALUE = "Houston"/>
        <CSR_ORGANIZATION VALUE = "Hewlett-Packard Company"/>
      </CERTIFICATE_SIGNING_REQUEST>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

```

        <CSR_ORGANIZATIONAL_UNIT VALUE = ""/>
        <CSR_COMMON_NAME VALUE = "test.com"/>
    </CERTIFICATE_SIGNING_REQUEST>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

## CERTIFICATE\_SIGNING\_REQUEST parameters (for custom CSR)

CSR\_STATE - Specifies state in which the company or organization that owns the iLO subsystem is located.

CSR\_COUNTRY - Specifies the two-character country code for the country in which the company or organization that owns the iLO subsystem is located.

CSR\_LOCALITY - Specifies the city or locality in which the company or organization that owns the iLO subsystem is located.

CSR\_ORGANIZATION - Specifies the name of the company or organization that owns the iLO subsystem.

CSR\_ORGANIZATIONAL\_UNIT - The unit within the company or organization that owns the iLO subsystem

CSR\_COMMON\_NAME - The FQDN of the iLO subsystem.

## CERTIFICATE\_SIGNING\_REQUEST errors

Possible error messages for CERTIFICATE\_SIGNING\_REQUEST for custom CSR scripts include:

- CSR\_STATE is too long.
- Need a value for the CSR\_STATE tag.
- CSR\_COUNTRY is too long.
- Need a value for the CSR\_COUNTRY tag.
- CSR\_LOCALITY is too long.
- Need a value for the CSR\_LOCALITY tag.
- CSR\_ORGANIZATION is too long.
- Need a value for the CSR\_ORGANIZATION tag.
- CSR\_ORGANIZATIONAL\_UNIT is too long.
- CSR\_COMMON\_NAME is too long.
- Need a value for the CSR\_COMMON\_NAME tag.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.

When you first request a new CSR, or if the system is already working on another CSR, you will see this message:

```
The iLO subsystem is currently generating a Certificate Signing Request(CSR), run script after 10 minutes or more to receive the CSR.
```

## IMPORT\_CERTIFICATE

The IMPORT\_CERTIFICATE command imports a signed certificate into iLO. The signed certificate must be a signed version of a certificate signing request. This command requires HPQLOCFG.EXE version 1.00 or later.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN = "adminname" PASSWORD = "password">

```

```

<RIB_INFO MODE = "write">
  <IMPORT_CERTIFICATE>
    <!-- Replace the following text and comments with the certificate -->
    <!-- INCLUDE the full header and full footer of the certificate -->
    <!-- For example: -->
      -----BEGIN CERTIFICATE-----
    <!-- Certificate Data -->
      -----END CERTIFICATE-----
  </IMPORT_CERTIFICATE>
  <!-- The iLO will be reset after the certificate has been imported. -->
  <RESET_RIB/>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

## IMPORT\_CERTIFICATE parameters

None

## IMPORT\_CERTIFICATE errors

The possible IMPORT\_CERTIFICATE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Error reading certificate: The imported certificate is invalid.

## AHS\_CLEAR\_DATA

The AHS\_CLEAR\_DATA command clears the Active Health System information from the AHS log. For this command to parse correctly, the command must appear within a RIB\_INFO command block, and RIB\_INFO MODE must be set to write. Use HPQLOCFG version 1.00 or later when executing this command. The user must have the Configure iLO Settings privilege to execute this command.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Command to clear AHS data. -->
      <AHS_CLEAR_DATA/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## AHS\_CLEAR\_DATA parameters

None

## AHS\_CLEAR\_DATA runtime errors

None

## GET\_AHS\_STATUS

Use the GET\_AHS\_STATUS command to determine whether AHS is enabled or disabled. 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. Use HPQLOCFG version 1.00 or later when executing this command. The user must have the Configure iLO Settings privilege to execute this command.

For example:

```

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

```

## GET\_AHS\_STATUS parameters

None

## GET\_AHS\_STATUS runtime errors

None

## SET\_AHS\_STATUS

Use the SET\_AHS\_STATUS command to enable or disable AHS logging. 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. Use HPQLOCFG version 1.00 or later when executing this command. The user must have the Configure iLO Settings privilege to execute this command.

---

**NOTE:** This command resets the iLO when changing the status. However, if the command results in no status change (for example, if setting the status to `Enable` when the status is already enabled) the iLO will not reset.

---

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Set to "Enable" or "Disable". -->
      <SET_AHS_STATUS="Disable"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## SET\_AHS\_STATUS parameters

None

## SET\_AHS\_STATUS runtime errors

Some possible error messages for SET\_AHS\_STATUS:

- AHS is already enabled.
- AHS is already disabled.

## ERS\_AHS\_Submit.xml (TRIGGER\_BB\_DATA)

Use this script to initiate Active Health System data submission to the Insight Remote Support server. Use HPQLOCFG.EXE ver 1.00 or later with this command. The user must have the Configure iLO Settings privilege to execute this command.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Command to initiate AHS data submission. -->

```

```

    <TRIGGER_BB_DATA>
      <MESSAGE_ID value="nnn . . . nnn"/>
      <BB_DAYS value="n"/>
    </TRIGGER_BB_DATA>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

### ERS\_AHS\_Submit.xml (TRIGGER\_BB\_DATA) parameters

- MESSAGE\_ID is a UUID format used to match the Active Health System package with the request. It is returned in the submission package SOAP envelope header.
- BB\_DAYS is the number of days to include in the transmission, up to a maximum of the last seven days not including the present day. Possible values are **1** to **7**.

### ERS\_AHS\_Submit.xml (TRIGGER\_BB\_DATA) runtime errors

None

## DISABLE\_ERS

Use this command to disable Insight Remote Support functionality and un-register the server. Use HPQLOCFG.EXE ver 1.00 or later with this command.

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Command to disable ERS and unregister the server. -->
      <DISABLE_ERS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

### DISABLE\_ERS parameters

None

### DISABLE\_ERS runtime errors

None

## GET\_ERS\_SETTINGS

Use this command to retrieve the current Insight Remote Support settings. Use HPQLOCFG.EXE ver 1.00 or later with this command.

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <!-- Command to retrieve the current ERS settings. -->
      <GET_ERS_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

### GET\_ERS\_SETTINGS parameters

None

### GET\_ERS\_SETTINGS runtime errors

None

## SET\_ERS\_IRS\_CONNECT

Use this command to connect to the Insight Remote Support server, and to register the server. Use HPQLOCFG.EXE ver 1.00 or later with this command.

```
<RIBCL VERSION="2.22">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Command to connect ERS to IRS and register the server.-->
      <SET_ERS_IRS_CONNECT>
        <ERS_DESTINATION_URL value = "00.0.00.000"/>
        <ERS_DESTINATION_PORT value = "0000"/>
      </SET_ERS_IRS_CONNECT>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### SET\_ERS\_IRS\_CONNECT parameters

ERS\_DESTINATION\_URL—The host name or IP address of IRS server.

ERS\_DESTINATION\_PORT—The port number of the IRS server.

### SET\_ERS\_IRS\_CONNECT runtime errors

None

## TRIGGER\_L2\_COLLECTION

Use this command to initiate an L2 data collection submission to the Insight Remote Support server. Use HPQLOCFG.EXE ver 1.00 or later with this command.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <TRIGGER_L2_COLLECTION>
        <MESSAGE_ID value="nnn . . . nnn"/>
      </TRIGGER_L2_COLLECTION>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### TRIGGER\_L2\_COLLECTION parameters

MESSAGE\_ID—Message UUID format used to match the test Service Event with this request. It is returned in the submission package SOAP envelope header.

### TRIGGER\_L2\_COLLECTION runtime errors

None

## TRIGGER\_TEST\_EVENT

Use this command to initiate a test service event submission to the Insight Remote Support server. Use HPQLOCFG.EXE ver 1.00 or later with this command.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <TRIGGER_TEST_EVENT >
        <MESSAGE_ID value="nnn . . . nnn"/>
      </TRIGGER_TEST_EVENT>
    </RIB_INFO>
  </LOGIN>
```

```
</RIBCL>
```

### TRIGGER\_TEST\_EVENT parameters

MESSAGE\_ID—Message UUID format used to match the test Service Event with this request. It is returned in the submission package SOAP envelope header.

### TRIGGER\_TEST\_EVENT runtime errors

None

## SET\_ERS\_DIRECT\_CONNECT

Enter this command to begin the registration of your device to HP Insight Online using Direct Connect. You must have the Configure iLO Settings privilege to modify iLO Remote Support settings, and a valid HP Passport Account is required to run this command. If you do not have an account, sign up at <http://www.hp.com/go/insightonline>.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <SET_ERS_DIRECT_CONNECT>
        <ERS_HPP_USER_ID value="HpUID"/>
        <ERS_HPP_PASSWORD value="HpPass"/>
        <!-- if proxy is needed, enter the proxy information:
        <ERS_WEB_PROXY_URL value="proxy.sample.hp.com"/>
        <ERS_WEB_PROXY_PORT value="8080"/>
        <ERS_WEB_PROXY_USERNAME value="proxy_user"/>
        <ERS_WEB_PROXY_PASSWORD value="proxy_pass"/> -->
      </SET_ERS_DIRECT_CONNECT>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

After running SET\_ERS\_DIRECT\_CONNECT, a final command is required to complete the registration process. See “DC\_REGISTRATION\_COMPLETE” (page 122) for more information.

### SET\_ERS\_DIRECT\_CONNECT parameters

ERS\_HPP\_USER\_ID—HP Passport Account user ID.

ERS\_HPP\_PASSWORD—HP Passport Account password.

If your device uses a web proxy server to access the Internet, enter the following:

- ERS\_WEB\_PROXY\_URL—Web proxy server host name or IP address.
- ERS\_WEB\_PROXY\_PORT—Port number on which to communicate with the web proxy server.
- ERS\_WEB\_PROXY\_USERNAME—Username for web proxy server authentication.
- ERS\_WEB\_PROXY\_PASSWORD—Password for web proxy server authentication.

---

**NOTE:** You can set your web proxy server configuration separately using the SET\_ERS\_WEB\_PROXY command. Remember to leave the web proxy section of the script commented out if not configuring web proxy settings in the same script as SET\_ERS\_DIRECT\_CONNECT.

---

### SET\_ERS\_DIRECT\_CONNECT runtime errors

Possible error messages returned for this command are:

- Device is already registered.
- HP Passport password entered is incorrect.

- HP Passport account is locked out due to excessive login authentication failures.
- User has reached half the maximum allowed HP Passport login authentication failures.
- HP Passport password has expired.
- Invalid Proxy Settings
- Cannot connect to proxy server.
- Cannot connect to remote host.

## DC\_REGISTRATION\_COMPLETE

To fully register your device, first enter the [SET\\_ERS\\_DIRECT\\_CONNECT](#) command, and then finish registering for Insight Remote Support by using the Direct Connect command `DC_REGISTRATION_COMPLETE`. You must have the Configure iLO Settings privilege to modify iLO Remote Support settings.

For example:

```
<RIBCL VERSION="2.22">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <DC_REGISTRATION_COMPLETE/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### DC\_REGISTRATION\_COMPLETE parameters

None

### DC\_REGISTRATION\_COMPLETE runtime errors

Possible errors messages returned for this command include:

- iLO information is open for read-only access. Write access is required for this operation.
- Internal Error
- Error reading ERS configuration
- ERS is disabled
- Invalid Command For Connect Model

## SET\_ERS\_WEB\_PROXY

Enter the `SET_ERS_WEB_PROXY` command to update the proxy settings for your device, or to configure proxy settings for the first time. You must have the Configure iLO Settings privilege to modify the iLO Remote Support settings.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <SET_ERS_WEB_PROXY>
        <ERS_WEB_PROXY_URL value="192.0.2.10"/>
        <ERS_WEB_PROXY_PORT value="8080"/>
        <ERS_WEB_PROXY_USERNAME value="proxy_user"/>
        <ERS_WEB_PROXY_PASSWORD value="proxy_pass"/>
      </SET_ERS_WEB_PROXY>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

```
</RIB_INFO>
</LOGIN>
</RIBCL>
```

## SET\_ERS\_WEB\_PROXY parameters

To configure your device to use a web proxy server to access the Internet, enter the following:

- ERS\_WEB\_PROXY\_URL—Web proxy server host name or IP address.
- ERS\_WEB\_PROXY\_PORT—Port number on which to communicate with the web proxy server.
- ERS\_WEB\_PROXY\_USERNAME—Username for web proxy server authentication.
- ERS\_WEB\_PROXY\_PASSWORD—Password for web proxy server authentication.

## SET\_ERS\_WEB\_PROXY runtime errors

Possible error messages returned for this command are:

- Invalid Proxy Settings

## SET\_LANGUAGE

Use this command to set the default language on iLO. Use HPQLOCFG.EXE version 1.00 or later with this command.

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

## SET\_LANGUAGE parameters

LANG\_ID is the two letter designation for a language. This parameter is case sensitive, and must not be blank.

Possible values for LANG\_ID are:

- EN (English)
- JA (Japanese)
- ZH (Simplified Chinese)

## SET\_LANGUAGE runtime errors

None

## GET\_LANGUAGE

Use this command to read the default language on iLO. Use HPQLOCFG.EXE version 1.00 or later with this command.

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

## GET\_LANGUAGE parameters

None

## GET\_LANGUAGE runtime errors

None

## GET\_ALL\_LANGUAGES

Use this command to read all languages on iLO. Use HPQLOCFG.EXE version 1.00 or later with this command.

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

## GET\_ALL\_LANGUAGES parameters

None

## GET\_ALL\_LANGUAGES runtime errors

None

## GET\_ASSET\_TAG

Use this command to get the asset tag. Use HPQLOCFG.EXE version 1.00 or later with this command.

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

## GET\_ASSET\_TAG parameters

None

## GET\_ASSET\_TAG runtime errors

- Problem reading the EV—There was a problem reading the EV. Retry the procedure later.
- There is no EV by the name given—The EV is not present. One possible cause is that the EV was never set using SET\_ASSET\_TAG.

When no tag has been set, GET\_ASSET\_TAG returns this informational message:

No Asset Tag Information.

## SET\_ASSET\_TAG

Use this command to set or clear the asset tag. Use HPQLOCFG.EXE version 1.00 or later with this command.

You must have the following privileges to execute this command: Virtual Media, Virtual Power and Reset, Remote Console.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Enter a string to set the asset tag, or an empty string -->
      <!-- to clear the asset tag. -->
      <SET_ASSET_TAG VALUE ="Asset Tag"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## SET\_ASSET\_TAG parameters

SET\_ASSET\_TAG sets or clears the asset tag. Enter a string to add or modify the asset tag, or enter an empty string to clear the asset tag.

## SET\_ASSET\_TAG runtime errors

A possible SET\_ASSET\_TAG error message is:

Problem manipulating EV

This message means that the asset tag was not set. Retry the procedure later.

Other possible error message for SET\_ASSET\_TAG include:

- Post in progress, EV unavailable.
- EV name too large.
- EV data too large.
- There is no such EV.
- EV is not supported.
- EV is not initialized.
- ROM is busy, EV unavailable.
- User does NOT have correct privilege for action. VIRTUAL\_MEDIA\_PRIV required.
- User does NOT have correct privilege for action. RESET\_SERVER\_PRIV required.
- User does NOT have correct privilege for action. REMOTE\_CONS\_PRIV required.
- String too long, maximum string length is 32 characters.

## GET\_SECURITY\_MSG

Use this command to retrieve the security message for the iLO login screen.

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

## GET\_SECURITY\_MSG parameters

None

## GET\_SECURITY\_MSG return messages

The following information is returned with the response:

- SECURITY\_MSG value="Enabled" or "Disabled"
- SECURITY\_MSG\_TEXT:

```
<SECURITY_MSG_TEXT>
  <![CDATA[The security message appears here, set using SET_SECURITY_MESSAGE.]]>
</SECURITY_MSG_TEXT>
```

## GET\_SECURITY\_MSG runtime errors

None

## SET\_SECURITY\_MSG

Use this command to configure the security text message in the iLO Login Banner. The Login Security Banner feature allows you to configure the security banner displayed on the iLO login screen. You need to have configure iLO Setting privileges to make changes to the banner.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <SET_SECURITY_MSG>
        <SECURITY_MSG value="y"/>
        <SECURITY_MSG_TEXT>
          <![CDATA[ message ]]>
        </SECURITY_MSG_TEXT>
      </SET_SECURITY_MSG>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## SET\_SECURITY\_MSG parameters

**SECURITY\_MSG**—Boolean value, must be either **Yes** (enabled) or **No** (disabled). When the value is No, the security message is removed.

**SECURITY\_MSG\_TEXT**—CDATA text message to appear when SECURITY\_MSG is set to Yes. Enter the text of the message between <![CDATA[ and ]]>.

## SET\_SECURITY\_MSG runtime errors

The value for the SECURITY\_MESSAGE parameter must a **Y** or an **N**, otherwise the command reports an error. You may also see this error:

```
User does NOT have correct privilege for action. CONFIG_ILO_PRIV
required.
```

## GET\_SPATIAL

Use this command to get the location information and system data with HP Asset Manager to obtain more precise and complete asset data. Use HPQLOCFG.EXE ver 1.0 or later with this command.

```
<RIBCL VERSION="2.22">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="read">
      <GET_SPATIAL/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_SPATIAL parameters

None

## GET\_SPATIAL return messages

The following response is typical of the data returned:

```
<SPATIAL>
  <PLATFORM>DL/ML</PLATFORM>
  <DISCOVERY_RACK>Supported</DISCOVERY_RACK>
  <DISCOVERY_DATA>Valid</DISCOVERY_DATA>
  <TAG_VERSION>1</TAG_VERSION>
  <RACK_ID>2CJ20500XC</RACK_ID>
  <RACK_ID_PN>BW946A</RACK_ID_PN>
  <RACK_cUUID>00000000-0000-0000-0000-000000000000</RACK_cUUID>
  <RACK_DESCRIPTION>HP I Series 42U Rack Location Option</RACK_DESCRIPTION>
  <RACK_UHEIGHT>42</RACK_UHEIGHT>
  <UPOSITION>6</UPOSITION>
  <ULOCATION>F</ULOCATION>
  <cUUID>00000000-0000-0000-0000-000000000000</cUUID>
  <UHEIGHT>100</UHEIGHT>
  <UOFFSET>0</UOFFSET>
  <DEVICE_UPOSITION>6</DEVICE_UPOSITION>
</SPATIAL>
```

- Discovery Rack Support <DISCOVERY\_RACK>—Whether the rack supports Discovery Services
- Discovery Data Error <DISCOVERY\_DATA>—Whether there was an error during discovery
- Tag Version [TAG\_VERSION]—The rack tag version number
- Rack Identifier [RACK\_ID]—The rack identifier
- Rack Location Discovery Product Part Number [RACK\_ID\_PN]—The rack part number
- Rack Location Discovery Product Description [RACK\_DESCRIPTION]—The rack product name
- Rack U Height [RACK\_UHEIGHT]—The rack height in U rack units. Possible values are between 1–50.
- U Position [UPOSITION]—The vertical U position value, which indicates the rack U where the device is installed. Possible values are between 1–50.
- U Location [ULOCATION]—The side of the rack where the device is installed. Possible values are Back, Front (default), Left, and Right.
- Server UUID [cUUID]—The Universally Unique Identifier of the server.
- <RACK\_cUUID>—UUID of the rack, only present if RACK\_ID AND RACK\_ID\_PN are used.
- Server/Enclosure/Rack U Position <DEVICE\_UPOSITION>—The physical U position of the device (server, enclosure, or rack) only present if UPOSITION is non-zero. Calculated by subtracting the UOFFSET from UPOSITION.

Additional fields are listed depending on the server, enclosure, or chassis type.

- Server/Enclosure/Chassis U Height [UHEIGHT]—The server height in U rack units. Possible values are between 100–5000 in increments of 100.
- Server/Enclosure/Chassis Contacts position U offset [UOFFSET]—Possible values are between 1–50.

### HP ProLiant BL specific data

Bay <BAY>—Server location in the enclosure.

Enclosure UUID <ENCLOSURE\_UUID>—UUID of the enclosure.

## HP ProLiant SL specific data

Bay <BAY>—Server location in the enclosure.

SL Chassis UUID <ENCLOSURE\_UUID>—UUID of the enclosure.

## GET\_SPATIAL runtime errors

Possible GET\_SPATIAL runtime errors include:

- This feature requires an installed license key
- Unknown error.
- Feature not supported

## HOTKEY\_CONFIG

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

Upper or lower case values are automatically changed to the proper case as needed (lower case is changed to upper case if needed, and upper case is changed to lower case if needed.) If you use double or single quotes, it must be different from the delimiter. Specifying a blank string removes the current value.

---

**NOTE:** Each hot key can have up to five selections (for example, CTRL\_T="CTRL,ALT,ESC,F2,F4"). Do not use spaces (" ") in the values; to set a space in a value type SPACE.

---

Use this command to configure hotkeys in iLO 4 v1.10 or later. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

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

## HOTKEY\_CONFIG parameters

The following parameters are optional. If a parameter is not specified, then the parameter value remains as previously set. Separated multiple setting values with commas (see example script above.) Up to five keystrokes can be configured for each hot key.

- CTRL+T
- CTRL+U
- CTRL+V
- CTRL+W
- CTRL+X
- CTRL+Y

## Supported hot keys

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

ESC	F1	-	d	s	BACKSPACE
L_ALT	F2	(	e	t	SYS RQ
R_ALT	F3	)	f	u	1
L_SHIFT	F4	*	g	v	2
R_SHIFT	F5	+	h	w	3
INS	F6	:	l	x	4
DEL	F7	<	i	y	5
HOME	F8	>	k	z	6
END	F9	=	l	;	7
PG UP	F10	[	m	'	8
PG DN	F11	]	n	L_CTRL	9
ENTER	F12	\	o	R_CTRL	0
TAB	SPACE	a	p	NUM PLUS	NONE
BREAK	/	b	q	NUM MINUS	L_GUI
COMMA	.	c	r	SCRL LCK	R_GUI

## HOTKEY\_CONFIG runtime errors

The possible HOTKEY\_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.
- Failed to update the hot key.

## GET\_HOTKEY\_CONFIG

Use this command to retrieve hotkeys available for use in remote console sessions. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

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

## GET\_HOTKEY\_CONFIG parameters

None

## GET\_HOTKEY\_CONFIG runtime errors

A possible GET\_HOTKEY\_CONFIG error message is:

Unable to get the hot keys.

## GET\_HOTKEY\_CONFIG return messages

An example of the information returned with the response:

```
<GET_HOTKEY_CONFIG>
  <CTRL_T VALUE="L_CTRL,L_ALT,ESC,NONE,NONE"/>
  <CTRL_U VALUE="L_SHIFT,F10,F12,NONE,NONE"/>
  <CTRL_V VALUE="NONE,NONE,NONE,NONE,NONE"/>
  <CTRL_W VALUE="NONE,NONE,NONE,NONE,NONE"/>
  <CTRL_X VALUE="NONE,NONE,NONE,NONE,NONE"/>
  <CTRL_Y VALUE="NONE,NONE,NONE,NONE,NONE"/>
</GET_HOTKEY_CONFIG>
```

## PROFILE\_APPLY

You can script automated server configuration packages (deployment settings) to install multiple servers through iLO using PROFILE scripts.

Use PROFILE\_APPLY to apply deployment settings in iLO 4. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

```
<RIBCL VERSION="2.2">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <PROFILE_APPLY>
        <PROFILE_DESC_NAME VALUE="profile_desc_name"/>
        <PROFILE_OPTIONS VALUE="none"/>
        <PROFILE_ACTION VALUE="Stage"/>
      </PROFILE_APPLY>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## PROFILE\_APPLY parameters

---

**NOTE:** All text fields must not contain inner quotes or new-line characters.

---

- PROFILE\_DESC\_NAME is the descriptive name of the profile. The value must be unique on the server, and be a maximum of 27 characters long. Only alphanumeric and underscores are accepted; spaces, periods, and slashes are invalid. An empty string is invalid.
- PROFILE\_OPTIONS is currently unused — always set it to **none**. An empty string is invalid.
- PROFILE\_ACTION is a toggle that controls whether the profile is immediately applied or is staged until the next reboot. Valid values are **Stage** and **Apply\_Now**.

## PROFILE\_APPLY runtime errors

These errors may appear:

- PROFILE\_DESC\_NAME is too long.
- PROFILE\_DESC\_NAME is not valid. Only alphanumeric characters and underscore are allowed.

- PROFILE\_OPTIONS is too long.
- PROFILE\_ACTION is too long.
- Problem manipulating EV
- There are missing parameters in the xml script.
- The PROFILE\_ACTION does not have a valid value.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.
- The value specified is invalid.
- Internal error.
- Retry later.
- Invalid, do not repeat.
- Profile descriptor name is not correct.
- Profile descriptor too large.
- Profile Descriptor is read only or write only.
- Profile descriptor has not been found.
- Profile descriptor is currently unavailable.
- The iLO is not configured for this command.
- Blob Store is not yet initialized.
- Feature not supported
- No data available
- Post in progress, EV unavailable.
- EV name too large.
- EV data too large.
- There is no such EV.
- EV is not supported.
- EV is not initialized.
- ROM is busy, EV unavailable.
- Need a value for the PROFILE\_OPTIONS tag.
- Need a value for the PROFILE\_DESC\_NAME tag.

## PROFILE\_APPLY\_GET\_RESULTS

Use this command to retrieve the results from the PROFILE\_APPLY script. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

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

## PROFILE\_APPLY\_GET\_RESULTS parameters

None

## PROFILE\_APPLY\_GET\_RESULTS runtime errors

These errors may appear:

- The value specified is invalid.
- Internal error.
- Retry later.
- Invalid, do not repeat.
- Profile descriptor name is not correct.
- Profile descriptor too large.
- Profile Descriptor is read only or write only.
- Profile descriptor has not been found.
- Profile descriptor is currently unavailable.
- The iLO is not configured for this command.
- Blob Store is not yet initialized.
- Feature not supported
- No data available

## PROFILE\_DELETE

Use this command to delete a deployment profile. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

```
<RIBCL VERSION="2.2">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <PROFILE_DELETE>
        <PROFILE_DESC_NAME VALUE="profile_desc_name"/>
      </PROFILE_DELETE>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### PROFILE\_DELETE parameters

PROFILE\_DESC\_NAME is the descriptive name of the profile. The value must be unique on the server, and be less than 27 characters long. Only alphanumeric and underscores are accepted; spaces, periods, and slashes are invalid. An empty string is invalid.

### PROFILE\_DELETE runtime errors

These errors may appear:

- PROFILE\_DESC\_NAME is too long.
- PROFILE\_DESC\_NAME is not valid. Only alphanumeric characters and underscore are allowed.
- There are missing parameters in the xml script.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.
- The value specified is invalid.
- Internal error.
- Retry later.

- Invalid, do not repeat.
- Profile descriptor name is not correct.
- Profile descriptor too large.
- Profile Descriptor is read only or write only.
- Profile descriptor has not been found.
- Profile descriptor is currently unavailable.
- The iLO is not configured for this command.
- Blob Store is not yet initialized.
- Feature not supported
- No data available

## PROFILE\_LIST

Use this command to list all the Profile Descriptors and the data stored in them in the perm directory of the blobstore (for example, the values stored in PROFILE\_DESC\_NAME, PROFILE\_NAME, PROFILE\_DESCRIPTION, PROFILE\_SCHEMA, PROFILE\_LINK, and PROFILE\_URL.) Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

---

**NOTE:** A high number of stored profile descriptors may cause a delay as the data is gathered and returned.

---

```
<RIBCL VERSION="2.2">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <PROFILE_LIST/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## PROFILE\_LIST parameters

None

## PROFILE\_LIST runtime errors

These errors may appear:

- The value specified is invalid.
- Internal error.
- Retry later.
- Invalid, do not repeat.
- Profile descriptor name is not correct.
- Profile descriptor too large.
- Profile Descriptor is read only or write only.
- Profile descriptor has not been found.
- Profile descriptor is currently unavailable.
- The iLO is not configured for this command.
- Blob Store is not yet initialized.

- Feature not supported
- No data available

## PROFILE\_DESC\_DOWNLOAD

Use this command to write a deployment profile description, download a specific blob, and write the blob to the blobstore. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

```
<RIBCL VERSION="2.2">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <PROFILE_DESC_DOWNLOAD>
        <PROFILE_DESC_NAME VALUE="profile_desc_name"/>
        <PROFILE_NAME VALUE="profile free form text name"/>
        <PROFILE_DESCRIPTION VALUE="Profile free form text description"/>
        <PROFILE_SCHEMA VALUE="intelligentprovisioning.1.0.0"/>
        <BLOB_NAMESPACE VALUE="perm"/>
        <BLOB_NAME VALUE="internal_unique_name"/>
        <PROFILE_URL VALUE="http(s)://uri_path_to_blob"/>
      </PROFILE_DESC_DOWNLOAD>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

## PROFILE\_DESC\_DOWNLOAD parameters

---

**NOTE:** All text fields must not contain inner quotes or new-line characters.

---

- PROFILE\_DESC\_NAME is the descriptive name of the profile. The value must be unique on the server, and be less than 27 characters long. Only alphanumeric and underscores are accepted — spaces, periods, and slashes are invalid.
- PROFILE\_NAME is the name of the profile. This value is optional, and accepts free-form text. Empty strings are invalid, and the string can be 512 characters long.
- PROFILE\_DESCRIPTION is a description of the profile. This value is optional, and accepts free-form text. Empty strings are invalid.
- PROFILE\_SCHEMA is the schema for which this script is compliant. The value should always be **intelligentprovisioning.1.0.0**. Empty strings are invalid.
- BLOB\_NAMESPACE is an internal iLO storage indicator. Used in conjunction with BLOB\_NAME when PROFILE\_URL is not used.
- BLOB\_NAME is the name iLO will use to store the profile internally. This value can be a maximum of 31 characters long. Only alphanumeric and underscores are accepted; spaces, periods, and slashes are invalid. HP recommends that you use the same value as PROFILE\_DESC\_NAME. Used in conjunction with BLOB\_NAMESPACE when PROFILE\_URL is not used.
- PROFILE\_URL is the URL from which iLO will attempt to download the profile for local storage if BLOB\_NAMESPACE and BLOB\_NAME are not used.

## PROFILE\_DESC\_DOWNLOAD runtime errors

The following errors may appear:

- PROFILE\_DESC\_NAME is too long.
- PROFILE\_DESC\_NAME is not valid. Only alphanumeric characters and underscore are allowed.
- PROFILE\_NAME is too long.

- PROFILE\_DESCRIPTION is too long.
- PROFILE\_SCHEMA is too long.
- There are missing parameters in the xml script.
- Need a value for the PROFILE\_URL tag.
- Need a value for the PROFILE\_DESC\_NAME tag.
- Incorrect url.
- Failed to connect to the url.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.
- The value specified is invalid.
- Internal error.
- Retry later.
- Invalid, do not repeat.
- Profile descriptor name is not correct.
- Profile descriptor too large.
- Profile Descriptor is read only or write only.
- Profile descriptor has not been found.
- Profile descriptor is currently unavailable.
- The iLO is not configured for this command.
- Blob Store is not yet initialized.
- Feature not supported
- No data available

## FIPS\_ENABLE

Use this script to enable the Federal Information Processing Standard **Enforce AES/3DES Encryption** setting, in iLO 4 v1.20 or later. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.



**WARNING!** All active connections (including Remote Console and Virtual Media sessions) to the iLO device are dropped immediately when this script executes.

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

### Disabling FIPS:

To disable FIPS, use the [FACTORY\\_DEFAULTS](#) command.

## FIPS\_ENABLE parameters

None

## FIPS\_ENABLE runtime errors

When running the FIPS\_ENABLE command, FIPS status is checked. If FIPS is already enabled, the following message appears:

```
FIPS is already enabled.
```

## GET\_FIPS\_STATUS

Use this script to retrieve the current **Enforce AES/3DES Encryption** status, in iLO 4 v1.20 or later. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

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

### GET\_FIPS\_STATUS parameters

None

### GET\_FIPS\_STATUS runtime errors

None

### GET\_FIPS\_STATUS return messages

A possible GET\_FIPS\_STATUS return message is:

```
<GET_FIPS_STATUS>
  <FIPS_MODE VALUE="Disabled"/>
</GET_FIPS_STATUS>
```

The value for FIPS\_MODE can be "Enabled" or "Disabled".

## GET\_ALL\_LICENSES

Use the GET\_ALL\_LICENSES command to retrieve license type, key, installation date, and class in iLO 4 v1.20 or later. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

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

### GET\_ALL\_LICENSES parameters

None

### GET\_ALL\_LICENSES runtime errors

None

### GET\_ALL\_LICENSES return messages

A possible GET\_ALL\_LICENSES return message is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
```

```

    MESSAGE='No error'
  />
<GET_ALL_LICENSES>
  <LICENSE>
    <LICENSE_TYPE VALUE= "iLO 4 Advanced"/>
    <LICENSE_KEY VALUE= "<advanced license key value>"/>
    <LICENSE_INSTALL_DATE VALUE="Thu Mar 21 18:47:53 2013"/>
    <LICENSE_CLASS VALUE="FQL"/>
  </LICENSE>
</GET_ALL_LICENSES>
</RIBCL>

```

## FACTORY\_DEFAULTS

Use this command to set the iLO device to factory default settings. Use HPQLOCFG.EXE version 1.00 or later with this command. Replace USER\_LOGIN and PASSWORD values with values that are appropriate for your environment.

**⚠ WARNING!** Resetting an iLO device to factory defaults changes the the DNS name to the default, and the iLO device can be accessed using only the default Administrator user account and default password. Without these defaults, iLO access must be reconfigured using the RBSU.

```

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

```

### FACTORY\_DEFAULTS parameters

None

### FACTORY\_DEFAULTS runtime errors

None

## IMPORT\_SSH\_KEY

The IMPORT\_SSH\_KEY command imports a SSH\_KEY and associated iLO user name into iLO. This command requires HPQLOCFG . EXE version 1.00 or later.

After generating an SSH key using `ssh-keygen`, `puttygen.exe`, or another SSH key generating utility to produce a 1024 bit DSA key, and creating the `key.pub` file, perform the following:

1. Locate the `key.pub` file and insert the contents between

```
-----BEGIN SSH KEY-----
```

and

```
-----END SSH KEY-----.
```

The file begins with the text:

```
ssh-dss .
```

2. At the end of the key, append a space and the name of a valid iLO 4 user name as displayed on the Modify User page. For example:

```
xxx_some text_xxx ASmith.
```

The user name is case-sensitive and must match the case of the iLO 4 user name to associate the SSH key with the correct user.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <IMPORT_SSH_KEY>
        -----BEGIN SSH KEY-----
        ssh-dss
        ASampleKeyAAALftnNE12JR8T8XQqyzqc1tt6FLFRXLRM5PJpOf/IG4hN45
        +x+JbaqkhH+aKqFjlf01NjszHrFN26H1AhWOjY2bEwj2wlJzBMAhXwnPQelQsCnJdf+
        zCzbDn+5Va86+qWxm0lsDEChvZPM6wpjkXvHwuInjxTzOGQTq++vmYlo1/AAAAFQC1M
        FaZjE995QhX9H1DaDzpsVTXvwAAAIA6ec/hAkas2N762jtlHvSuvZaQRzu49D0tjXVI
        pNdJAhTC802505PzkGLf5qhrbDnusc1CvoH7DuxyHjeOUVxbC5wFQBcGF4VnpYZ8nGQ
        Gt9TQ0iUV+NRwn4CR5ESoi63zTJIvKIYZDT2ISeXhF2iU6txjZzdeEm7vQz3slaY3dg
        AAAIAQ46i6FBzJAYXziF/qmWMT4y6SlylOQDAsxPKk7rpxegv8RlTeon/aeL7objb9GQ
        2xnEN5gobaNZxKz2d4/jwg3+qgTDT6V1G+b7+nEI/XHIc717/7oqgiOv4VE3WxN+HE9
        JWsv2jwUpAzRGqJOoojRG/CCru0K+jgTOF/di1o0sw== ASmith
        -----END SSH KEY-----
      </IMPORT_SSH_KEY>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

## IMPORT\_SSH\_KEY parameters

None

## IMPORT\_SSH\_KEY runtime errors

The possible IMPORT\_SSH\_KEY error messages include:

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

## DIR\_INFO

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

DIR\_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

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

For example:

```

<DIR_INFO MODE="read">
..... DIR_INFO commands .....
</DIR_INFO>

```

## 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.

For 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 4 1.01, 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:

- 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_CONTEXT_1 VALUE="CN=Users0,DC=HPRIB0, DC=LABS"/>
<DIR_USER_CONTEXT_2 VALUE="CN=Users1,DC=HPRIB1, DC=LABS"/>
<DIR_USER_CONTEXT_3 VALUE= ""/>
<DIR_USER_CONTEXT_4 VALUE= ""/>
<DIR_USER_CONTEXT_5 VALUE= ""/>
<DIR_USER_CONTEXT_6 VALUE= ""/>
<DIR_USER_CONTEXT_7 VALUE= ""/>
<DIR_USER_CONTEXT_8 VALUE= ""/>
<DIR_USER_CONTEXT_9 VALUE= ""/>
<DIR_USER_CONTEXT_10 VALUE= ""/>
<DIR_USER_CONTEXT_11 VALUE= ""/>
<DIR_USER_CONTEXT_12 VALUE= ""/>
<DIR_USER_CONTEXT_13 VALUE= ""/>
<DIR_USER_CONTEXT_14 VALUE= ""/>
<DIR_USER_CONTEXT_15 VALUE= ""/>
<DIR_ENABLE_GRP_ACCT VALUE= "N"/>
<DIR_GRPACCT1_NAME VALUE= "Administrators"/>
<DIR_GRPACCT1_PRIV VALUE= "1,2,3,4,5,6"/>
<DIR_GRPACCT1_SID VALUE= ""/>
<DIR_GRPACCT2_NAME VALUE= "Authenticated Users"/>
<DIR_GRPACCT2_PRIV VALUE= "6"/>
<DIR_GRPACCT2_SID VALUE= "S-1-5-11"/>
<DIR_KERBEROS_ENABLED VALUE="N"/>
<DIR_KERBEROS_REALM VALUE=""/>
<DIR_KERBEROS_KDC_ADDRESS VALUE= ""/>
<DIR_KERBEROS_KDC_PORT VALUE= "88"/>
</GET_DIR_CONFIG>

```

- 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_CONTEXT_1 VALUE="CN=Users,DC=demo,DC=com"/>
<DIR_USER_CONTEXT_2 VALUE=""/>
<DIR_USER_CONTEXT_3 VALUE=""/>
<DIR_USER_CONTEXT_4 VALUE=""/>
<DIR_USER_CONTEXT_5 VALUE=""/>
<DIR_USER_CONTEXT_6 VALUE=""/>
<DIR_USER_CONTEXT_7 VALUE=""/>
<DIR_USER_CONTEXT_8 VALUE=""/>
<DIR_USER_CONTEXT_9 VALUE=""/>
<DIR_USER_CONTEXT_10 VALUE=""/>
<DIR_USER_CONTEXT_11 VALUE=""/>
<DIR_USER_CONTEXT_12 VALUE=""/>
<DIR_USER_CONTEXT_13 VALUE=""/>
<DIR_USER_CONTEXT_14 VALUE=""/>
<DIR_USER_CONTEXT_15 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_GRPACCT1_SID VALUE="S-1-0"/>
<DIR_KERBEROS_ENABLED VALUE="N"/>
<DIR_KERBEROS_REALM VALUE=""/>
<DIR_KERBEROS_KDC_ADDRESS VALUE=""/>
<DIR_KERBEROS_KDC_PORT VALUE="88"/>
</GET_DIR_CONFIG>

```

- A Kerberos-enabled directory return message:

```

<GET_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE="N"/>
<DIR_LOCAL_USER_ACCT VALUE="Y"/>
<DIR_SERVER_ADDRESS VALUE=""/>
<DIR_SERVER_PORT VALUE="636"/>
<DIR_OBJECT_DN VALUE=""/>
<DIR_USER_CONTEXT_1 VALUE=""/>
<DIR_USER_CONTEXT_2 VALUE=""/>
<DIR_USER_CONTEXT_3 VALUE=""/>
<DIR_USER_CONTEXT_4 VALUE=""/>
<DIR_USER_CONTEXT_5 VALUE=""/>
<DIR_USER_CONTEXT_6 VALUE=""/>
<DIR_USER_CONTEXT_7 VALUE=""/>
<DIR_USER_CONTEXT_8 VALUE=""/>
<DIR_USER_CONTEXT_9 VALUE=""/>
<DIR_USER_CONTEXT_10 VALUE=""/>
<DIR_USER_CONTEXT_11 VALUE=""/>
<DIR_USER_CONTEXT_12 VALUE=""/>
<DIR_USER_CONTEXT_13 VALUE=""/>
<DIR_USER_CONTEXT_14 VALUE=""/>
<DIR_USER_CONTEXT_15 VALUE=""/>
<DIR_ENABLE_GRP_ACCT VALUE="N"/>
<DIR_GRPACCT1_NAME VALUE="Administrators"/>
<DIR_GRPACCT1_PRIV VALUE="1,2,3,4,5,6"/>
<DIR_GRPACCT1_SID VALUE=""/>
<DIR_GRPACCT2_NAME VALUE="Authenticated Users"/>
<DIR_GRPACCT2_PRIV VALUE="6"/>
<DIR_GRPACCT2_SID VALUE="S-1-5-11"/>
<DIR_GRPACCT3_NAME VALUE="user0"/>
<DIR_GRPACCT3_PRIV VALUE="1,2,3,4,5,6"/>
<DIR_GRPACCT3_SID VALUE="S-1-5-21-123456789-123456789-

```

```

1234567890-1234"/>
<DIR_KERBEROS_ENABLED VALUE="Y"/>
<DIR_KERBEROS_REALM VALUE="EXAMPLE.NET"/>
<DIR_KERBEROS_KDC_ADDRESS VALUE= "kdc.example.net"/>
<DIR_KERBEROS_KDC_PORT VALUE= "88"/>
</GET_DIR_CONFIG>

```

## MOD\_DIR\_CONFIG

The MOD\_DIR\_CONFIG command modifies 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 Settings privilege to execute this command.

The MOD\_DIR\_CONFIG is used in different ways depending on the environment. See MOD\_DIRECTORY.XML (example below) for an example suitable for use in an environment with directory integration and existing schemas. See MOD\_SCHEMALESS\_DIRECTORY.XML for an example suitable for use in a schemaless directory configuration.

For 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"/>
        <!-- NOTE: For schemaless Directory configuration, please -->
        <!-- ensure that the following settings are modified as -->
        <!-- required so that user can logon with Email format and -->
        <!-- Netbios formats successfully: -->
        <!-- 1. DIR_SERVER_ADDRESS value need to be set to -->
        <!-- directory server DNS Name or FQDN(Full qualified -->
        <!-- Domain Name) -->
        <!-- Please check and update the following iLO Network -->
        <!-- Settings . -->
        <!-- 1. The domain name of iLO should match the domain of -->
        <!-- the directory server. -->
        <!-- 2. One of the primary, secondary or Tertiary DNS -->
        <!-- server must have the same IP address as the -->
        <!-- Directory server. -->
        <DIR_SERVER_ADDRESS value="dlilo1.mycompu.com"/>
        <DIR_SERVER_PORT value="636"/>
        <DIR_OBJECT_DN value="CN=server1_rib,OU=RIB, DC=mycompu,DC=com"/>
        <DIR_OBJECT_PASSWORD value="password"/>
        <DIR_USER_CONTEXT_1 value="CN=Users,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_2 value="CN=Users2,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_3 value="CN=Users3,DC=mycompu, DC=com"/>
        <!-- Firmware support information for next 12 tags: -->
        <!-- iLO 4 - All versions. -->
        <!-- iLO 3 - All versions. -->
        <!-- iLO 2 - 1.77 and later. -->
        <DIR_USER_CONTEXT_4 value="CN=Users4,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_5 value="CN=Users5,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_6 value="CN=Users6,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_7 value="CN=Users7,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_8 value="CN=Users8,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_9 value="CN=Users9,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_10 value="CN=Users10,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_11 value="CN=Users11,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_12 value="CN=Users12,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_13 value="CN=Users13,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_14 value="CN=Users14,DC=mycompu, DC=com"/>
        <DIR_USER_CONTEXT_15 value="CN=Users15,DC=mycompu, DC=com"/>
        <!--NOTE: Set the value to "NO" to enable the HP Extended -->
        <!-- Schema and Value "YES" to enable Default Directory -->
        <!-- Login. To set Group Accounts and privileges for -->
        <!-- Default Schema run Mod_Schemaless_Directory.xml. -->
        <DIR_ENABLE_GRP_ACCT value = "yes"/>
      </MOD_DIR_CONFIG>
    </DIR_INFO>
  </LOGIN_USER_LOGIN>
</RIBCL>

```

```

<!-- Firmware support information for next 5 tags: -->
<!-- iLO 4 - All versions. -->
<!-- iLO 3 - 1.20 and later. -->
<!-- iLO 2 - None. -->
<DIR_KERBEROS_ENABLED value="Yes"/>
<DIR_KERBEROS_REALM VALUE="realmname.domain.dom"/>
<DIR_KERBEROS_KDC_ADDRESS VALUE="realmkdc.domain.dom"/>
<DIR_KERBEROS_KDC_PORT VALUE="88"/>
<DIR_KERBEROS_KEYTAB>
-----BEGIN KEYTAB-----
VGhpcyBpcyBhIHRlc3Qgb2YgdGhlIEJhc2U2NCBlbmNvZGVyLiAgVGhpcy
BpcyBvbmx5IGEGdGVz
dC4=
-----END KEYTAB-----
</DIR_KERBEROS_KEYTAB>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>

```

---

**NOTE:** To modify only the kerberos authentication, start with the sample script `Mod_Kerberos_Config.xml`.

**NOTE:** Do not use the following tags when using directory integration with schema extension:

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

Do not use the following tags when using schema-free directories:

- `DIR_OBJECT_DN`
  - `DIR_OBJECT_PASSWORD`
- 

### Schemaless directory example (MOD\_SCHEMALESS\_DIR.XML)

```

<!-- RIBCL Sample Script for HP Lights-Out Products -->
<!--Copyright (c) 2003,2011 Hewlett-Packard Development Company, L.P.-->

<!-- Description: This is a sample XML script to modify the current -->
<!-- schemaless directory configuration on following -->
<!-- device: -->
<!-- Integrated Lights-Out 4 (iLO 4) -->
<!-- Integrated Lights-Out 3 (iLO 3) -->
<!-- Integrated Lights-Out 2 (iLO 2) -->

<!-- NOTE: You will need to replace the USER_LOGIN and PASSWORD -->
<!-- values with values that are appropriate for your -->
<!-- environment. -->

<!-- NOTE: Run Mod_directory.xml to enable Directory login, -->
<!-- And to set the directory server address. -->

<!-- The Privilege values are: -->
<!-- 1 = Administer User Accounts -->
<!-- 2 = Remote Console Access -->
<!-- 3 = Virtual Power and Reset -->
<!-- 4 = Virtual Media -->
<!-- 5 = Configure iLO settings -->
<!-- 6 = Login Privilege -->
<!-- Values "6" is supported by iLO 3 and iLO 4 -->
<!-- firmware only. -->

<!-- This script was written for iLO 3 firmware version 1.20 -->
<!-- release. -->

<!-- See "HP Integrated Lights-Out Management Processor -->
<!-- Scripting and Command Line Resource Guide" for more -->
<!-- information on scripting and the syntax of the RIBCL -->
<!-- XML. -->

<!-- Firmware support information for this script: -->

```

```

<!--          iLO 4 - All versions.          -->
<!--          iLO 3 - All versions.          -->
<!--          iLO 2 - Version 1.10 or later.  -->

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="admin" PASSWORD="admin123">
    <DIR_INFO MODE = "write">
      <MOD_DIR_CONFIG>
        <DIR_ENABLE_GRP_ACCT value = "Yes"/>

        <DIR_GRPACCT1_NAME value = "test1"/>
        <DIR_GRPACCT1_PRIV value = "3,4,5"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT1_SID value= "S-1-0"/>

        <DIR_GRPACCT2_NAME value = "test2"/>
        <DIR_GRPACCT2_PRIV value = "2,3,5"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT2_SID value= "S-2-0"/>

        <DIR_GRPACCT3_NAME value = "test3"/>
        <DIR_GRPACCT3_PRIV value = "1,3,4"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT3_SID value= "S-3-0"/>

        <DIR_GRPACCT4_NAME value = "test4"/>
        <DIR_GRPACCT4_PRIV value = "3,6"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT4_SID value= "S-4-0"/>

        <DIR_GRPACCT5_NAME value = "test5"/>
        <DIR_GRPACCT5_PRIV value = "2,3"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT5_SID value= "S-5-0"/>

        <DIR_GRPACCT6_NAME value = "test6"/>
        <DIR_GRPACCT6_PRIV value = "1,3,4,6"/>
        <!--          Firmware support information for next tag:          -->
        <!--          iLO 4 - All versions.          -->
        <!--          iLO 3 - Version 1.20 or later only          -->
        <DIR_GRPACCT6_SID value= "S-6-0"/>

        <!-- alternative method for ilo3/4 only -->
        <!-- <DIR_GRPACCT INDEX="1">          -->
        <!--          <NAME VALUE="string"/>          -->
        <!--          <SID VALUE="S-1-0"/>          -->
        <!--          <LOGIN_PRIV VALUE="Y"/>          -->
        <!-- </DIR_GRPACCT>          -->

      </MOD_DIR_CONFIG>
    </DIR_INFO>
  </LOGIN>
</RIBCL>

```

## MOD\_DIR\_CONFIG parameters

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

DIR\_AUTHENTICATION\_ENABLED enables or disables directory authentication. The possible values are Yes and No.

DIR\_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\_KERBEROS\_ENABLED enables or disables Kerberos authentication. The possible values are Yes and No.

DIR\_KERBEROS\_REALM specifies the Kerberos realm for which the domain controller is configured. By convention, the Kerberos realm name for a given domain is the domain name converted to uppercase.

DIR\_KERBEROS\_KDC\_ADDRESS specifies the location of the domain controller. The domain controller location is specified as an IP address or DNS name.

DIR\_KERBEROS\_KDC\_PORT specifies the port number used to connect to the domain controller. The Kerberos port number is 88, but the domain controller can be configured for a different port number.

DIR\_KERBEROS\_KEYTAB specifies the contents of the keytab file which is a binary file containing pairs of principals and encrypted passwords. In the Windows environment, the keytab file is generated with a ktpass utility. After generating a binary keytab file using the appropriate utility, use a Base64 encoder to convert the binary file to ASCII format.

Place the Base64 contents between:

```
-----BEGIN KEYTAB-----
```

and

```
-----END KEYTAB-----
```

- DIR\_GRPACCT1\_NAME identifies a group container in the directory, such as Administrators, Users, or Power Users.
- DIR\_GRPACCT1\_PRIV numerically identifies 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 (1,2,3,4,5,6) which correlate to:

1—Administer Group Accounts

2—Remote Console Access

3—Virtual Power and Reset

4—Virtual Media

5—Configure iLO 4 Settings

6—Login Privilege

---

**NOTE:** Do not use the following tags when using directory integration with schema extension:

- DIR\_ENABLE\_GRP\_ACCT
- DIR\_GRPACCT1\_NAME
- DIR\_GRPACCT1\_PRIV

Do not use the following tags when using schema-free directories

- 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 4 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 4 object in the directory server. Passwords are limited to 39 characters.

DIR\_USER\_CONTEXT\_1, DIR\_USER\_CONTEXT\_2, and DIR\_USER\_CONTEXT\_15 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user is not 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

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.

## MOD\_KERBEROS

The MOD\_KERBEROS command modifies the directory settings in iLO. For this command to parse correctly, the MOD\_KERBEROS command must appear within a MOD\_DIR\_CONFIG command block, and DIR\_INFO MODE must be set to *write*. The user must have the Configure iLO Settings privilege to execute this command.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="write">
      <MOD_DIR_CONFIG>
        <DIR_KERBEROS_ENABLED value="Yes"/>
        <DIR_KERBEROS_REALM VALUE="realmname.domain.dom"/>
        <DIR_KERBEROS_KDC_ADDRESS VALUE="realmkdc.domain.dom"/>
        <DIR_KERBEROS_KDC_PORT VALUE="88"/>
        <DIR_KERBEROS_KEYTAB>
        -----BEGIN KEYTAB-----
VGhpcyBpcyBhIHRlc3Qgb2YgdGhlIEJhc2U2NCBlbmNvZGVyLiAgVGhpcy
BpcyBvbmx5IGEdGVz
dC4=
        -----END KEYTAB-----
      </DIR_KERBEROS_KEYTAB>
    </MOD_DIR_CONFIG>
  </DIR_INFO>
</LOGIN>
</RIBCL>
```

## RACK\_INFO

The RACK\_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the rack infrastructure database into memory and prepares to edit it. Only commands that are RACK\_INFO type commands are valid inside the RACK\_INFO command block. The RACK\_INFO command generates a response that indicates to the host application whether

the database was successfully read. If the database is open for writing by another application, then this call will fail.

This command block is only valid on ProLiant BL Class Servers, and requires the MODE parameter with a value of read or write. The MODE parameter value is a specific string with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO information. Read mode prevents modification of the iLO information. The possible RACK\_INFO error messages include:

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

For example:

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

## GET\_RACK\_SETTINGS

The GET\_RACK\_SETTING command requests the rack settings for an iLO. For this command to parse correctly, the GET\_RACK\_SETTINGS command must appear within a RACK\_INFO command block, and RACK\_INFO MODE can be set to read or write.

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

### GET\_RACK\_SETTINGS parameters

None

### GET\_RACK\_SETTINGS runtime errors

None

### GET\_RACK\_SETTINGS return messages

A possible GET\_RACK\_SETTINGS return message is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
  <RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
  />
  <GET_RACK_SETTINGS>
    <RACK_NAME VALUE="Don_PowerCap_Rack"/>
    <ENCLOSURE_NAME VALUE="OA-001CC45F6A59"/>
    <ENCLOSURE_SN VALUE="2UX74403NS"/>
    <ENCLOSURE_UUID VALUE="092UX74403NS"/>
    <BAY VALUE="6"/>
    <ENCLOSURE_TYPE VALUE="BladeSystem c3000 Enclosure"/>
  </GET_RACK_SETTINGS>
</RIBCL>
```

## BLADESYSTEM\_INFO

The BLADESYSTEM\_INFO command only appears within a LOGIN command block. Only commands that are BLADESYSTEM\_INFO type commands are valid inside the BLADESYSTEM\_INFO command block.

This command block is only valid on ProLiant BL c-Class blade servers. BLADESYSTEM\_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Write mode enables both reading and writing of information to the blade system. Read mode prevents modification of the blade system information.

The possible BLADESYSTEM\_INFO error messages include:

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

For example:

```
<BLADESYSTEM_INFO MODE="read">
..... BLADESYSTEM_INFO commands .....
</BLADESYSTEM_INFO>
```

## GET\_OA\_INFO

The GET\_OA\_INFO command requests the Onboard Administrator information from the enclosure where iLO 4 is located. For this command to parse correctly, the GET\_OA\_INFO command must appear within a BLADESYSTEM\_INFO command block, and BLADESYSTEM\_INFO MODE can be set to read or write.

For example:

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

### GET\_OA\_INFO parameters

None

### GET\_OA\_INFO runtime errors

None

### GET\_OA\_INFO return messages

A possible GET\_OA\_INFO return message is:

```
<GET_OA_INFO>
<ipAddress>192.168.1.105</ipAddress/>
<macAddress>00:22:44:55:33:77</macAddress/>
<System_Health>1</System_Health>
<uidStatus>On</uidStatus>
<RACK>South Park</RACK>
<ENCL>Kenny</ENCL>
<Location>7</Location>
</GET_OA_INFO>
```

## SERVER\_INFO

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

SERVER\_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

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

For example:

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

Reset server example:

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

Set host power example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Modify the HOST_POWER attribute to toggle power on the host server -->
      <!-- HOST_POWER="No" (Turns host server power off) -->
      <!-- A graceful shutdown will be attempted for ACPI-aware -->
      <!-- operating systems configured to support graceful shutdown. -->
      <!-- HOST_POWER="Yes" (Turns host server power on) -->
      <SET_HOST_POWER HOST_POWER="No"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_TPM\_STATUS

Use GET\_TPM\_STATUS to retrieve the status of the Trusted Platform Module. The response includes whether a TPM is supported, if a TPM is present, and whether the TPM is enabled (indicated by YES or NO). The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

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

### GET\_TPM\_STATUS parameters

None

### GET\_TPM\_STATUS runtime errors

None

### GET\_TPM\_STATUS return messages

A possible GET\_TPM\_STATUS return message includes:

```

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_TPM_STATUS>
  <TPM_SUPPORTED VALUE="Yes">
  <TPM_PRESENT VALUE="Yes">
  <TPM_ENABLED VALUE="Yes">
</GET_TPM_STATUS>

```

## GET\_CURRENT\_BOOT\_MODE

Use GET\_CURRENT\_BOOT\_MODE to retrieve the current boot mode. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read. For example:

```

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

```

Possible return values are LEGACY, UEFI, or UNKNOWN.

### GET\_CURRENT\_BOOT\_MODE parameters

None

### GET\_CURRENT\_BOOT\_MODE runtime errors

None

### GET\_CURRENT\_BOOT\_MODE return messages

A possible GET\_CURRENT\_BOOT\_MODE return message includes:

```

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_CURRENT_BOOT_MODE>
  <BOOT_MODE VALUE="UEFI"/>
</GET_CURRENT_BOOT_MODE>
</RIBCL>

```

## GET\_PENDING\_BOOT\_MODE

Use GET\_PENDING\_BOOT\_MODE to retrieve the pending boot mode, which becomes active on the next server reboot. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

```

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

```

```
</LOGIN>
</RIBCL>
```

Possible return values are LEGACY, UEFI, or UNKNOWN.

## GET\_PENDING\_BOOT\_MODE parameters

None

## GET\_PENDING\_BOOT\_MODE runtime errors

None

## GET\_PENDING\_BOOT\_MODE return messages

```
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_PENDING_BOOT_MODE>
  <BOOT_MODE VALUE="LEGACY"/>
</GET_PENDING_BOOT_MODE></RIBCL>
```

## SET\_PENDING\_BOOT\_MODE

Use SET\_PENDING\_BOOT\_MODE to set the mode for the next server boot. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

For example:

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

## SET\_PENDING\_BOOT\_MODE parameters

SET\_PENDING\_BOOT\_MODE sets the mode for the next server boot. Valid values include **LEGACY** or **UEFI**.

## SET\_PENDING\_BOOT\_MODE runtime errors

Possible error messages include:

- This system is UEFI only.
- This system is Legacy only.
- Unable to determine if system supports UEFI, try again.

## GET\_PERSISTENT\_BOOT

The GET\_PERSISTENT\_BOOT command returns the current boot order, regardless of UEFI or Legacy mode. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

```

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

```

## GET\_PERSISTENT\_BOOT return messages

A possible GET\_PERSISTENT\_BOOT return message when LEGACY is enabled includes:

```

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<PERSISTENT_BOOT>
  <DEVICE value="CDROM"/>
  <DEVICE value="HDD"/>
  <DEVICE value="FLOPPY"/>
  <DEVICE value="USB"/>
  <DEVICE value="NETWORK"/>
</PERSISTENT_BOOT>
</RIBCL>

```

A possible GET\_PERSISTENT\_BOOT return message when UEFI is enabled includes:

```

<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<PERSISTENT_BOOT>
  <DEVICE value="Boot0009" DESCRIPTION="Embedded FlexibleLOM 1 Port 1 : HP
Ethernet 1Gb 4-port 331FLR Adapter - NIC (IPv4) "/>
  <DEVICE value="Boot000A" DESCRIPTION="Front USB 1 : Imation Nano Pro"/>
  <DEVICE value="Boot000D" DESCRIPTION="Windows Boot Manager"/>
  <DEVICE value="Boot0007" DESCRIPTION="Embedded SAS : Smart Array P830i
Controller - 68 GB, RAID 0 Logical Drive(Target:0, Lun:0)"/>
  <DEVICE value="Boot0008" DESCRIPTION="Embedded FlexibleLOM 1 Port 1 : HP
Ethernet 1Gb 4-port 331FLR Adapter - NIC (IPv6) "/>
</PERSISTENT_BOOT>
</RIBCL>

```

## SET\_PERSISTENT\_BOOT (Legacy)

On non-UEFI systems, or UEFI systems in legacy mode, the SET\_PERSISTENT\_BOOT command takes one or more boot parameters and sets the normal boot order. If you do not list every option, the remaining options are shifted toward the bottom of the list. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

**NOTE:** This code modifies EVs. The one time boot EV is:

CQTBT1.

This was modified to set the one-time boot and to display the current status.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">

```

```

    <SERVER_INFO MODE="write">
      <SET_PERSISTENT_BOOT>
        <DEVICE value = "FLOPPY"/>
        <DEVICE value = "CDROM"/>
      </SET_PERSISTENT_BOOT>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>

```

## SET\_PERSISTENT\_BOOT parameters

The value sets the default boot order. Valid values are:

- CDROM
- FlexibleLOM
- EmbeddedLOM
- NIC
- HDD
- SA\_HDD
- USB\_HDD
- PCI\_DEVICE

## SET\_PERSISTENT\_BOOT runtime errors

Some possible error messages you may see when running this command:

- Post in progress, EV unavailable.
- EV name too large.
- EV data too large.
- There is no such EV.
- EV is not supported.
- EV is not initialized.
- ROM is busy, EV unavailable.

## SET\_PERSISTENT\_BOOT (UEFI)

On UEFI systems, the SET\_PERSISTENT\_BOOT command takes one or more UEFI boot parameters and sets the normal boot order. If you do not list every option, the remaining options are shifted toward the bottom of the list. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_PERSISTENT_BOOT>
        <DEVICE value = "Boot0008"/>
        <DEVICE value = "Boot0009"/>
        <DEVICE value = "Boot000A"/>
        <DEVICE value = "Boot000D"/>
      </SET_PERSISTENT_BOOT>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>

```

---

**NOTE:** Before using the SET\_PERSISTENT\_BOOT command in UEFI mode, use GET\_PERSISTENT\_BOOT to retrieve the list of available boot selections. A server in UEFI mode does not have unique selections, as opposed to a non-UEFI server, or a UEFI server running in legacy mode.

---

## SET\_PERSISTENT\_BOOT parameters

Base the parameters sent with the SET\_PERSISTENT\_BOOT command on the BootXXXX values available returned by the GET\_PERSISTENT\_BOOT command. For example, assume the following is returned from the GET command, indicating Boot0009 is the primary boot selection:

```
<PERSISTENT_BOOT>
  <DEVICE value="Boot0009" DESCRIPTION="Embedded FlexibleLOM 1 Port 1 : HP
Ethernet 1Gb 4-port 331FLR Adapter - NIC (IPv4)"/>
  <DEVICE value="Boot000A" DESCRIPTION="Front USB 1 : Imation Nano Pro"/>
  <DEVICE value="Boot000D" DESCRIPTION="Windows Boot Manager"/>
  <DEVICE value="Boot0007" DESCRIPTION="Embedded SAS : Smart Array P830i
Controller - 68 GB, RAID 0 Logical Drive(Target:0, Lun:0)/>
  <DEVICE value="Boot0008" DESCRIPTION="Embedded FlexibleLOM 1 Port 1 : HP
Ethernet 1Gb 4-port 331FLR Adapter - NIC (IPv6)"/>
</PERSISTENT_BOOT>
```

The UEFI boot order is based on the order of the device values. To change the UEFI boot order, for example so that the Windows Boot Manager is first:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_PERSISTENT_BOOT>
        <DEVICE value = "Boot000D"/>
        <DEVICE value = "Boot0009"/>
        <DEVICE value = "Boot000A"/>
        <DEVICE value = "Boot0007"/>
      </SET_PERSISTENT_BOOT>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

Alternatively, you can list only the device value that should be first (<DEVICE value = "Boot000D" />). Any devices not specified in the SET command are moved to the end of the list, just as they are handled in Legacy mode.

---

**NOTE:** The DEVICE values are case sensitive, and must be entered exactly as they are shown in the return from GET\_PERSISTENT\_BOOT.

---

## SET\_PERSISTENT\_BOOT runtime errors

Some possible error messages you may see when running this command:

- DEVICE is invalid.
- Invalid device choice.
- No UEFI Target boot device with the specified BootXXXX is available
- Unable to allocate memory.
- Boot mode is unknown.

## GET\_ONE\_TIME\_BOOT

The GET\_ONE\_TIME\_BOOT command retrieves the current setting for the one time boot. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

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

## GET\_ONE\_TIME\_BOOT return messages

A possible GET\_ONE\_TIME\_BOOT return message includes:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<ONE_TIME_BOOT>
  <BOOT_TYPE VALUE="UEFI_SHELL"/>
</ONE_TIME_BOOT>
</RIBCL>
```

Possible BOOT\_TYPE values include:

- NORMAL
- FLOPPY
- CDROM
- HDD
- USB
- RBSU
- NETWORK
- UEFI\_SHELL
- Intelligent\_Provisioning
- <BootXXXX>

---

**NOTE:** Boot<XXXX> is a possible response on systems that support UEFI and are not in Legacy mode. This type of response also includes a DESCRIPTION, which includes the title of the device and other details.

---

## SET\_ONE\_TIME\_BOOT

The SET\_ONE\_TIME\_BOOT command configures a single boot from a specific device. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

---

**NOTE:** This code modifies EVs.

The one-time boot is accomplished by reading and modifying CQTBT1, CQTBOOTNEXT, and CQTESS, and reading CQHBOOTORDER to determine the valid boot devices.

---

For example:

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

```
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="write">
    <SET_ONE_TIME_BOOT value = "UEFI_SHELL"/>
  </SERVER_INFO>
</LOGIN>
</RIBCL>
```

## SET\_ONE\_TIME\_BOOT parameters

The value sets a specified device as the source for a single boot. Valid values include the following:

- NORMAL
- FLOPPY
- CDROM
- HDD
- USB
- RBSU
- NETWORK
- UEFI\_SHELL

---

**NOTE:** UEFI\_SHELL is only valid on systems that support UEFI.

---

- Intelligent\_Provisioning
- Boot <XXXX>

---

**NOTE:** Boot <XXXX> is only valid on systems that support UEFI and are not in Legacy mode. Use [GET\\_PERSISTENT\\_BOOT](#) to see available values.

---

iLO 4 options:

- EMB-MENU—Displays the default boot menu
- EMB-ACU—Boots into ACU
- EMB-HPSUM-AUTO—Boots HPSUM in automatic update mode
- EMB-DIAGS—Launches Insight Diagnostics for Linux in interactive mode
- RBSU—Boots into the system RBSU.

## SET\_ONE\_TIME\_BOOT runtime errors

Some possible error messages you may see when running this command:

- Post in progress, EV unavailable.
- EV name too large.
- EV data too large.
- There is no such EV.
- EV is not supported.
- EV is not initialized.
- ROM is busy, EV unavailable.
- Unable to determine if system supports UEFI, try again.
- UEFI is not available on this system.

## GET\_SUPPORTED\_BOOT\_MODE

Use GET\_SUPPORTED\_BOOT\_MODE to retrieve the supported boot modes. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

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

Possible values returned include:

- LEGACY\_ONLY
- UEFI\_ONLY
- LEGACY\_UEFI
- UNKNOWN

## GET\_SUPPORTED\_BOOT\_MODE return messages

A possible GET\_SUPPORTED\_BOOT\_MODE return message includes:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_SUPPORTED_BOOT_MODE>
  <SUPPORTED_BOOT_MODE VALUE="LEGACY_ONLY"/>
</GET_SUPPORTED_BOOT_MODE>
</RIBCL>
```

## GET\_SUPPORTED\_BOOT\_MODE runtime errors

None

## GET\_SERVER\_NAME

Use GET\_SERVER\_NAME command to retrieve the host server name used by iLO.

For example:

```
<RIBCL version="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="READ" >
      <GET_SERVER_NAME />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

The iLO firmware maintains consistency between the various places the server name is used. The host RBSU has a two-line limitation of 14 characters each, or 28 characters of total server name text length.

Normally, HP ProLiant Management Agents are used to forward the server name attribute to iLO. This command can be used in instances where management agents are not used. However, the host operating system remains unaffected.

### GET\_SERVER\_NAME return message

GET\_SERVER\_NAME returns the currently stored server name, operating system name, and the operating system version, if available. The server name is a quoted ASCII string and cannot be a network name.

For example:

```
<SERVER_NAME VALUE="WIN-DPOHJLI9DO8" />
<SERVER_OSNAME VALUE="Windows Server 2008 R2, x64 Enterprise Edition
Service Pack 1"/>
<SERVER_OSVERSION VALUE="6.1"/>
```

### GET\_SERVER\_NAME runtime errors

None

## SERVER\_NAME

The SERVER\_NAME command is used to assign the Server Name attribute shown in the user interface and host RBSU. This setting is not forwarded to the host operating system and does not affect the host operating system.

You must have the Configure iLO Settings privilege to change this attribute using the scripting interface. The SERVER\_INFO section must be set to WRITE mode or an error is returned.

For example:

```
<RIBCL version="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="write" >
      <SERVER_NAME VALUE = "Exchange05" />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

### SERVER\_NAME parameters

VALUE is a quoted ASCII string less than 50 characters in total length.

### SERVER\_NAME return message

If this attribute is successfully set, no specific message returns.

### SERVER\_NAME runtime errors

- If the configure iLO settings privilege is absent, a runtime error is returned.
- If SERVER\_INFO is not opened for write, a runtime error is returned.

## GET\_SERVER\_FQDN/GET\_SMH\_FQDN

The GET\_SERVER\_FQDN and GET\_SMH\_FQDN commands are used to retrieve the fully qualified domain name of the server and HP System Management Homepage (HP SMH).

For example:

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

```

        <GET_SERVER_FQDN />
        <GET_SMH_FQDN />
    </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## GET\_SERVER\_FQDN/GET\_SMH\_FQDN parameters

None

## GET\_SERVER\_FQDN/GET\_SMH\_FQDN return messages

A typical response for these commands might include the following:

```

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
    />
<SERVER_FQDN VALUE="server.example.com" />
</RIBCL>

```

```

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
    />
<SMH_FQDN VALUE="192.168.2.153" />
</RIBCL>

```

## SERVER\_FQDN/SMH\_FQDN

The commands `SERVER_FQDN` and `SMH_FQDN` set the fully qualified domain names for the server and the System Management Homepage. IP addresses are also accepted. This allows you to place the system management homepage at a separate FQDN or IP address from the server. You must have the Configure iLO Settings privilege to change this attribute using the scripting interface. The `SERVER_INFO` section must be set to `WRITE` mode or an error is returned.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SERVER_FQDN value="server.example.com" />
      <SMH_FQDN value="192.168.2.153" />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>

```

## SERVER\_FQDN/SMH\_FQDN parameters

`SERVER_FQDN`—Value must be the FQDN or IP address of the host server.

`SMH_FQDN`—Value must be the FQDN or IP address of the server hosting the SMH.

## SERVER\_FQDN/SMH\_FQDN return messages

If the attributes are successfully set, no specific messages return.

## SERVER\_FQDN/SMH\_FQDN runtime errors

- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.

## GET\_PRODUCT\_NAME

The GET\_PRODUCT\_NAME command returns the name and model of the queried server. The specified user must have a valid iLO account to execute RIBCL commands. For this command to parse correctly, the command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

For example:

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

## GET\_PRODUCT\_NAME parameters

USER\_LOGIN is the login name of the user account. This parameter is case sensitive and must not be blank.

## GET\_PRODUCT\_NAME runtime errors

Possible GET\_PRODUCT\_NAME error messages include:

- User login name must not be blank.
- User login name was not found.
- Record not found or bad input.

## GET\_PRODUCT\_NAME return messages

A possible GET\_PRODUCT\_NAME return message includes:

```
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_PRODUCT_NAME>
  <PRODUCT_NAME VALUE ="ProLiant BL420c Gen8"/>
</GET_PRODUCT_NAME>
</RIBCL>
```

## GET\_EMBEDDED\_HEALTH

The GET\_EMBEDDED\_HEALTH command is used to retrieve server health information. For this command to parse correctly, the GET\_EMBEDDED\_HEALTH command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read.

For example:

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

```
</LOGIN>
</RIBCL>
```

An expanded version is also available (see example below). Not all tags are required, however if no tags are specified then the command operates as if all the tags are listed and outputs all of the embedded health data:

```
<RIBCL VERSION="2.22">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="read">
      <GET_EMBEDDED_HEALTH>
        <GET_ALL_FANS/>
        <GET_ALL_TEMPERATURES/>
        <GET_ALL_POWER_SUPPLIES/>
        <GET_ALL_VRM/>
        <GET_ALL_PROCESSORS/>
        <GET_ALL_MEMORY/>
        <GET_ALL_NICS/>
        <GET_ALL_STORAGE/>
        <GET_ALL_HEALTH_STATUS/>
        <!-- Following tag is for iLO 4 1.30 or later. -->
        <GET_ALL_FIRMWARE_VERSIONS/>
      </GET_EMBEDDED_HEALTH>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## GET\_EMBEDDED\_HEALTH parameters

None

## GET\_EMBEDDED\_HEALTH return messages

---

**NOTE:** PART NUMBER (for MEMORY\_DETAILS) is only returned for HP Smart Memory.

---

A possible GET\_EMBEDDED\_HEALTH return message is:

```
<GET_EMBEDDED_HEALTH>
  <FANS>
    <FAN>
      <ZONE VALUE = "System"/>
      <LABEL VALUE = "Virtual Fan"/>
      <STATUS VALUE = "OK"/>
      <SPEED VALUE = "20" UNIT="Percentage"/>
    </FAN>
  </FANS>
  <TEMPERATURE>
    <TEMP>
      <LABEL VALUE = "01-Inlet Ambient"/>
      <LOCATION VALUE = "Ambient"/>
      <STATUS VALUE = "OK"/>
      <CURRENTREADING VALUE = "16" UNIT="Celsius"/>
      <CAUTION VALUE = "42" UNIT="Celsius"/>
      <CRITICAL VALUE = "46" UNIT="Celsius"/>
    </TEMP>
    <TEMP>
      <LABEL VALUE = "02-CPU 1"/>
      <LOCATION VALUE = "CPU"/>
      <STATUS VALUE = "OK"/>
      <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
      <CAUTION VALUE = "70" UNIT="Celsius"/>
      <CRITICAL VALUE = "N/A"/>
    </TEMP>
    <TEMP>
      <LABEL VALUE = "03-CPU 2"/>
      <LOCATION VALUE = "CPU"/>
      <STATUS VALUE = "OK"/>
      <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
      <CAUTION VALUE = "70" UNIT="Celsius"/>
      <CRITICAL VALUE = "N/A"/>
    </TEMP>
  </TEMPERATURE>
```

```

<TEMP>
  <LABEL VALUE = "04-P1 DIMM 1-6"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "24" UNIT="Celsius"/>
  <CAUTION VALUE = "87" UNIT="Celsius"/>
  <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "05-P2 DIMM 1-6"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "23" UNIT="Celsius"/>
  <CAUTION VALUE = "87" UNIT="Celsius"/>
  <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "06-P1 Mem Zone"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "24" UNIT="Celsius"/>
  <CAUTION VALUE = "90" UNIT="Celsius"/>
  <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "07-P1 Mem Zone"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "24" UNIT="Celsius"/>
  <CAUTION VALUE = "90" UNIT="Celsius"/>
  <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "08-P2 Mem Zone"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "22" UNIT="Celsius"/>
  <CAUTION VALUE = "90" UNIT="Celsius"/>
  <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "09-P2 Mem Zone"/>
  <LOCATION VALUE = "Memory"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "22" UNIT="Celsius"/>
  <CAUTION VALUE = "90" UNIT="Celsius"/>
  <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "10-HD Max"/>
  <LOCATION VALUE = "System"/>
  <STATUS VALUE = "Not Installed"/>
  <CURRENTREADING VALUE = "N/A"/>
  <CAUTION VALUE = "N/A"/>
  <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "11-Chipset"/>
  <LOCATION VALUE = "System"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "44" UNIT="Celsius"/>
  <CAUTION VALUE = "105" UNIT="Celsius"/>
  <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "12-VR P1"/>
  <LOCATION VALUE = "Power Supply"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "25" UNIT="Celsius"/>
  <CAUTION VALUE = "115" UNIT="Celsius"/>
  <CRITICAL VALUE = "120" UNIT="Celsius"/>
</TEMP>
<TEMP>
  <LABEL VALUE = "13-VR P2"/>
  <LOCATION VALUE = "Power Supply"/>
  <STATUS VALUE = "OK"/>
  <CURRENTREADING VALUE = "23" UNIT="Celsius"/>
  <CAUTION VALUE = "115" UNIT="Celsius"/>
  <CRITICAL VALUE = "120" UNIT="Celsius"/>
</TEMP>
<TEMP>

```

```

    <LABEL VALUE = "14-VR P1 Zone"/>
    <LOCATION VALUE = "Power Supply"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "28" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "15-VR P1 Mem"/>
    <LOCATION VALUE = "Power Supply"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "25" UNIT="Celsius"/>
    <CAUTION VALUE = "115" UNIT="Celsius"/>
    <CRITICAL VALUE = "120" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "16-VR P2 Mem"/>
    <LOCATION VALUE = "Power Supply"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "21" UNIT="Celsius"/>
    <CAUTION VALUE = "115" UNIT="Celsius"/>
    <CRITICAL VALUE = "120" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "17-SuperCap Max"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "18-HD controller"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
    <CAUTION VALUE = "100" UNIT="Celsius"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "19-HDcntl Inlet"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
    <CAUTION VALUE = "70" UNIT="Celsius"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "20-Mezz 1"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "21-Mezz 1 Inlet"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "22-Mezz 2"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "23-Mezz 2 Inlet"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "24-IOM Card"/>

```

```

        <LOCATION VALUE = "I/O Board"/>
        <STATUS VALUE = "Not Installed"/>
        <CURRENTREADING VALUE = "N/A"/>
        <CAUTION VALUE = "N/A"/>
        <CRITICAL VALUE = "N/A"/>
    </TEMP>
<TEMP>
    <LABEL VALUE = "25-LOM Card Zone"/>
    <LOCATION VALUE = "I/O Board"/>
    <STATUS VALUE = "Not Installed"/>
    <CURRENTREADING VALUE = "N/A"/>
    <CAUTION VALUE = "N/A"/>
    <CRITICAL VALUE = "N/A"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "26-I/O Zone"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "27" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "28-I/O Zone"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "31" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "29-I/O Zone"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "30" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "30-System Board"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "27" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "31-System Board"/>
    <LOCATION VALUE = "System"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "20" UNIT="Celsius"/>
    <CAUTION VALUE = "90" UNIT="Celsius"/>
    <CRITICAL VALUE = "95" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "32-Sys Exhaust"/>
    <LOCATION VALUE = "Chassis"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "26" UNIT="Celsius"/>
    <CAUTION VALUE = "80" UNIT="Celsius"/>
    <CRITICAL VALUE = "85" UNIT="Celsius"/>
</TEMP>
<TEMP>
    <LABEL VALUE = "33-Sys Exhaust"/>
    <LOCATION VALUE = "Chassis"/>
    <STATUS VALUE = "OK"/>
    <CURRENTREADING VALUE = "29" UNIT="Celsius"/>
    <CAUTION VALUE = "80" UNIT="Celsius"/>
    <CRITICAL VALUE = "85" UNIT="Celsius"/>
</TEMP>
</TEMPERATURE>
<POWER_SUPPLIES>
    <POWER_SUPPLY_SUMMARY>
        <PRESENT_POWER_READING VALUE = "117 Watts"/>
        <POWER_MANAGEMENT_CONTROLLER_FIRMWARE_VERSION VALUE = "3.1"/>
        <POWER_SYSTEM_REDUNDANCY VALUE = "Not Redundant"/>
        <HP_POWER_DISCOVERY_SERVICES_REDUNDANCY_STATUS VALUE = "Not Redundant"/>
        <HIGH EFFICIENCY MODE VALUE = "Balanced"/>
    </POWER_SUPPLY_SUMMARY>
    <SUPPLY>
        <LABEL VALUE = "Power Supply 1"/>

```

```

    <PRESENT VALUE = "Yes"/>
    <STATUS VALUE = "Input Voltage Lost"/>
    <PDS VALUE = "Yes"/>
    <HOTPLUG_CAPABLE VALUE = "Yes"/>
    <MODEL VALUE = "656364-B21"/>
    <SPARE VALUE = "660185-001"/>
    <SERIAL_NUMBER VALUE = "5BXRK0BLL2C0CK"/>
    <CAPACITY VALUE = "1200 Watts"/>
    <FIRMWARE_VERSION VALUE = "1.00"/>
</SUPPLY>
<SUPPLY>
  <LABEL VALUE = "Power Supply 2"/>
  <PRESENT VALUE = "Yes"/>
  <STATUS VALUE = "Good, In Use"/>
  <PDS VALUE = "Yes"/>
  <HOTPLUG_CAPABLE VALUE = "Yes"/>
  <MODEL VALUE = "656364-B21"/>
  <SPARE VALUE = "660185-001"/>
  <SERIAL_NUMBER VALUE = "5BXRK0BLL2C0CK"/>
  <CAPACITY VALUE = "1200 Watts"/>
  <FIRMWARE_VERSION VALUE = "1.00"/>
</SUPPLY>
<POWER_DISCOVERY_SERVICES_IPDU_SUMMARY>
  <IPDU>
    <BAY VALUE = "2"/>
    <STATUS VALUE = "IPDU Not Redundant"/>
    <PART_NUMBER VALUE = "AF522A"/>
    <SERIAL_NUMBER VALUE = "2CJ0221672"/>
    <MAC_ADDRESS VALUE = "d8:d3:85:6d:36:9c"/>
    <IPDU_LINK VALUE = "http://16.85.177.189"/>
  </IPDU>
</POWER_SUPPLIES>
<VRM>
</VRM>
<PROCESSORS>
  <PROCESSOR>
    <LABEL VALUE = "Proc 1"/>
    <NAME VALUE = " Intel(R) Xeon(R) CPU E5-2470 0 @ 2.30GHz "/>
    <STATUS VALUE = "OK"/>
    <SPEED VALUE = "2300 MHz"/>
    <EXECUTION_TECHNOLOGY VALUE = "8/8 cores; 16 threads"/>
    <MEMORY_TECHNOLOGY VALUE = "64-bit Capable"/>
    <INTERNAL_L1_CACHE VALUE = "256 KB"/>
    <INTERNAL_L2_CACHE VALUE = "2048 KB"/>
    <INTERNAL_L3_CACHE VALUE = "20480 KB"/>
  </PROCESSOR>
  <PROCESSOR>
    <LABEL VALUE = "Proc 2"/>
    <NAME VALUE = " Intel(R) Xeon(R) CPU E5-2470 0 @ 2.30GHz "/>
    <STATUS VALUE = "OK"/>
    <SPEED VALUE = "2300 MHz"/>
    <EXECUTION_TECHNOLOGY VALUE = "8/8 cores; 16 threads"/>
    <MEMORY_TECHNOLOGY VALUE = "64-bit Capable"/>
    <INTERNAL_L1_CACHE VALUE = "256 KB"/>
    <INTERNAL_L2_CACHE VALUE = "2048 KB"/>
    <INTERNAL_L3_CACHE VALUE = "20480 KB"/>
  </PROCESSOR>
</PROCESSORS>
<MEMORY>
  <ADVANCED_MEMORY_PROTECTION>
    <AMP_MODE_STATUS VALUE = "Advanced ECC"/>
    <CONFIGURED_AMP_MODE VALUE = "Advanced ECC"/>
    <AVAILABLE_AMP_MODES VALUE = "On-line Spare, Advanced ECC"/>
  </ADVANCED_MEMORY_PROTECTION>
  <MEMORY_DETAILS_SUMMARY>
    <CPU_1>
      <NUMBER_OF_SOCKETS VALUE = "6"/>
      <TOTAL_MEMORY_SIZE VALUE = "2 GB"/>
      <OPERATING_FREQUENCY VALUE = "1333 MHz"/>
      <OPERATING_VOLTAGE VALUE = "N/A"/>
    </CPU_1>
    <CPU_2>
      <NUMBER_OF_SOCKETS VALUE = "6"/>
      <TOTAL_MEMORY_SIZE VALUE = "2 GB"/>
      <OPERATING_FREQUENCY VALUE = "1333 MHz"/>
      <OPERATING_VOLTAGE VALUE = "N/A"/>
    </CPU_2>
  </MEMORY_DETAILS_SUMMARY>
<MEMORY_DETAILS>
  <CPU_1>
    <SOCKET VALUE = "1"/>

```

```

        <STATUS VALUE = "Good, In Use"/>
        <HP_SMART_MEMORY VALUE = "Yes"/>
    <PART NUMBER = "647647-071"/>
        <TYPE VALUE = "DIMM DDR3"/>
        <SIZE VALUE = "2048 MB"/>
        <FREQUENCY VALUE = "1333 MHz"/>
        <MINIMUM_VOLTAGE VALUE = "1.50 v"/>
        <RANKS VALUE = "2"/>
        <TECHNOLOGY VALUE = "RDIMM"/>
</CPU_1>
<CPU_1>
    <SOCKET VALUE = "2"/>
    <STATUS VALUE = "Good, In Use"/>
    <HP_SMART_MEMORY VALUE = "Yes"/>
    <PART NUMBER = "647647-071"/>
        <TYPE VALUE = "DIMM DDR3"/>
        <SIZE VALUE = "4096 MB"/>
        <FREQUENCY VALUE = "1333 MHz"/>
        <MINIMUM_VOLTAGE VALUE = "1.35 v"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "RDIMM"/>
</CPU_1>
<CPU_1>
    <SOCKET VALUE = "3"/>
    <STATUS VALUE = "Good, In Use"/>
    <HP_SMART_MEMORY VALUE = "No"/>
    <PART NUMBER = "N/A"/>
        <TYPE VALUE = "DIMM DDR3"/>
        <SIZE VALUE = "4096 MB"/>
        <FREQUENCY VALUE = "1600 MHz"/>
        <MINIMUM_VOLTAGE VALUE = "1.50 v"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "RDIMM"/>
</CPU_1>
<CPU_1>
    <SOCKET VALUE = "4"/>
    <STATUS VALUE = "Not Present"/>
    <HP_SMART_MEMORY VALUE = "No"/>
    <TYPE VALUE = "N/A"/>
    <SIZE VALUE = "N/A"/>
    <FREQUENCY VALUE = "N/A"/>
    <MINIMUM_VOLTAGE VALUE = "N/A"/>
    <RANKS VALUE = "1"/>
    <TECHNOLOGY VALUE = "N/A"/>
</CPU_1>
<CPU_1>
    <SOCKET VALUE = "5"/>
    <STATUS VALUE = "Not Present"/>
    <HP_SMART_MEMORY VALUE = "No"/>
    <TYPE VALUE = "N/A"/>
    <SIZE VALUE = "N/A"/>
    <FREQUENCY VALUE = "N/A"/>
    <MINIMUM_VOLTAGE VALUE = "N/A"/>
    <RANKS VALUE = "1"/>
    <TECHNOLOGY VALUE = "N/A"/>
</CPU_1>
<CPU_1>
    <SOCKET VALUE = "6"/>
    <STATUS VALUE = "Not Present"/>
    <HP_SMART_MEMORY VALUE = "No"/>
    <TYPE VALUE = "N/A"/>
    <SIZE VALUE = "N/A"/>
    <FREQUENCY VALUE = "N/A"/>
    <MINIMUM_VOLTAGE VALUE = "N/A"/>
    <RANKS VALUE = "1"/>
    <TECHNOLOGY VALUE = "N/A"/>
</CPU_1>
<CPU_2>
    <SOCKET VALUE = "1"/>
    <STATUS VALUE = "Good, In Use"/>
    <HP_SMART_MEMORY VALUE = "Yes"/>
    <TYPE VALUE = "DIMM DDR3"/>
    <SIZE VALUE = "2048 MB"/>
    <FREQUENCY VALUE = "1333 MHz"/>
    <MINIMUM_VOLTAGE VALUE = "1.50 v"/>
    <RANKS VALUE = "2"/>
    <TECHNOLOGY VALUE = "RDIMM"/>
</CPU_2>
<CPU_2>
    <SOCKET VALUE = "2"/>
    <STATUS VALUE = "Not Present"/>

```

```

        <HP_SMART_MEMORY VALUE = "No"/>
        <TYPE VALUE = "N/A"/>
        <SIZE VALUE = "N/A"/>
        <FREQUENCY VALUE = "N/A"/>
        <MINIMUM_VOLTAGE VALUE = "N/A"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "N/A"/>
    </CPU_2>
    <CPU_2>
        <SOCKET VALUE = "3"/>
        <STATUS VALUE = "Not Present"/>
        <HP_SMART_MEMORY VALUE = "No"/>
        <TYPE VALUE = "N/A"/>
        <SIZE VALUE = "N/A"/>
        <FREQUENCY VALUE = "N/A"/>
        <MINIMUM_VOLTAGE VALUE = "N/A"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "N/A"/>
    </CPU_2>
    <CPU_2>
        <SOCKET VALUE = "4"/>
        <STATUS VALUE = "Not Present"/>
        <HP_SMART_MEMORY VALUE = "No"/>
        <TYPE VALUE = "N/A"/>
        <SIZE VALUE = "N/A"/>
        <FREQUENCY VALUE = "N/A"/>
        <MINIMUM_VOLTAGE VALUE = "N/A"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "N/A"/>
    </CPU_2>
    <CPU_2>
        <SOCKET VALUE = "5"/>
        <STATUS VALUE = "Not Present"/>
        <HP_SMART_MEMORY VALUE = "No"/>
        <TYPE VALUE = "N/A"/>
        <SIZE VALUE = "N/A"/>
        <FREQUENCY VALUE = "N/A"/>
        <MINIMUM_VOLTAGE VALUE = "N/A"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "N/A"/>
    </CPU_2>
    <CPU_2>
        <SOCKET VALUE = "6"/>
        <STATUS VALUE = "Not Present"/>
        <HP_SMART_MEMORY VALUE = "No"/>
        <TYPE VALUE = "N/A"/>
        <SIZE VALUE = "N/A"/>
        <FREQUENCY VALUE = "N/A"/>
        <MINIMUM_VOLTAGE VALUE = "N/A"/>
        <RANKS VALUE = "1"/>
        <TECHNOLOGY VALUE = "N/A"/>
    </CPU_2>
</MEMORY_DETAILS>
</MEMORY>
<NIC_INFORMATION>
    <NIC>
        <NETWORK_PORT VALUE = "Port 1"/>
        <PORT_DESCRIPTION VALUE = "N/A"/>
        <MAC_ADDRESS VALUE = "a0:36:9f:01:4e:bc"/>
        <IP_ADDRESS VALUE = "N/A"/>
        <STATUS VALUE = "Other"/>
    </NIC>
    <iLO_4>
        <NETWORK_PORT VALUE = "iLO Dedicated Network Port"/>
        <PORT_DESCRIPTION VALUE = "iLO Dedicated Network Port"/>
        <MAC_ADDRESS VALUE = "9c:8e:99:0a:1d:96"/>
        <IP_ADDRESS VALUE = "16.85.177.5"/>
        <STATUS VALUE = "OK"/>
    </iLO_4>
</NIC_INFORMATION>
<STORAGE>
    <CONTROLLER>
        <LABEL VALUE = "Controller on System Board"/>
        <STATUS VALUE = "OK"/>
        <CONTROLLER_STATUS VALUE = "OK"/>
        <SERIAL_NUMBER VALUE = "50014380215F0070"/>
        <MODEL VALUE = "HP Smart Array P420i Controller"/>
        <FW_VERSION VALUE = "3.41"/>
    <DRIVE_ENCLOSURE>
        <LABEL VALUE = "Port 1I Box 1"/>
        <STATUS VALUE = "OK"/>

```

```

        <DRIVE_BAY VALUE = "04"/>
    </DRIVE_ENCLOSURE>
    <DRIVE_ENCLOSURE>
        <LABEL VALUE = "Port 2I Box 0"/>
        <STATUS VALUE = "OK"/>
        <DRIVE_BAY VALUE = "01"/>
    </DRIVE_ENCLOSURE>
    <LOGICAL_DRIVE>
        <LABEL VALUE = "01"/>
        <STATUS VALUE = "OK"/>
        <CAPACITY VALUE = "68 GB"/>
        <FAULT_TOLERANCE VALUE = "RAID 0"/>
        <PHYSICAL_DRIVE>
            <LABEL VALUE = "Port 1I Box 1 Bay 3"/>
            <STATUS VALUE = "OK"/>
            <SERIAL_NUMBER VALUE = "6TA0N3SZ0000B231CYDT"/>
            <MODEL VALUE = "EH0072FAWJA"/>
            <CAPACITY VALUE = "68 GB"/>
            <LOCATION VALUE = "Port 1I Box 1 Bay 3"/>
            <FW_VERSION VALUE = "HPDH"/>
            <DRIVE_CONFIGURATION VALUE = "Configured"/>
        </PHYSICAL_DRIVE>
    </LOGICAL_DRIVE>
</CONTROLLER>
</STORAGE>
<FIRMWARE_INFORMATION>
    <INDEX_1>
        <FIRMWARE_NAME VALUE = "HP ProLiant System ROM"/>
        <FIRMWARE_VERSION VALUE = "02/09/2012"/>
    </INDEX_1>
    <INDEX_2>
        <FIRMWARE_NAME VALUE = "HP ProLiant System ROM - Backup"/>
        <FIRMWARE_VERSION VALUE = "02/09/2012"/>
    </INDEX_2>
    <INDEX_3>
        <FIRMWARE_NAME VALUE = "HP ProLiant System ROM Bootblock"/>
        <FIRMWARE_VERSION VALUE = "10/18/2011"/>
    </INDEX_3>
    <INDEX_4>
        <FIRMWARE_NAME VALUE = "iLO"/>
        <FIRMWARE_VERSION VALUE = "1.05 Feb 22 2012"/>
    </INDEX_4>
    <INDEX_5>
        <FIRMWARE_NAME VALUE = "Power Management Controller Firmware"/>
        <FIRMWARE_VERSION VALUE = "3.0"/>
    </INDEX_5>
    <INDEX_6>
        <FIRMWARE_NAME VALUE = "Power Management Controller Firmware Bootloader"/>
        <FIRMWARE_VERSION VALUE = "2.7"/>
    </INDEX_6>
    <INDEX_7>
        <FIRMWARE_NAME VALUE = "System Programmable Logic Device"/>
        <FIRMWARE_VERSION VALUE = "Version 0x15"/>
    </INDEX_7>
    <INDEX_8>
        <FIRMWARE_NAME VALUE = "Server Platform Services (SPS) Firmware"/>
        <FIRMWARE_VERSION VALUE = "2.1.5.2B.4"/>
    </INDEX_8>
</FIRMWARE_INFORMATION>
<HEALTH_AT_A_GLANCE>
    <BIOS_HARDWARE STATUS= "OK"/>
    <FANS STATUS= "OK"/>
    <FANS_REDUNDANCY= "Redundant"/>
    <TEMPERATURE STATUS= "OK"/>
    <POWER_SUPPLIES STATUS= "Failed"/>
    <POWER_SUPPLIES_REDUNDANCY= "Not Redundant"/>
    <PROCESSOR STATUS= "OK"/>
    <MEMORY STATUS= "OK"/>
    <NETWORK STATUS= "Link Down"/>
    <STORAGE STATUS= "OK"/>
</HEALTH_AT_A_GLANCE>
</GET_EMBEDDED_HEALTH_DATA>

```

---

### Variable **POWER\_SUPPLIES** tags:

- The **POWER\_SUPPLIES** tags **HP\_POWER\_DISCOVERY\_SERVICES\_REDUNDANCY\_STATUS** and **HIGH\_EFFICIENCY\_MODE** appear only for blade servers.
- The following **POWER\_SUPPLIES** tags appear only when **SNMP** is available, otherwise they are replaced by the tags **SUPPLY\_LABEL** AND **SUPPLY\_STATUS**:
  - **PRESENT**
  - **PDS**
  - **HOTPLUG\_CAPABLE**
  - **MODEL**
  - **SPARE**
  - **SERIAL\_NUMBER**
  - **CAPACITY**
  - **FIRMWARE\_VERSION**
- The following **POWER\_SUPPLIES** tags appear only when an **iPDU** is present:
  - **POWER\_DISCOVERY\_SERVICES\_IPDU\_SUMMARY**
  - **IPDU**
  - **BAY**
  - **STATUS**
  - **PART\_NUMBER**
  - **SERIAL\_NUMBER**
  - **MAC\_ADDRESS**
  - **IPDU\_LINK**

---

## GET\_POWER\_READINGS

The **GET\_POWER\_READINGS** command is used to get the power readings from the server power supply.

For example:

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

### GET\_POWER\_READINGS parameters

None

## GET\_POWER\_READINGS return messages

Two types of responses are available from the GET\_POWER\_READINGS command, depending on whether or not an advanced license is applied.

If an advanced license is not applied, a typical response is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_POWER_READINGS>
<PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
</GET_POWER_READINGS>
</RIBCL>
```

If an advanced license is applied, a typical response is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
STATUS="0x0000"
MESSAGE='No error'
/>
<GET_POWER_READINGS>
<PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
<AVERAGE_POWER_READING VALUE="278" UNIT="Watts"/>
<MAXIMUM_POWER_READING VALUE="283" UNIT="Watts"/>
<MINIMUM_POWER_READING VALUE="270" UNIT="Watts"/>
</GET_POWER_READINGS>
</RIBCL>
```

## GET\_PWREG

The GET\_PWREG command gets the power alert threshold for iLO 4 devices. For this command to parse correctly, the GET\_PWREG command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE can be set to read. You must purchase the iLO Advanced license to enable this feature.

For example:

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

## GET\_PWREG parameters

None

## GET\_PWREG return messages

A GET\_PWREG return message includes:

```
<RESPONSE STATUS="0x0000" MSG="No Errors"/>
<GET_PWREG USER_NAME="Admin User" USER_LOGIN="username"
PCAP MODE="OFF"
EFFICIENCY_MODE="1"
PWRALERT TYPE="PEAK" THRESHOLD="250" DURATION="5"
GET_HOST_POWER HOST_POWER="ON"/>
```

Where:

- PCAP mode is either set to MAN followed by a positive integer, or set to OFF.
- EFFICIENCY\_MODE is a number between 1 and 4:
  - 1 — PWRREGMODE\_OS\_CONTROL
  - 2 — PWRREGMODE\_STATIC\_LOW
  - 3 — PWRREGMODE\_DYNAMIC
  - 4 — PWRREGMODE\_STATIC\_HIGH
- GET\_HOST\_POWER reports whether the virtual power button is enabled.

## GET\_PWREG runtime errors

Possible GET\_PWREG runtime errors:

- Feature not supported.
- This feature requires an installed license key.

## SET\_PWREG

The SET\_PWREG command sets the power alert threshold for iLO 4 devices. For this command to parse correctly, the SET\_PWREG command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE can be set to write. You must purchase the iLO Advanced license to enable this feature.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminame" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_PWREG>
        <PWRALERT TYPE="PEAK"/>
        <PWRALERT_SETTINGS THRESHOLD="200" DURATION="35"/>
      </SET_PWREG>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## SET\_PWREG parameters

PWRALERT TYPE—Valid values are:

- DISABLED—No power alerts are set.
- PEAK—Represents the half-second average power reading during the sample.
- AVERAGE—Represents the mean power reading during the sample.

PWRALERT\_SETTINGS

- THRESHOLD—Sets the alert threshold, in watts.
- DURATION—Sets the length of the sample time, in minutes, starting at 5. Duration will always be in 5 minute intervals up to 240 minutes maximum. Any positive integer can be used, but it will be rounded off to the nearest 5.

## SET\_PWREG runtime errors

Possible SET\_PWREG error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Internal error.
- The value specified is invalid.
- This feature requires an installed license key.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.
- The PWRALERT value is invalid.
- The THRESHOLD value is invalid.
- The DURATION value is invalid. Values supported are between 1 and 240.
- Invalid integer.

## GET\_POWER\_CAP

The GET\_POWER\_CAP command is used to get the power cap of the server. For this command to parse correctly, the GET\_POWER\_CAP command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE can be set to read. You must purchase the iLO Advanced license to enable this feature.

For example:

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

## GET\_POWER\_CAP parameters

None

## GET\_POWER\_CAP return messages

A cap value of zero indicates a power cap is not currently set on the server.

## SET\_POWER\_CAP

The SET\_POWER\_CAP command is used to set a power cap on the server. For this command to parse correctly, the SET\_POWER\_CAP command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. You must have the Configure iLO Settings privilege to execute this command.

You cannot set this property if a dynamic power cap is set for the server. Dynamic power capping is set and modified using either Onboard Administrator or Insight Power Manager. You must purchase the iLO Advanced license to enable this feature.

For example, enabling the power cap:

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

```
<SET_POWER_CAP POWER_CAP="300"/>
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

## SET\_POWER\_CAP parameters

SET\_POWER\_CAP POWER\_CAP is the power cap on the server. Valid power cap values are determined using a power test run on the server at boot. The possible values are 0 to disable the power cap, or a numeric value in watts (as determined in the power test.)

## SET\_POWER\_CAP runtime errors

The possible SET\_POWER\_CAP error messages include:

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

## GET\_HOST\_POWER\_SAVER\_STATUS

The GET\_HOST\_POWER\_SAVER\_STATUS command requests the state of the processor power regulator feature of the server. For this command to parse correctly, the GET\_HOST\_POWER\_SAVER\_STATUS command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read or write.

For example:

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

## GET\_HOST\_POWER\_SAVER\_STATUS parameters

None

## GET\_HOST\_POWER\_SAVER\_STATUS runtime errors

The possible GET\_HOST\_POWER\_SAVER\_STATUS error messages include:

Feature not supported

## GET\_HOST\_POWER\_SAVER\_STATUS return messages

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

- <GET\_HOST\_POWER\_SAVER HOST POWER\_SAVER= "OFF"/>
- <GET\_HOST\_POWER\_SAVER HOST POWER\_SAVER= "MIN"/>
- <GET\_HOST\_POWER\_SAVER HOST POWER\_SAVER= "AUTO"/>
- <GET\_HOST\_POWER\_SAVER HOST POWER\_SAVER= "MAX"/>

## SET\_HOST\_POWER\_SAVER

The SET\_HOST\_POWER\_SAVER command is used to set the Power Regulator Setting for the server processor. For this command to parse correctly, the SET\_HOST\_POWER\_SAVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Modify the HOST_POWER_SAVER attribute to modify
           power saver on the host server -->
      <SET_HOST_POWER_SAVER HOST_POWER_SAVER="1"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

### SET\_HOST\_POWER\_SAVER parameters

The HOST\_POWER\_SAVER command controls the Dynamic Power Saver feature of the server processor if the feature is supported. The possible values are:

- **1**—Operating system control mode
- **2**—HP Static Low Power mode
- **3**—HP Dynamic Power Savings mode
- **4**—HP Static High Performance mode

### SET\_HOST\_POWER\_SAVER runtime errors

The possible SET\_HOST\_POWER error messages include:

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

## 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. You can set SERVER\_INFO MODE to read or write.

For example:

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

For example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="write">
    <!-- Modify the HOST_POWER attribute to toggle power on the host server -->
    <!-- HOST_POWER="No" (Turns host server power off) -->
    <!-- A graceful shutdown will be attempted for ACPI-aware -->
    <!-- operating systems configured to support graceful shutdown. -->
    <!-- HOST_POWER="Yes" (Turns host server power on) -->
    <SET_HOST_POWER HOST_POWER="No"/>
  </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.

## GET\_HOST\_PWR\_MICRO\_VER

The GET\_HOST\_PWR\_MICRO\_VER command provides the power micro version number. The GET\_HOST\_PWR\_MICRO\_VER command must appear within a SERVER\_INFO command block to parse correctly. SERVER\_INFO must be set to read.

For example:

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

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="read">
    <GET_HOST_PWR_MICRO_VER/>
  </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## GET\_HOST\_PWR\_MICRO\_VER parameters

None

## GET\_HOST\_PWR\_MICRO\_VER runtime errors

The possible GET\_HOST\_PWR\_MICRO\_VER error messages include:

- `Error`—if the power micro cannot be read (hardware problem).
- `Power Off`—if the server is powered off.
- `N/A`—if the server does not support a power micro.

## GET\_HOST\_PWR\_MICRO\_VER return messages

- No errors and displays version information:

```

<GET_HOST_PWR_MICRO_VER>
<PWR_MICRO VERSION="2.3"/>
</GET_HOST_PWR_MICRO_VER>

```

- Failed to read power micro version:

```

<GET_HOST_PWR_MICRO_VER>
<PWR_MICRO VERSION="Error"/>
</GET_HOST_PWR_MICRO_VER>

```

- Power micro not supported on the server:

```

<GET_HOST_PWR_MICRO_VER>
<PWR_MICRO VERSION="UNKNOWN"/>
</GET_HOST_PWR_MICRO_VER>

```

## RESET\_SERVER

The `RESET_SERVER` command forces a warm boot of the server if the server is currently on. For this command to parse correctly, the `RESET_SERVER` command must appear within a `SERVER_INFO` command block, and `SERVER_INFO MODE` must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

```

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

```

## RESET\_SERVER error messages

The possible RESET\_SERVER error messages include:

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

## RESET\_SERVER parameters

None

## PRESS\_PWR\_BTN

The PRESS\_PWR\_BTN command is used to simulate a physical press (or press and hold) of the server power button. For this command to parse correctly, the PRESS\_PWR\_BTN command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

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

## PRESS\_PWR\_BTN parameters

None

## PRESS\_PWR\_BTN runtime errors

The possible error messages include:

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

## HOLD\_PWR\_BTN

The HOLD\_PWR\_BTN command is used to simulate a physical press and hold of the server power button. For this command to parse correctly, the HOLD\_PWR\_BTN command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

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

## HOLD\_PWR\_BTN parameters

Without the TOGGLE parameter, the HOLD\_PWR\_BTN command powers off a running server. If the server power is off, the server power will remain off. The affect of using the command with the TOGGLE parameter defines the action to take based on the current power state of the server. The following occurs based on the value of TOGGLE:

- When the server power is on, a Yes value for TOGGLE will turn the power off.
- When the server power is off, a Yes value for TOGGLE will turn the power on.
- When the server power is off, a No value for TOGGLE will leave the power off.

## HOLD\_PWR\_BTN runtime errors

The possible error messages include:

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

## COLD\_BOOT\_SERVER

The COLD\_BOOT\_SERVER command forces a cold boot of the server, if the server is currently on. For this command to parse correctly, the COLD\_BOOT\_SERVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

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

## COLD\_BOOT\_SERVER parameters

None

## COLD\_BOOT\_SERVER runtime errors

The possible error messages include:

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

## WARM\_BOOT\_SERVER

The WARM\_BOOT\_SERVER command forces a warm boot of the server, if the server is currently on. For this command to parse correctly, the WARM\_BOOT\_SERVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the Virtual Power and Reset privilege to execute this command.

For example:

```

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

```

## WARM\_BOOT\_SERVER parameters

None

## WARM\_BOOT\_SERVER runtime errors

Possible error messages include:

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

## SERVER\_AUTO\_PWR

The SERVER\_AUTO\_PWR command is used to set the automatic power on and power on delay settings. Any power delays set using this command are invoked after iLO is running.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Enable automatic power on -->
      <SERVER_AUTO_PWR VALUE="On"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>

```

---

**NOTE:** Enabling a power on delay using the SERVER\_AUTO\_PWR command requires you to run the script twice. First, run the script and set the SERVER\_AUTO\_PWR value to `on`. Next, run the script with a value of `15`, `30`, `45`, `60` to set up the power on delay.

---

## SERVER\_AUTO\_PWR parameters

The available values for the VALUE parameter are:

- `Yes`—Enables automatic power on (APO) with a minimum delay.
- `No`—APO restores last power state.
- `15`, `30`, `45`, `60`—Sets APO delay time in seconds.
- `Random`—Sets an automatic power on with a random delay of up to 2 minutes.
- `On`—APO always powers on.
- `Off`—APO always remains off.
- `Restore`—Restores last power state before power interruption.

## SERVER\_AUTO\_PWR runtime errors

The possible errors include:

- User does not have correct privilege for action. Configure iLO privilege is required
- SERVER\_INFO mode is not WRITE
- The value specified for SERVER\_AUTO\_PWR is invalid or not accepted on blades

## GET\_SERVER\_AUTO\_PWR

The GET\_SERVER\_AUTO\_PWR command is used to get the automatic power on and power on delay settings of the server.

The command is supported by all iLO 4 firmware versions.

For example:

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

## GET\_SERVER\_AUTO\_PWR parameters

None

## GET\_SERVER\_AUTO\_PWR return message

Possible GET\_SERVER\_AUTO\_PWR return is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_SERVER_AUTO_PWR>
<!--
  Automatically Power On Server is enabled to power-on.
  Power On Delay is random.
-->
<SERVER_AUTO_PWR VALUE="ON" />
</GET_SERVER_AUTO_PWR>
</RIBCL>
```

## GET\_UID\_STATUS

The GET\_UID\_STATUS command requests the state of the server UID. For this command to parse correctly, the GET\_UID\_STATUS command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read.

For example:

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

```
<GET_UID_STATUS />
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

## GET\_UID\_STATUS parameters

None

## GET\_UID\_STATUS response

The following information is returned within the response:

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

## UID\_CONTROL

The UID\_CONTROL command toggles the server UID. For this command to parse correctly, the UID\_CONTROL command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Modify the UID attribute to toggle UID on the host server -->
      <!-- UID="No" (Turns host server UID off) -->
      <!-- UID="Yes" (Turns host server UID on) -->
      <UID_CONTROL UID="Yes"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

## UID\_CONTROL parameters

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

## UID\_CONTROL errors

The possible UID\_CONTROL error messages include:

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

## SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED

The SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED command sets the persistent mouse and keyboard setting. The possible values are Y (enabled) or N (disabled). For this command to parse correctly, the command must appear within a SERVER\_INFO command block. You must set SERVER\_INFO MODE to write.

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

## SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED parameters

SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED—Configures persistent keyboard and mouse. Valid values are **Y** (enabled) and **N** (disabled).

## SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED runtime errors

The possible runtime errors are:

- There was an error on setting the persistent mouse and keyboard.
- iLO information is open for read-only access. Write access is required for this operation.
- User does NOT have correct privilege for action. CONFIG\_ILO\_PRIV required.

## GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED

GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED returns the persistent mouse and keyboard status. A return value of **Y** indicates that persistent mouse and keyboard is enabled. A return value of **N** indicates it is disabled.

For example:

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

## GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED parameters

None

## GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED return messages

A possible GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED message is:

```
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
  />
<GET_PERS_MOUSE_KEYBOARD_ENABLED>
  <PERSMOUSE_ENABLED VALUE="Y"/>
</GET_PERS_MOUSE_KEYBOARD_ENABLED>
</RIBCL>
```

## GET\_SERVER\_POWER\_ON\_TIME

The GET\_SERVER\_POWER\_ON\_TIME command is used to retrieve the virtual clock value, in minutes, since the server was last powered on. For this command to parse correctly, the GET\_SERVER\_POWER\_ON\_TIME command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read.

For example:

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

## GET\_SERVER\_POWER\_ON\_TIME parameters

None

## GET\_SERVER\_POWER\_ON\_TIME return message

A possible GET\_SERVER\_POWER\_ON\_TIME return is:

```
<SERVER_POWER_ON_MINUTES VALUE="33815" />
```

## CLEAR\_SERVER\_POWER\_ON\_TIME

The CLEAR\_SERVER\_POWER\_ON\_TIME command is used to clear the virtual clock counter without power-cycling the server. For this command to parse correctly, the CLEAR\_SERVER\_POWER\_ON\_TIME command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

For example:

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

## CLEAR\_SERVER\_POWER\_ON\_TIME parameters

None

## CLEAR\_SERVER\_POWER\_ON\_TIME return message

None

---

**NOTE:** To verify the command, use the GET\_SERVER\_POWER\_ON\_TIME command and verify it returns the following message:

```
<SERVER_POWER_ON_MINUTES VALUE="0" />
```

---

## SSO\_INFO

The SSO\_INFO MODE command can only appear within a LOGIN command block. Only commands that are SSO\_INFO MODE-type commands are valid inside the SSO\_INFO MODE command block.

SSO\_INFO MODE requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO information. Read mode prevents modification of the iLO information. You must have the Configure iLO Settings privilege to execute this command.

For example:

```
<SSO_INFO MODE="write">
```

..... SSO\_INFO commands .....

```
</SSO_INFO>
```

Deleting a SSO HP SIM Server Record by index number example:

```
<RIBCL VERSION="2.0">  
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">  
    <SSO_INFO MODE="write">  
      <DELETE_SERVER INDEX="6" />  
    </SSO_INFO>  
  </LOGIN>  
</RIBCL>
```

```

    </SSO_INFO>
  </LOGIN>
</RIBCL>

```

## GET\_SSO\_SETTINGS

The GET\_SSO\_SETTINGS command is used to retrieve SSO settings for iLO. For this command to parse correctly, the GET\_SSO\_SETTINGS command must appear within a SSO\_INFO command block, and SSO\_INFO MODE can be set to read or write.

For example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SSO_INFO MODE="read">
      <GET_SSO_SETTINGS/>
    </SSO_INFO>
  </LOGIN>
</RIBCL>

```

## GET\_SSO\_SETTINGS parameters

None

## GET\_SSO\_SETTINGS return messages

The following is an example of an SSO settings response from a configured iLO device. There are 0 or more SSO\_SERVER records reflecting the number of stored server records in each.

```

<GET_SSO_SETTINGS>
<TRUST_MODE VALUE="CERTIFICATE" />
<USER_ROLE LOGIN_PRIV="Y" />
<USER_ROLE REMOTE_CONS_PRIV="N" />
<USER_ROLE RESET_SERVER_PRIV="N" />
<USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
<USER_ROLE CONFIG_ILO_PRIV="N" />
<USER_ROLE ADMIN_PRIV="N" />
<OPERATOR_ROLE LOGIN_PRIV="Y" />
<OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
<OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
<OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
<OPERATOR_ROLE ADMIN_PRIV="N" />
<ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />
<ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
<ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
<ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
<ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
<SSO_SERVER INDEX="0"
  ISSUED_TO="viv.hp.com"
  ISSUED_BY="viv.hp.com"
  VALID_FROM="061108192059Z"
  VALID_UNTIL="161108192059Z">
-----BEGIN CERTIFICATE-----
.
.
.
-----END CERTIFICATE-----
</SSO_SERVER>
<SSO_SERVER INDEX="1">
ant.hp.com

```

```
</SSO_SERVER>
</GET_SSO_SETTINGS>
```

## MOD\_SSO\_SETTINGS

The MOD\_SSO\_SETTINGS command is used to modify the HP SSO settings for iLO 4. For this command to parse correctly, the MOD\_SSO\_SETTINGS command must appear within a SSO\_INFO command block, and SSO\_INFO MODE must be set to write. The user must have the Configure iLO Settings privilege to execute this command.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SSO_INFO MODE="write">
      <MOD_SSO_SETTINGS>
        <!-- Specify the desired trust mode Options: DISABLED(default),
          CERTIFICATE (recommended), NAME, or ALL -->
        <TRUST_MODE="CERTIFICATE" />
        <!-- Specify the privileges assigned to the user role -->
        <USER_ROLE LOGIN_PRIV="Y" />
        <USER_ROLE REMOTE_CONS_PRIV="N" />
        <USER_ROLE RESET_SERVER_PRIV="N" />
        <USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
        <USER_ROLE CONFIG_ILO_PRIV="N" />
        <USER_ROLE ADMIN_PRIV="N" />
        <!-- Specify the privileges assigned to the operator role -->
        <OPERATOR_ROLE LOGIN_PRIV="Y" />
        <OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
        <OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
        <OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
        <OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
        <OPERATOR_ROLE ADMIN_PRIV="N" />
        <!-- Specify the privileges assigned to the administrator role -->
        <ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />
        <ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
        <ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
        <ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
        <ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
        <ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
        <ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
      </MOD_SSO_SETTINGS>
    </SSO_INFO>
  </LOGIN>
</RIBCL>
```

### MOD\_SSO\_SETTINGS parameters

TRUST\_MODE sets the Single Sign-On trust mode. The current setting is unchanged if this setting is omitted from the script. Accepted values are:

- Disabled—Disables HP SSO on this processor.
- Certificate—Accepts only SSO requests authenticated using a certificate.
- Name—Trusts SSO requests from the named HP SIM Server.
- All—Accepts any SSO request from the network.

Role names are used to associate iLO privileges. The specified privileges are set accordingly for that role, and a privilege that is omitted is unchanged. Enable a privilege for the role using the argument Y and disable the privilege for the role using the argument N.

There are three roles for privilege assignment. Omitting a role leaves the current assignment unchanged:

- `USER_ROLE`—Privileges associated with User
- `OPERATOR_ROLE`—Privileges associated with Operator
- `ADMINISTRATOR_ROLE`—Privileges associated with Administrator

For each role, you can manipulate multiple privileges. The privilege is specified within the role tag. If a privilege is omitted, the current value is unchanged. Each privilege assignment is Boolean and can be set to Y (privilege granted) or N (privilege denied). For more details on account privileges, see the **User Administration** section of the *HP iLO User Guide* on the HP website at <http://www.hp.com/go/ilo/docs>.

- `LOGIN_PRIV`—Allows login for this role.
- `REMOTE_CONS_PRIV`—Grants access to remote console resources.
- `RESET_SERVER_PRIV`—Grants access to power and reset controls.
- `VIRTUAL_MEDIA_PRIV`—Grants access to virtual media resources.
- `CONFIG_ILO_PRIV`—Allows settings modification.
- `ADMIN_PRIV`—Allows local user account modification.

## MOD\_SSO\_SETTINGS runtime errors

Possible `MOD_SSO_SETTINGS` error messages include:

- Incorrect firmware version. SSO is only supported on iLO 4 v1.01 firmware or later.
- User does not have correct privilege for action. `CONFIG_ILO_PRIV` required.
- `SSO_INFO` must be in write mode.

## SSO\_SERVER

The `SSO_SERVER` command is used to create HP SIM Trusted SSO Server records. For this command to parse correctly, it must appear within an `SSO_INFO` command block, and `SSO_INFO MODE` must be set to write. You must have the Configure iLO Settings privilege to execute this command. This command can be combined with `MOD_SSO_SETTINGS`.

You can specify multiple SSO server records by using multiple instances of this command. The servers are added in the order that the records are specified. Duplicate records might be rejected and generate an error. The number of records stored by the lights-out processor depends on the size of the entries because certificates do not have a fixed size. Multiple certificates can normally be stored.

There are three ways to add an HP SIM Trusted Server record using the `SSO_SERVER` command:

- The server can be specified by network name (requires SSO trust level set to trust by name or trust all, but is not supported for trust by certificate). Use the fully qualified network name.
- The server certificate can be imported by iLO 4 (the LOM processor requests the certificate from the specified HP SIM server using anonymous HTTP request). The iLO 4 processor must be able to contact the HP SIM server on the network at the time this command is processed for this method to work.
- The server certificate can be directly installed on iLO 4. However, you must obtain the x.509 certificate in advance. This method enables you to configure the iLO 4 in advance of placing it on the network with the HP SIM server. The method also enables you to verify the contents of the HP SIM server certificate. For additional methods of obtaining the certificate from the HP SIM server, see the *HP iLO User Guide* on the HP website at: <http://www.hp.com/go/>

[ilo/docs](http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html), or the *HP SIM User Guide* on the HP website at: <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SSO_INFO MODE="write">
      <!-- Add an SSO server record using the network name
           (works for TRUST_MODE NAME or ALL) -->
      <SSO_SERVER NAME="hpsim1.hp.net" />
      <!-- Add an SSO server record using indirect iLO import
           from the network name -->
      <SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />
      <!-- Add an SSO server certificate record using direct
           import of certificate data -->
      <IMPORT_CERTIFICATE>
        -----BEGIN CERTIFICATE-----
          .
          .
          .
          -----END CERTIFICATE-----
      </IMPORT_CERTIFICATE>
    </SSO_INFO>
  </LOGIN>
</RIBCL>
```

## SSO\_SERVER parameters

NAME indicates that the server is being specified by network name. It receives a quoted string containing the fully qualified network name of the HP SIM Trusted Server. The name is not validated by iLO until an SSO login is attempted. For example, the syntax to add an HP SIM Trusted Server name:

```
<SSO_SERVER NAME="hpsim1.hp.net" />
```

IMPORT\_FROM indicates that iLO must request the HP SIM Trusted Server certificate from HP SIM. This request is implemented using an anonymous HTTP request similar to:

```
http://<sim network address>:280/GetCertificate
```

The iLO firmware requests the certificate when this command is processed. If the HP SIM server is unreachable, then an error occurs.

For example, the syntax to have iLO import a server certificate resembles:

```
<SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />
```

IMPORT\_CERTIFICATE indicates that iLO must import the literal .PEM encoded x.509 certificate data that follows. The data is encoded in a block of text that includes:

```
-----BEGIN CERTIFICATE-----
```

and

```
-----END CERTIFICATE-----
```

For example, the syntax to import an HP SIM Trusted Server certificate resembles the following:

```
<SSO_SERVER>
  -----BEGIN CERTIFICATE-----
  MIIC3TCCAkYCBESzWfUwDQYJKoZIhvcNAQEFBQAwgUxCzAJBgNVBAYTA1VTMRMwE...
  kXzhuVzPfWzQ+a2E9tGAE/YgNGTfs9vKkVLUF6QoP/RQpYpk15BxrsN3gM/PeT3zrxyTleE=
  -----END CERTIFICATE-----
</SSO_SERVER>
```

The certificate is validated by iLO to ensure that it can be decoded before it is stored. An error results if the certificate is a duplicate or corrupt.

The iLO firmware does not support certificate revocation and does not honor certificates that appear expired. You must remove revoked or expired certificates.

### SSO\_SERVER runtime errors

A runtime error is generated if the:

- Certificate is a duplicate.
- Certificate is corrupt.
- HP SIM server cannot be contacted using IMPORT\_FROM.
- HP SIM Trusted Server database is full (you must delete other records to make sufficient room to add a new entry).
- Trust mode is set incorrectly.

### DELETE\_SERVER

The DELETE\_SERVER command is used to remove an HP SIM Trusted SSO Server record. For this command to parse correctly, it must appear within an SSO\_INFO command block, and SSO\_INFO MODE must be set to write. You must have the Configure iLO Settings privilege to execute this command.

You can specify multiple SSO server records by using multiple instances of this command. The servers are deleted in the order that the records are specified, and the records are renumbered by each deletion. Delete records in the highest-to-lowest order if you want to delete multiple records at the same time.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SSO_INFO MODE="write">
      <DELETE_SERVER INDEX="6" />
    </SSO_INFO>
  </LOGIN>
</RIBCL>
```

### DELETE\_SERVER parameters

INDEX indicates the record number to delete. This number is consistent with the index returned using a GET\_SSO\_SETTINGS command. The index is 0-based; that is the first record is index 0, the second record is index 1, and so on.

### DELETE\_SERVER runtime errors

A runtime error is generated if the index is invalid.

# 9 Secure Shell

## SSH overview

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

iLO 4 supports:

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

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

## Supported SSH features

The library supports only version 2 (SSH-2) of the protocol. [Table 31 \(page 188\)](#) shows the SSH features supported by iLO.

**Table 31 Supported SSH Features**

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

## Using Secure Shell

### Using SSH

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

### Using OpenSSH

To start an OpenSSH client in Linux, use:

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

## Using PuTTY

- To start a PuTTY session, double-click the PuTTY icon in the directory where PuTTY is installed.
- To start a PuTTY session from the command line, do the following:
  - Start a connection to a server called *host* by entering:  
`putty.exe [-ssh | -rlogin | -raw] [user@]host`
  - Start an existing saved session called *sessionname* by entering:  
`putty.exe -load session name`

## SSH key authorization

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.

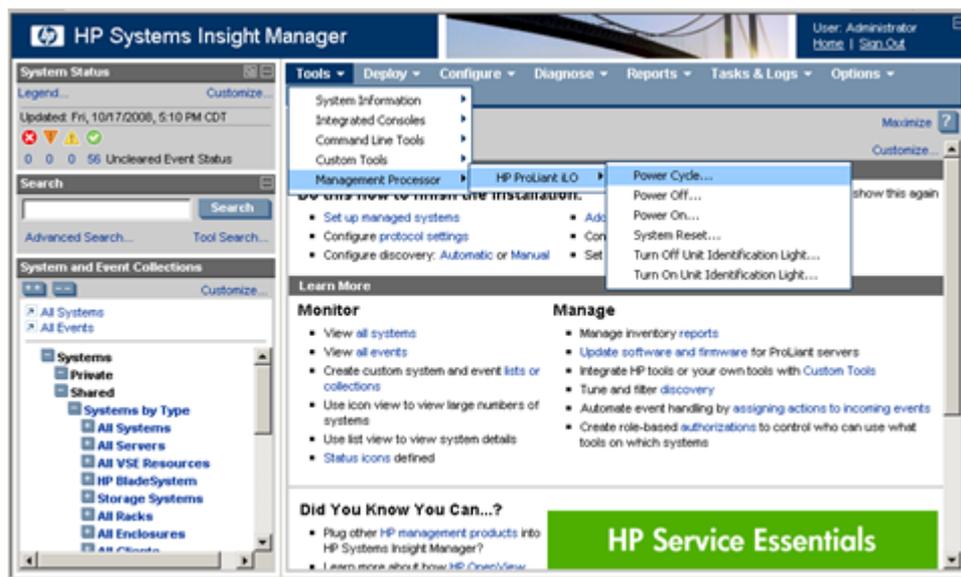
An HP SIM instance is established as a trusted SSH client by installing the public key in iLO. This is completed either manually through a Web-based GUI, or automatically with the `mxagentconfig` utility.

SSH keys do not need to be created to use SSH in interactive mode. For information about using SSH in interactive mode, see “SSH overview” (page 188).

## Tool definition files

TDEF files extend the menu system of HP SIM to provide the CLP commands that HP SIM transmits to iLO 4 through an SSH connection.

Figure 1 HP Systems Insight Manager menus



## Mxagentconfig utility

`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 makes an SSH connection to iLO, authenticates with a user name and password, and transmits the necessary public key. The iLO firmware 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 4. The following example illustrates, a PuTTY generated public key file:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: "Administrator"  
AAAAB3NzaC1yc2EAAAABJQAAAIB0x0wVO9itQB11o+tHnY3VvmsGgwghCyLOVzJ1  
3A9F5yzKj+RXJVPxOGusAhmJwF8PBQ9wV5E0Rumm6gNOaPyvAMJCG/10PW7Fhac1  
VLt8i5F3Lossw+/LWa+6H0da13TF2vq3ZoYFUT4esC6YbAACM7kLuGwxF5XMNR2E  
Foup3w==  
----- END SSH2 PUBLIC KEY -----
```

Note that this sample key conforms to RFC 4716 (SSH Public Key File Format). The iLO interface supports two key formats, OpenSSH 2 and RFC 4716. A third format is supported only in scripting (see ["IMPORT\\_SSH\\_KEY"](#) (page 137)).

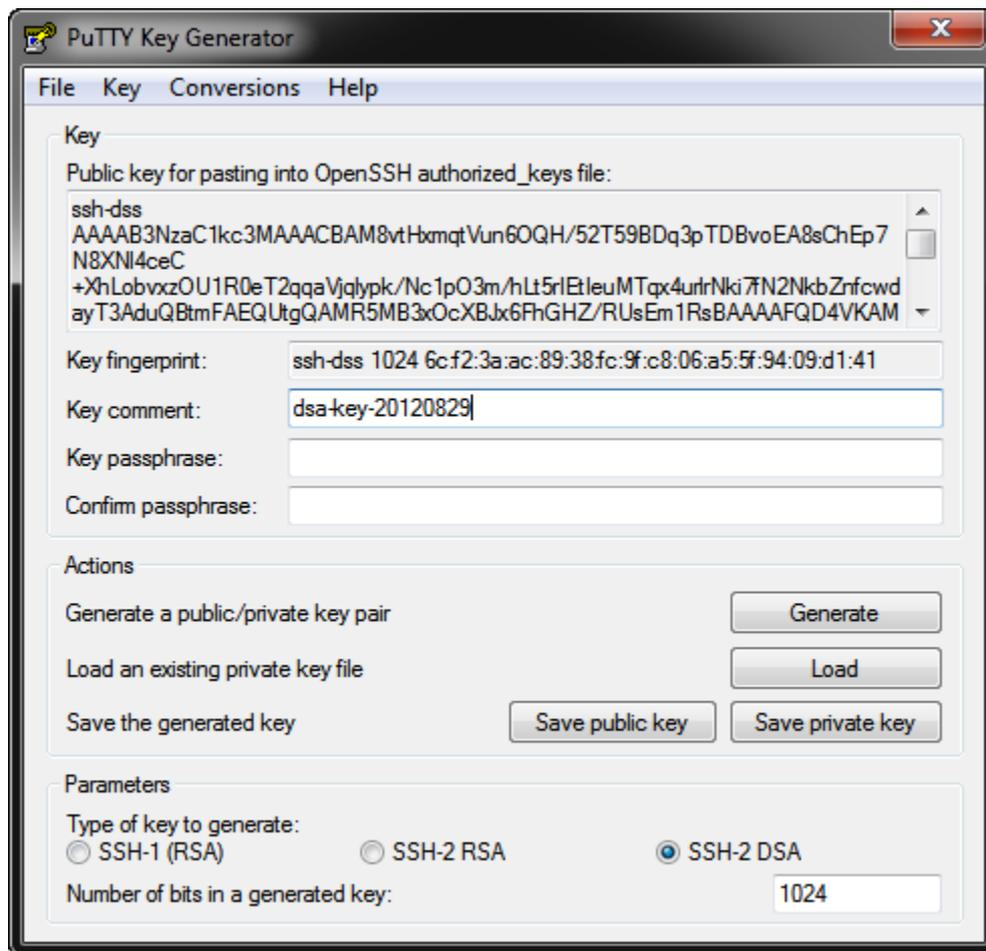
The iLO firmware expects public key file information on a single line. You can use the PuTTY Key Generator utility (`puttygen.exe`) to generate and properly format a key file for import into iLO.

To import SSH keys to iLO from PuTTY:

1. Double-click the PuTTY Key Generator icon to launch the utility.
2. Select **SSH-2 DSA**.
3. Click **Generate**.

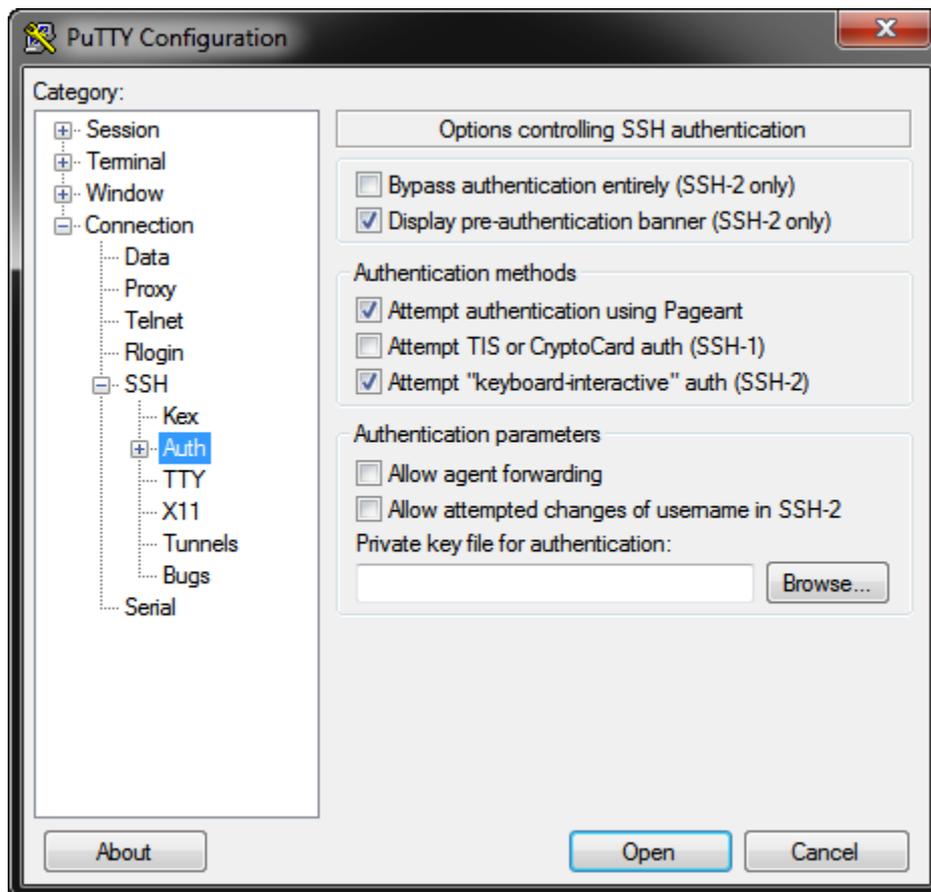
On the key area, move the mouse around to generate the key. You must keep moving the mouse until the key generation process completes.

Figure 2 PuTTY Key Generator



4. Click **Save public key** and then enter a file name when prompted.
5. Click **Save private key** and then enter a file name when prompted. Note that you have the option to enter and confirm a Key passphrase.
6. Open your public key in a text editor, and copy the contents to the clipboard.
7. Log in to iLO (if not already open).
8. On the iLO SSH Key Administration page, select a user from the Authorized SSH Keys list, and then click **Authorize New Key**.  
A DSA Public Key Import Data box appears.
9. Paste the PEM encoded DSA public key in the box, and then click **Import Public Key**.  
A new Public Key Hash appears for the user in the list of authorized SSH keys.
10. Launch PuTTY.
11. Select **Session**, and then configure your iLO 4 IP address.
12. Select **Connection+SSH→Auth**.
13. Click **Browse**, and then locate the private key file.

Figure 3 PuTTY Configuration window



14. Click **Open**.

The iLO firmware prompts for a user name.

15. Enter the logon name associated with the public key.

The public key in iLO authenticates with the private key in PuTTY. If the keys match, you are logged in to 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 are prompted for the key passphrase before you log in to iLO.

## Importing SSH keys generated using ssh-keygen

After generating an SSH key using `ssh-keygen` and creating the `key.pub` file, perform the following steps:

1. Locate and open the `key.pub` file with a text editor. The file begins with the text `ssh-dsa.`
2. Save and close the file.

The key file is ready to import and authorize.

# 10 PERL scripting

## Using PERL with the XML scripting interface

The scripting interface provided enables administrators to manage virtually every aspect of the device in an automated fashion. Primarily, administrators use tools like HPQLOCFG to assist deployment efforts. Administrators using a non-Windows client can use PERL scripts to send XML scripts to the iLO devices. Administrators can also use PERL to perform more complex tasks than HPQLOCFG can perform.

This section discusses how to use PERL scripting in conjunction with the Lights-Out XML scripting language. PERL scripts require a valid user ID and password with appropriate privileges.

Download the sample scripts from the HP website at <http://www.hp.com/go/ilo>. Click **iLO Sample Scripts for Windows** or **Lights-Out XML scripting sample for Linux** on the **Resources** tab, under **Support**.

## XML enhancements

If you are using a utility other than HPQLOCFG (such as PERL), the following steps help ensure that the iLO 4 firmware returns properly formatted XML. You must incorporate the following tag into the script sent to iLO 4:

```
<LOCFG version="2.0">
```

You can place this tag in either the PERL script or the XML script. Placement of this tag is important. If you place this tag in the PERL script, the tag must be sent after `<?xml version="1.0"?>` and before the XML script is sent. If you place the tag in the XML script, the tag must be placed before `<RIBCL version="2.0">`. If you are using the PERL script provided by HP, you can add the bold line in the following example to return properly formatted XML syntax.

For example:

- PERL script modification

```
...
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr => $host);
open(F, "<$file") || die "Can't open $file\n";
# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
#Send tag to iLO firmware to insure properly formatted XML is returned.
print $client '<LOCFG version="2.0">' . "\r\n";
...
```

- XML script modification

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

## Opening an SSL connection

Perl scripts must open an SSL connection to the device HTTPS port, by default port 443.

For example:

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

#
# opens an ssl connection to port 443 of the passed host

#
sub openSSLconnection($)
{
my $host = shift;
my ($ctx, $ssl, $sin, $ip, $nip);
if (not $ip = inet_aton($host))
{
print "$host is a DNS Name, performing lookup\n" if $debug;
$ip = gethostbyname($host) or die "ERROR: Host $hostname not found.\n";
}
$nip = inet_ntoa($ip);
print STDERR "Connecting to $nip:443\n";
$sin = sockaddr_in(443, $ip);
socket (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR: socket: $!";
connect (S, $sin) or die "connect: $!";
$ctx = Net::SSLeay::CTX_new() or die_now("ERROR: Failed to create SSL_CTX $! ");
Net::SSLeay::CTX_set_options($ctx, &Net::SSLeay::OP_ALL);
die_if_ssl_error("ERROR: ssl ctx set options");
$ssl = Net::SSLeay::new($ctx) or die_now("ERROR: Failed to create SSL $!");
Net::SSLeay::set_fd($ssl, fileno(S));
Net::SSLeay::connect($ssl) and die_if_ssl_error("ERROR: ssl connect");
print STDERR 'SSL Connected ';
print 'Using Cipher: ' . Net::SSLeay::get_cipher($ssl) if $debug;
print STDERR "\n\n";

return $ssl;
}
```

## Sending the XML header and script body

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

For example:

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

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

$n = Net::SSLeay::ssl_write_all($ssl, $script);
print "Wrote $n\n$script\n" if $debug;
$reply = "";
$lastreply = "";
```

```

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

```

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

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

- PERL scripts must send the XML header before sending the body of the script.
- PERL scripts must provide script data fast enough to prevent the device from timing out.
- Only one XML document is allowed per connection, which means one pair of RIBCL tags.
- The device does not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

## 11 iLO 4 ports

### Enabling the Shared Network Port feature through XML scripting

For information on how to use the `SHARED_NETWORK_PORT` command to enable the iLO 4 Shared Network Port through XML scripting, see [“RIBCL XML Scripting Language” \(page 64\)](#).

The following sample script configures the iLO 4 to select the Shared Network Port. You can customize this script to your needs. All non-blade platforms support some variation of this script. Use `LOM` or `FlexibleLOM` for the `SHARED_NETWORK_PORT` VALUE. If you pick a value that your platform does not support, the script generates an error when it is run.

```
<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="WRITE">
      <MOD_NETWORK_SETTINGS>
        <!-- Desired NIC: Substitute: -->
        <!-- iLO NIC <SHARED_NETWORK_PORT VALUE="N"/> -->
        <!-- Embedded Host NIC <SHARED_NETWORK_PORT VALUE="LOM"/> -->
        <!-- Optional Host NIC <SHARED_NETWORK_PORT VALUE="FlexibleLOM"/> -->
        <SHARED_NETWORK_PORT VALUE="Y" />
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

### Re-enabling the dedicated NIC management port

You can re-enable the iLO-dedicated NIC management port using the User Interface, RBSU, CLP, or XML scripting.

For information about how to use the `SHARED_NETWORK_PORT` command, see [“RIBCL XML Scripting Language” \(page 64\)](#)

To re-enable the dedicated management port using RBSU:

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

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

To re-enable the dedicated iLO port using XML, use the following sample RIBCL script. The sample script configures iLO to select the iLO Network Port. You can modify the script for your specific needs. Using this script on platforms that do not support the Shared Network Port causes an error.

For example:

```
<RIBCL version="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="WRITE">
      <MOD_NETWORK_SETTINGS>
        <SHARED_NETWORK_PORT VALUE="N" />
      </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
```

```
</LOGIN>  
</RIBCL>
```

---

## 12 Support and other resources

### Information to collect before contacting HP

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

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

### How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:  
[http://welcome.hp.com/country/us/en/contact\\_us.html](http://welcome.hp.com/country/us/en/contact_us.html)
- In the United States, call 1-800-HP-INVENT (1-800-474-6836) to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.
- In other locations, see the Contact HP Worldwide website for contact options:  
<http://welcome.hp.com/country/us/en/wwcontact.html>

### Security bulletin and alert policy for non-HP owned software components

Open source software (such as OpenSSL) or third-party software (such as Java) are sometimes included in HP products. HP discloses that the non-HP owned software components listed in the Insight Management end user license agreement (EULA) are included with Insight Management. The EULA is included with the Insight Management Installer on Insight Management DVD #1.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

When a security defect is found, HP has a well defined process that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

### Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

[http://www.hp.com/country/us/en/contact\\_us.html](http://www.hp.com/country/us/en/contact_us.html)

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

### Registering for software technical support and update service

Insight Management includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP. Customers who purchase an electronic license are eligible for electronic updates.

With this service, Insight Management customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

<http://www.hp.com/services/insight>

Registration for this service takes place following online redemption of the license certificate.

## How to use your software technical support and update service

As HP releases updates to software, the latest versions of the software and documentation are made available to you. The Software Updates and Licensing portal gives you access to software, documentation, and license updates for products on your HP software support agreement.

You can access this portal from the HP Support Center:

<http://www.hp.com/go/hpsc>

After creating your profile and linking your support agreements to your profile, see the Software Updates and Licensing portal at <http://www.hp.com/go/hpsoftwareupdatesupport> to obtain software, documentation, and license updates.

## HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator web site:  
[http://www.hp.com/service\\_locator](http://www.hp.com/service_locator)
- In other locations, see the Contact HP worldwide web site:  
<http://welcome.hp.com/country/us/en/wwcontact.html>

## Related information

### Documents

- *HP iLO User Guide*
- *HP iLO Release Notes*

These documents are on the HP website at:

<http://www.hp.com/go/ilo/docs>

### Websites

- iLO website:  
<http://www.hp.com/go/ilo>
- iLO 4 website:  
<http://h20000.www2.hp.com/bizsupport/TechSupport/SupportResources.jsp?lang=en&cc=us&prodTypeId=329290&prodSeriesId=5219994>
- iLO 4 downloads website:  
<http://www.hp.com/support/ilo4>
- Insight Control website:  
<http://www.hp.com/go/insightcontrol>

- Intel IPMI specification website:  
<http://www.intel.com/design/servers/ipmi/tools.htm>
- Timezone information:  
<ftp://ftp.iana.org/tz/>
- HP iLO videos:  
<http://www.hp.com/go/ilo/videos>

---

## 13 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hp.com](mailto:docsfeedback@hp.com)). Include the document title and part number, version number, or the URL when submitting your feedback.

# A Sample script and command reference

The HP Lights-Out XML Scripting Sample bundle contains sample scripts that you can modify as needed for use in your environment. [Table 32 \(page 202\)](#) lists all the available sample scripts and the related command for each.

**Table 32 Sample scripts and related commands**

<b>Sample script</b>	<b>Related Command</b>
Add_Federation_Group.xml	ADD_FEDERATION_GROUP
add_sso_rec.xml	SSO_SERVER
Add_User.xml	ADD_USER
Administrator_reset_pw.xml	MOD_USER
Cert_Request.xml	CERTIFICATE_SIGNING_REQUEST
Change_Password.xml	MOD_USER
Clear_AHS_Data.xml	AHS_CLEAR_DATA
Clear_EventLog.xml	CLEAR_EVENTLOG
Clear_IML.xml	CLEAR_IML
Clear_Power_On_Time.xml	CLEAR_SERVER_POWER_ON_TIME
Computer_Lock_Config.xml	COMPUTER_LOCK_CONFIG
Delete_Federation_Group.xml	DELETE_FEDERATION_GROUP
Delete_SSH_Key.xml	MOD_USER
delete_sso_rec.xml	DELETE_SERVER
Delete_User.xml	DELETE_USER
Eject_Virtual_Media.xml	EJECT_VIRTUAL_MEDIA_DEVICE
ERS_AHS_Submit.xml	TRIGGER_BB_DATA
ERS_DC_CompleteRegistration.xml	DC_REGISTRATION_COMPLETE
ERS_DC_RegisterDevice.xml	SET_ERS_DIRECT_CONNECT
ERS_DC_SetWebProxy.xml	SET_ERS_WEB_PROXY
ERS_Disable.xml	DISABLE_ERS
ERS_Get_Settings.xml	GET_ERS_SETTINGS
ERS_IRS_Enable.xml	SET_ERS_IRS_CONNECT
ERS_L2_Collection_Submit.xml	TRIGGER_L2_COLLECTION
ERS_Test_Event_Submit.xml	TRIGGER_TEST_EVENT
Factory_Defaults.xml	FACTORY_DEFAULTS
Get_AHS_Status.xml	GET_AHS_STATUS
Get_All_Languages.xml	GET_ALL_LANGUAGES
Get_All_Licenses.xml	GET_ALL_LICENSES
Get_All_Users.xml	GET_ALL_USERS
Get_All_User_Info.xml	GET_ALL_USER_INFO

**Table 32 Sample scripts and related commands** *(continued)*

Get_Asset_Tag.xml	GET_ASSET_TAG
Get_Boot_Mode.xml	GET_PENDING_BOOT_MODE
Get_Current_Boot_Mode.xml	GET_CURRENT_BOOT_MODE
Get_Directory.xml	GET_DIR_CONFIG
get_discovery_services.xml	GET_SPATIAL
Get_Embedded_Health.xml	GET_EMBEDDED_HEALTH
Get_EmHealth.xml	GET_EMBEDDED_HEALTH
Get_Encrypt.xml	GET_ENCRYPT_SETTINGS
Get_Federation_All_Groups.xml	GET_FEDERATION_ALL_GROUPS
Get_Federation_All_Groups_Info.xml	GET_FEDERATION_ALL_GROUPS_INFO
Get_Federation_Group.xml	GET_FEDERATION_GROUP
Get_Federation_Multicast_Options.xml	GET_FEDERATION_MULTICAST
Get_FIPS_Status.xml	GET_FIPS_STATUS
Get_FW_Version.xml	GET_FW_VERSION
Get_Global.xml	GET_GLOBAL_SETTINGS
Get_Host_APO.xml	GET_SERVER_AUTO_PWR
Get_Host_Data.xml	GET_HOST_DATA
Get_Host_Power.xml	GET_HOST_POWER_STATUS
Get_Host_Power_Saver.xml	GET_HOST_POWER_SAVER_STATUS
Get_Host_Pwr_Micro_Ver.xml	GET_HOST_PWR_MICRO_VER
Get_Hotkey_Config.xml	GET_HOTKEY_CONFIG
Get_iLO_Log.xml	GET_EVENT_LOG
Get_IML.xml	GET_EVENT_LOG
Get_language.xml	GET_LANGUAGE
Get_Network.xml	GET_NETWORK_SETTINGS
Get_OA_Info.xml	GET_OA_INFO
Get_One_Time_Boot_Order.xml	GET_ONE_TIME_BOOT
Get_Persistent_Boot_Order.xml	GET_PERSISTENT_BOOT
Get_Persmouse_Status.xml	GET_PERS_MOUSE_KEYBOARD_ENABLED
Get_PowerCap.xml	GET_POWER_CAP
Get_Power_On_Time.xml	GET_SERVER_POWER_ON_TIME
Get_Power_Readings.xml	GET_POWER_READINGS
Get_Product_Name.xml	GET_PRODUCT_NAME
Get_Pwreg_Alert_Threshold.xml	GET_PWREG
Get_Rack_Settings.xml	GET_RACK_SETTINGS
Get_Security_Msg.xml	GET_SECURITY_MSG
Get_Server_FQDN.xml	GET_SERVER_FQDN and GET_SMH_FQDN

**Table 32 Sample scripts and related commands** *(continued)*

Get_Server_Name.xml	GET_SERVER_NAME
Get_SNMP_IM.xml	GET_SNMP_IM_SETTINGS
Get_SSO_Settings.xml	GET_SSO_SETTINGS
Get_Supported_Boot_Mode.xml	GET_SUPPORTED_BOOT_MODE
Get_TPM_Status.xml	GET_TPM_STATUS
Get_UID_Status.xml	GET_UID_STATUS
Get_User.xml	GET_USER
Get_VM_Status.xml	GET_VM_STATUS
Hotkey_Config.xml	HOTKEY_CONFIG
Import_Cert.xml	IMPORT_CERTIFICATE
Import_SSH_Key.xml	IMPORT_SSH_KEY
Insert_Virtual_Media.xml	INSERT_VIRTUAL_MEDIA
License.xml	LICENSE
Lock_Configuration.xml	MOD_GLOBAL_SETTINGS
Mod_Directory.xml	MOD_DIR_CONFIG
Mod_Encrypt_Settings.xml	MOD_ENCRYPT_SETTINGS
Mod_Federation_Group.xml	MOD_FEDERATION_GROUP
Mod_Global_Settings.xml	MOD_GLOBAL_SETTINGS
Mod_Kerberos_Config.xml	MOD_DIR_CONFIG
Mod_Network_Settings.xml	MOD_NETWORK_SETTINGS
Mod_Schemaless_Directory.xml	MOD_DIR_CONFIG
Mod_SNMP_IM_Settings.xml	MOD_SNMP_IM_SETTINGS
Mod_SSO_Settings.xml	MOD_SSO_SETTINGS
Mod_User.xml	MOD_USER
Mod_VLAN.xml	MOD_NETWORK_SETTINGS
Mod_VM_Port_Settings.xml	MOD_GLOBAL_SETTINGS
Profile_Apply.xml	PROFILE_APPLY
Profile_Apply_Get_Results.xml	PROFILE_APPLY_GET_RESULTS
Profile_Desc_Delete.xml	PROFILE_DELETE
Profile_Desc_Download.xml	PROFILE_DESC_DOWNLOAD
Profile_Desc_List.xml	PROFILE_LIST
RBSU_POST_IP.xml	MOD_GLOBAL_SETTINGS
Reset_RIB.xml	RESET_RIB
Reset_Server.xml	RESET_SERVER
Set_AHS_Status.xml	SET_AHS_STATUS
Set_Asset_tag.xml	SET_ASSET_TAG
Set_Boot_Mode.xml	SET_PENDING_BOOT_MODE

**Table 32 Sample scripts and related commands** *(continued)*

Set_Brownout.xml	MOD_GLOBAL_SETTINGS
Set_Federation_Multicast_Options.xml	SET_FEDERATION_MULTICAST
Set_FIPS_Enable.xml	FIPS_ENABLE
Set_Host_APO.xml	SERVER_AUTO_PWR
Set_Host_Power.xml	SET_HOST_POWER
Set_Host_Power_Saver.xml	SET_HOST_POWER_SAVER
Set_Language.xml	SET_LANGUAGE
Set_One_Time_Boot_Order.xml	SET_ONE_TIME_BOOT
Set_Persistent_Boot_Order.xml	SET_PERSISTENT_BOOT
Set_Persmouse_Status.xml	SET_PERS_MOUSE_KEYBOARD_ENABLED
Set_PowerCap.xml	SET_POWER_CAP
Set_Pwreg_Alert_Threshold.xml	SET_PWREG
Set_Security_Msg.xml	SET_SECURITY_MSG
Set_Server_FQDN.xml	SERVER_FQDN and SMH_FQDN
Set_Server_Name.xml	SERVER_NAME
Set_Virtual_Power_BTN.xml	PRESS_PWR_BTN COLD_BOOT_SERVER WARM_BOOT_SERVER HOLD_PWR_BTN
Set_VM_Status.xml	SET_VM_STATUS
Shared_Network_Port.xml	MOD_NETWORK_SETTINGS
UID_Control.xml	UID_CONTROL
Update_Firmware.xml	UPDATE_RIB_FIRMWARE
Update_Language.xml	UPDATE_LANG_PACK

---

# Glossary

<b>AHS</b>	Active Health System
<b>ARP</b>	Address Resolution Protocol
<b>ASCII</b>	American Standard Code for Information Interchange.
<b>CGI</b>	Common Gateway Interface.
<b>CLI</b>	Command-line interface. An interface comprised of various commands which are used to control operating system responses.
<b>CLP</b>	Command Line Protocol.
<b>CPQLOCFG</b>	Compaq Lights-Out Configuration Utility
<b>DAD</b>	Duplicate Address Detection
<b>DDNS</b>	Dynamic Domain Name System.
<b>DHCP</b>	Dynamic Host Configuration Protocol.
<b>DMTF</b>	Desktop Management Task Force
<b>DNS</b>	Domain Name System.
<b>EV</b>	Environment Variable
<b>FQDN</b>	Fully Qualified Domain Name
<b>GUI</b>	Graphical user interface.
<b>HPONCFG</b>	HP Lights-Out Online Configuration Utility.
<b>HPQLOCFG</b>	HP Lights-Out Configuration Utility.
<b>HPQLOMGC</b>	HP Lights-Out Migration Command Line.
<b>ICMP</b>	Internet Control Message Protocol.
<b>iLO</b>	Integrated Lights-Out.
<b>IML</b>	Integrated Management Log.
<b>IP</b>	Internet Protocol.
<b>IPMI</b>	Intelligent Platform Management Interface.
<b>LAN</b>	Local area network. A communications infrastructure designed to use dedicated wiring over a limited distance (typically a diameter of less than five kilometers) to connect to a large number of intercommunicating nodes. Ethernet and token ring are the two most popular LAN technologies. (SNIA)
<b>LDAP</b>	Lightweight Directory Access Protocol.
<b>LED</b>	Light-emitting diode.
<b>LOCFG.PL</b>	The Lights-Out Configuration Utility is a PERL script that runs on any client that has a compatible PERL environment installed.
<b>LOM</b>	Lights-Out Management.
<b>MAC</b>	Media Access Control.
<b>NIC</b>	Network interface card. A device that handles communication between a device and other devices on a network.
<b>NMI</b>	Non-maskable interrupt.
<b>PERL</b>	Practical Extraction and Report Language.
<b>POST</b>	Power-on self test.
<b>RA</b>	Router Advertisement
<b>RBSU</b>	ROM-Based Setup Utility.
<b>RDP</b>	HP Rapid Deployment Pack.
<b>RIB</b>	Remote Insight Board.
<b>RIBCL</b>	Remote Insight Board Command Language.

<b>RILOE</b>	Remote Insight Lights-Out Edition.
<b>RILOE II</b>	Remote Insight Lights-Out Edition II.
<b>RMCP</b>	Remote Management and Control Protocol
<b>RSA</b>	An algorithm for public-key cryptography.
<b>RSM</b>	Remote Server Management.
<b>SAID</b>	Service Agreement Identifier
<b>SLAAC</b>	Stateless Address Auto Configuration
<b>SMASH</b>	Systems Management Architecture for Server Hardware.
<b>SNMP</b>	Simple Network Management Protocol.
<b>SSH</b>	Secure Shell.
<b>SSL</b>	Secure Sockets Layer.
<b>SUM</b>	Software Update Manager
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol.
<b>UID</b>	Unit identification.
<b>USB</b>	Universal serial bus. A serial bus standard used to interface devices.
<b>VM</b>	Virtual Machine.
<b>VSP</b>	Virtual Serial Port
<b>WINS</b>	Windows Internet Name Service.
<b>XML</b>	eXtensible markup language.

# Index

## A

- ADD\_USER, 69
  - obtaining the basic configuration, 27
  - parameters, 70
  - runtime errors, 70
- AHS\_CLEAR\_DATA, 117
  - parameters, 117
  - runtime errors, 117
- authorized resellers, 199

## B

- BLADESYSTEM\_INFO, 146
- boot commands, 56
- BROWNOUT\_RECOVERY, 101
  - parameters, 101
  - runtime errors, 101

## C

- certificate, settings
  - CERTIFICATE\_SIGNING\_REQUEST parameters, 116
  - IMPORT\_CERTIFICATE, 116
- CERTIFICATE\_SIGNING\_REQUEST, 115
  - errors, 116
  - parameters, 116
- CLEAR\_EVENTLOG, 86
  - parameters, 86
  - runtime errors, 86
- CLEAR\_SERVER\_POWER\_ON\_TIME, 182
- CLP base commands, 37
- CLP, boot commands, 56
- CLP, embedded health settings, 45
- CLP, escape commands, 36
- CLP, license commands, 49
- CLP, miscellaneous commands, 63
- CLP, network commands, 41
- CLP, SNMP settings, 47
- CLP, user commands, 38
- CLP, using, 35
- CLP, virtual media commands, 51
- COLD\_BOOT\_SERVER, 177
  - parameters, 177
  - runtime errors, 177
- command block, DIR\_INFO, 138
- command block, RIB\_INFO, 76
- command block, SERVER\_INFO, 147
- command block, USER\_INFO, 69
- command line utilities
  - HPONCFG.EXE, 14
  - HPQLOCFG.EXE, 14
  - IPMI, 15
  - LOCFG.PL, 14
  - Scripting and command line utilities, 13
  - SMASH CLP, 14
- command-line parameters, HPONCFG, 26
- commands

- firmware, 54
  - LED, 59
- commands, base, 37
- commands, blade, 56
- commands, network, 41
- commands, user, 38
- commands, virtual media, 51
- COMPUTER\_LOCK\_CONFIG, 86
  - parameters, 87
  - runtime errors, 87
- configuration procedures
  - Obtaining a specific configuration, 28
  - obtaining the basic configuration, 27
  - Setting a configuration, 29
- configuration utilities, 24
- configuration, capturing, 29
- configuration, obtaining specific information, 28
- configuration, restoring, 30
- configuration, setting a configuration, 29
- contacting HP, 198

## D

- data types, RIBCL, 65
- dedicated NIC, re-enabling, 196
- DELETE\_SERVER, 187
  - parameters, 187
  - runtime errors, 187
- DELETE\_USER, 71
  - parameters, 71
  - runtime errors, 71
- DIR\_INFO command block, 138
- directory commands, 49
- DISABLE\_ERS, 119
  - parameters, 119
  - runtime errors, 119
- documentation
  - providing feedback on, 201
- domain name system (DNS)
  - GET\_NETWORK\_SETTINGS return messages, 88
  - HPQLOCFG parameters, 20
  - MOD\_NETWORK\_SETTINGS, 89
  - obtaining the basic configuration, 27
  - Opening an SSL connection, 193
- Dynamic Host Configuration Protocol (DHCP)
  - GET\_NETWORK\_SETTINGS return messages, 88
  - MOD\_NETWORK\_SETTINGS, 89
  - obtaining the basic configuration, 27

## E

- EJECT\_VIRTUAL\_MEDIA, 112
  - parameters, 112
  - runtime errors, 112
- embedded health settings, CLP, 45
- ERS\_AHS\_Submit, 118
  - parameters, 119
  - runtime errors, 119

eventlog commands, CLP, 55  
eventlog commands, RIBCL  
  CLEAR\_EVENT\_LOG, 86  
  GET\_EVENT\_LOG, 77

## F

FACTORY\_DEFAULTS, 137  
features, SSH, 188  
FIPS\_ENABLE, 135  
firmware, 54  
firmware commands, 54

## G

GET\_AHS\_STATUS , 117  
  parameters, 118  
  runtime errors, 118  
GET\_ALL\_LANGUAGES, 124  
  parameters, 124  
  runtime errors, 124  
GET\_ALL\_LICENSES, 136  
GET\_ALL\_USERS, 74  
  parameters, 75  
  return messages, 75  
  runtime errors, 75  
GET\_ALL\_USERS\_INFO, 75  
  parameters, 75  
  return messages, 76  
  runtime errors, 76  
GET\_ASSET\_TAG, 124  
  parameters, 124  
  runtime errors, 124  
GET\_DIR\_CONFIG, 138  
  parameters, 139  
  runtime errors, 139  
GET\_DISCOVERY\_SERVICES, 126  
GET\_EMBEDDED\_HEALTH, 159  
  parameters, 160  
  return messages, 160  
GET\_ERS\_SETTINGS, 119  
  parameters, 119  
  runtime errors, 119  
GET\_EVENT\_LOG, 77  
  parameters, 77  
  return messages, 78  
  runtime errors, 78  
GET\_FIPS\_STATUS, 136  
GET\_FIRMWARE\_VERSION, 109  
  parameters, 109  
  return messages, 110  
  runtime errors, 110  
GET\_GLOBAL\_SETTINGS, 96  
  runtime errors, 96  
  parameters, 96  
GET\_HOST\_POWER\_SAVER\_STATUS, 172  
  parameters, 172  
  return messages, 172  
  runtime errors, 172  
GET\_HOST\_POWER\_STATUS, 173  
  parameters, 173

  return messages, 174  
  runtime errors, 174  
GET\_HOST\_PWR\_MICRO\_VER, 174  
  parameters, 175  
  return messages, 175  
  runtime errors, 175  
GET\_LANGUAGE, 123  
  parameters, 124  
  runtime errors, 124  
GET\_NETWORK\_SETTINGS, 87  
  parameters, 87  
  return messages, 88  
  runtime errors, 87  
GET\_OA\_INFO, 147  
GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED, 181  
GET\_POWER\_CAP, 171  
  parameters, 171  
  return messages, 171  
GET\_POWER\_READINGS, 168  
  parameters, 168  
  return messages, 169  
GET\_PRODUCT\_NAME, 159  
GET\_SECURITY\_MSG, 125  
  parameters, 125  
  runtime errors, 126  
GET\_SERVER\_AUTO\_PWR, 179  
  parameters, 179  
  return message, 179  
GET\_SERVER\_FQDN, 157  
GET\_SERVER\_NAME, 156  
  return messages, 157  
  runtime errors, 157  
GET\_SERVER\_POWER\_ON\_TIME, 181  
GET\_SMH\_FQDN, 157  
GET\_SNMP\_IM\_SETTINGS, 101  
  parameters, 101  
  return messages, 102  
  runtime errors, 101  
GET\_SPATIAL, 126  
  parameters, 127  
  runtime errors, 128  
GET\_SSO\_SETTINGS, 183  
  parameters, 183  
  return messages, 183  
GET\_UID\_CONTROL  
  errors, 180  
  parameters, 180  
GET\_UID\_STATUS, 179  
  parameters, 180  
  response, 180  
GET\_USER, 72  
  parameters, 72  
  return messages, 72  
  runtime errors, 72  
GET\_VM\_STATUS, 112  
  parameters, 113  
  return messages, 113  
  runtime errors, 113

## H

- help
  - obtaining, 198
- HOLD\_PWR\_BTN, 176
  - parameters, 177
  - runtime errors, 177
- HP
  - technical support, 198
- HP Insight Control server deployment, 16
- HP Insight Control software, 16
- HP SIM, application launch, 19
- HP SIM, grouping LOM devices, 19
- HP SIM, integration, 189
- HP SSO settings, 39
- HPONCFG, 24
  - HPONCFG, commands, 26
  - HPONCFG, configuration examples
    - obtaining the basic configuration, 27
    - Setting a configuration, 29
  - HPONCFG, iLO configuration examples
    - Capturing and restoring a configuration, 30
    - Obtaining a specific configuration, 28
  - HPONCFG, installation, 24
  - HPONCFG, installing on a Linux server, 25
  - HPONCFG, installing with VMware, 25
  - HPONCFG, Linux
    - Using HPONCFG on Linux servers, 27
    - Using HPONCFG on Windows servers, 26
    - Windows server installation, 25
  - HPONCFG, online configuration utility, 24
  - HPONCFG, parameters, 26
  - HPONCFG, requirements, 24
    - HPONCFG supported operating systems, 24
  - HPONCFG, using
    - HPONCFG online configuration utility, 24
    - Installing HPONCFG, 24
    - Using HPONCFG on Windows servers, 26
  - HPONCFG, utility overview, 25
  - HPONCFG, variable substitution, 29
  - HPONCFG.EXE utility, 14
- HPQLOCFG, batch processing, 19
- HPQLOCFG.EXE utility
  - HPQLOCFG.EXE, 14
- HPQLOCFG.EXE, parameters, 20

## I

- iLO 4 settings, 44
- iLO ports, 196
- iLO settings, RIBCL, 76
- IMPORT\_CERTIFICATE, 116
  - errors, 117
  - parameters, 117
- IMPORT\_SSH\_KEY, 137
  - parameters, 138
  - runtime errors, 138
- importing SSH keys, PuTTY, 190
- INSERT\_VIRTUAL\_MEDIA, 111
  - parameters, 111
  - runtime errors, 112

- installation, Windows server, 25
- integration, HP Insight Control Software, 16
- introduction, 13
- IPMI (Intelligent Platform Management Interface), 15
- IPMI tool usage, 33
- IPMI tool usage, advanced, 33
- IPMI usage, 33
- IPMI util usage on Windows, 34
- IPMI utility, 33

## L

- LED comamnds, 59
- LICENSE, 110
  - parameters, 110
  - runtime errors, 110
- license commands, CLP, 49
- Lights-Out Configuration Utility *see* HPQLOCFG
- LOCFG.PL utility
  - LOCFG.PL, 14
  - LOCFG.PL usage, 23
- LOGIN
  - BLADESYSTEM\_INFO, 146
  - command block, 68
  - parameters, 69
  - runtime errors, 69

## M

- management port, 196
- MOD\_DIR\_CONFIG, 141
  - parameters, 143
  - runtime errors, 145
- MOD\_GLOBAL\_SETTINGS, 97
  - BROWNOUT\_RECOVERY, 101
  - parameters, 98
  - runtime errors, 100
- MOD\_NETWORK\_SETTINGS, 89
  - obtaining the basic configuration, 27
  - parameters, 92
  - runtime errors, 92
- MOD\_SNMP\_IM\_SETTINGS, 102
  - parameters, 104
  - runtime errors, 105
- MOD\_SSO\_SETTINGS, 184
  - parameters, 184
  - runtime errors, 185
- MOD\_USER, 73
  - ADD\_USER, 69
  - parameters, 73
  - runtime errors, 74
- Mxagentoconfig utility, 189

## N

- network settings, CLP, 41
- NIC management port, re-enabling, 196

## O

- online configuration utility, 24
- OpenSSH utility, 188
- operating systems supported, 24

overview, HPONCFG, 24  
overview, PERL scripting, 193  
overview, SSH, 188

## P

Perl, sending XML scripts, 194  
Perl, SSL connection, 193  
PERL, using, 193  
power management  
  HP Insight Control Software deployment, 16  
PRESS\_PWR\_BTN  
  parameters, 176  
  runtime errors, 176  
PROFILE\_APPLY, 130  
  parameters, 130  
  runtime errors, 130  
PROFILE\_APPLY\_GET\_RESULTS, 131  
  parameters, 131  
  runtime errors, 132  
PROFILE\_DESC\_DOWNLOAD, 134  
PuTTY utility, 188  
PuTTY, importing SSH keys, 190

## R

RACK\_INFO  
  GET\_OA\_INFO, 147  
RESET\_RIB, 77  
  parameters, 77  
  runtime errors, 77  
RESET\_SERVER, 175  
  HOLD\_PWR\_BTN, 176  
  parameters, 176  
  PRESS\_PWR\_BTN, 176  
  runtime errors, 176  
response definition, RIBCL, 66  
RIB\_INFO  
  ADD\_FEDERATION\_GROUP, 83  
    parameters, 83  
    runtime errors, 84  
  BROWNOUT\_RECOVERY, 101  
  DC\_REGISTRATION\_COMPLETE, 122  
    parameters, 122  
    runtime errors, 122  
  DELETE\_FEDERATION\_GROUP, 85  
    parameters, 85  
    runtime errors, 85  
  GET\_FEDERATION\_ALL\_GROUPS, 80  
    parameters, 80  
    return messages, 81  
    runtime errors, 80  
  GET\_FEDERATION\_ALL\_GROUPS\_INFO, 81  
    parameters, 81  
    return messages, 81  
    runtime errors, 81  
  GET\_FEDERATION\_GROUP, 82  
    parameters, 82  
    return messages, 83  
    runtime errors, 82  
  GET\_FEDERATION\_MULTICAST, 79

  parameters, 79  
  return messages, 79  
  runtime errors, 79  
  MOD\_FEDERATION\_GROUP, 84  
    parameters, 84  
    runtime errors, 85  
  SET\_ERS\_DIRECT\_CONNECT, 121  
    parameters, 121  
    runtime errors, 121  
  SET\_ERS\_WEB\_PROXY, 122  
    parameters, 123  
    runtime errors, 123  
  SET\_FEDERATION\_MULTICAST, 79  
    parameters, 80  
    runtime errors, 80  
RIB\_INFO command block, 76  
RIBCL  
  AHS\_CLEAR\_DATA, 117  
  BLADESYSTEM\_INFO, 146  
  Boolean string, 66  
  CERTIFICATE\_SIGNING\_REQUEST, 115  
  CLEAR\_EVENTLOG, 86  
  CLEAR\_SERVER\_POWER\_ON\_TIME, 182  
  COLD\_BOOT\_SERVER, 177  
  command block, 66  
  COMPUTER\_LOCK\_CONFIG, 86  
  data types, 65  
  DELETE\_SERVER, 187  
  DIR\_INFO, 138  
  DISABLE\_ERS, 119  
  EJECT\_VIRTUAL\_MEDIA, 112  
  ERS\_AHS\_Submit, 118  
  FACTORY\_DEFAULTS, 137  
  FIPS\_ENABLE, 135  
  GET\_AHS\_STATUS, 117  
  GET\_ALL\_LANGUAGES, 124  
  GET\_ALL\_LICENSES, 136  
  GET\_ASSET\_TAG, 124  
  GET\_DIR\_CONFIG, 138  
  GET\_DISCOVERY\_SERVICES, 126  
  GET\_EMBEDDED\_HEALTH, 159  
  GET\_ERS\_SETTINGS, 119  
  GET\_EVENT\_LOG, 77  
  GET\_FIPS\_STATUS, 136  
  GET\_FW\_VERSION, 109  
  GET\_GLOBAL\_SETTINGS, 96  
  GET\_HOST\_POWER\_SAVER\_STATUS, 172  
  GET\_HOST\_POWER\_STATUS, 173  
  GET\_HOST\_PWR\_MICRO\_VER, 174  
  GET\_LANGUAGE, 123  
  GET\_NETWORK\_SETTINGS, 87  
  GET\_OA\_INFO, 147  
  GET\_PERS\_MOUSE\_KEYBOARD\_ENABLED, 181  
  GET\_POWER\_CAP, 171  
  GET\_POWER\_READINGS, 168  
  GET\_PRODUCT\_NAME, 159  
  GET\_SECURITY\_MSG, 125  
  GET\_SERVER\_AUTO\_PWR, 179  
  GET\_SERVER\_FQDN, 157

- GET\_SERVER\_POWER\_ON\_TIME, 181
- GET\_SMH\_FQDN, 157
- GET\_SNMP\_IM\_SETTINGS, 101
- GET\_SPATIAL, 126
- GET\_SSO\_SETTINGS, 183
- GET\_UID\_STATUS, 179
- GET\_VM\_STATUS, 112
- HOLD\_PWR\_BTN, 176
- IMPORT\_CERTIFICATE, 116
- IMPORT\_SSH\_KEY, 137
- INSERT\_VIRTUAL\_MEDIA, 111
- license commands, 110
- LOGIN, 68
- MOD\_DIR\_CONFIG, 141
- MOD\_GLOBAL\_SETTINGS, 97
- MOD\_NETWORK\_SETTINGS, 89
- MOD\_SNMP\_IM\_SETTINGS, 102
- MOD\_SSO\_SETTINGS, 184
- overview, 64
- parameters, 66
- PRESS\_PWR\_BTN, 176
- PROFILE\_APPLY, 130
- PROFILE\_APPLY\_GET\_RESULTS, 131
- PROFILE\_DESC\_DOWNLOAD, 134
- RESET\_RIB, 77
- RESET\_SERVER, 175
- response definitions, 66
- RIB\_INFO commands, 76
- runtime errors, 67
- SERVER\_AUTO\_PWR, 178
- SERVER\_FQDN, 158
- SERVER\_INFO, 147
- SERVER\_NAME, 157
- SET\_AHS\_STATUS, 118
- SET\_ASSET\_TAG, 124
- SET\_ERS\_IRS\_CONNECT, 120
- SET\_HOST\_POWER, 174
- SET\_HOST\_POWER\_SAVER, 173
- SET\_LANGUAGE, 123
- SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED, 180
- SET\_POWER\_CAP, 171
- SET\_SECURITY\_MSG, 126
- SET\_VM\_STATUS, 113
- SMH\_FQDN, 158
- specific string, 66
- SSH, 188
- SSO\_INFO, 182
- SSO\_SERVER, 185
- string, 65
- TRIGGER\_BB\_DATA, 118
- TRIGGER\_L2\_COLLECTION, 120
- TRIGGER\_TEST\_EVENT, 120
- UID\_CONTROL, 180
- UPDATE\_FIRMWARE, 107
- USER\_INFO, 69
- WARM\_BOOT\_SERVER, 177
- XML header, 64

RIBCL XML scripting language, 64

## S

- scripting guide overview, 13
- scripting interface, PERL, 193
- scripting utilities
  - HPONCFG.EXE, 14
  - HPQLOCFG.EXE, 14
  - IPMI, 15
  - LOCFG.PL, 14
  - Scripting and command line utilities , 13
  - SMASH CLP, 14
- scripts
  - HPONCFG online configuration utility, 24
  - Opening an SSL connection, 193
  - Sending the XML header and script body, 194
  - Using HPONCFG on Windows servers, 26
  - using PERL with the XML scripting interface, 193
  - Windows server installation, 25
  - XML header, 64
- Secure Sockets Layer (SSL)
  - Opening an SSL connection, 193
  - Sending the XML header and script body, 194
- SERVER\_AUTO\_PWR, 178
  - parameters, 178
  - runtime errors, 179
- SERVER\_FQDN, 158
- SERVER\_INFO
  - GET\_CURRENT\_BOOT\_MODE, 149
    - parameters, 149
    - return messages, 149
    - runtime errors, 149
  - GET\_ONE\_TIME\_BOOT, 153
    - return messages, 154
  - GET\_PENDING\_BOOT\_MODE, 149
    - parameters, 150
    - return messages, 150
    - runtime errors, 150
  - GET\_PERSISTENT\_BOOT, 150
    - return messages, 151
  - GET\_SUPPORTED\_BOOT\_MODE, 156
    - return messages, 156
    - runtime errors, 156
  - GET\_TPM\_STATUS, 148
    - parameters, 148
    - return messages, 148
    - runtime errors, 148
  - SET\_ONE\_TIME\_BOOT, 154
    - parameters, 155
    - runtime errors, 155
  - SET\_PENDING\_BOOT\_MODE, 150
    - parameters, 150
    - runtime errors, 150
  - SET\_PERSISTENT\_BOOT (Legacy), 151
    - parameters, 152
    - runtime errors, 152
  - SET\_PERSISTENT\_BOOT (UEFI), 152
    - parameters, 153
    - runtime errors, 153
- SERVER\_INFO command block, 147
- SERVER\_NAME, 157

- parameters, 157
- return messages, 157
- runtime errors, 157
- SET\_AHS\_STATUS , 118
  - parameters, 118
  - runtime errors, 118
- SET\_ASSET\_TAG, 124
  - parameters, 125
  - runtime errors, 125
- SET\_ERS\_IRS\_CONNECT, 120
  - parameters, 120
  - runtime errors, 120
- SET\_HOST\_POWER, 174
  - parameters, 173, 174
  - runtime errors, 173, 174
- SET\_HOST\_POWER\_SAVER, 173
- SET\_LANGUAGE, 123
  - parameters, 123
  - runtime errors, 123
- SET\_PERS\_MOUSE\_KEYBOARD\_ENABLED, 180
- SET\_POWER\_CAP, 171
  - parameters, 172
  - runtime errors, 172
- SET\_SECURITY\_MSG, 126
  - parameters, 126
  - runtime errors, 126
- SET\_VM\_STATUS, 113
  - parameters, 114
  - runtime errors, 115
- setup, scripted, 193
- shared network port, enabling, 196
- shared network port, features, 196
- shared ports, 196
- signing request, certificate, 115
- SMASH CLP , 14
  - SMASH CLP command line access, 35
  - SMASH CLP command line overview, 35
  - SMASH CLP scripting language, 35
  - SMASH CLP usage, 32
- SMH\_FQDN, 158
- SNMP settings, CLP, 47
- software
  - technical support, 198
  - update service, 198
- specific commands, 38
- SSH, 188
  - features, 188
  - importing SSH keys from PuTTY, 190
  - importing SSH keys generated using ssh-keygen, 192
  - key authorization, 189
  - key authorization, tool definition files, 189
  - Mxagentoconfig utility, 189
  - overview, 188
- SSH utility, 188
- SSH, connection, 188
- ssh-keygen, 192
- SSL connection, opening, 193
- SSO\_INFO, 182
- SSO\_SERVER, 185

- parameters, 186
- runtime errors, 187
- start and reset commands, 53
- start and reset commands, RIBCL
  - RESET\_RIB, 77
- string
  - RIBCL, 65
  - RIBCL Boolean string, 66
  - RIBCL specific string, 66
- supported operating systems, 24
- system properties , 60
- system target information, RIBCL, 147
- system targets, 60

## T

- technical support, 198
  - HP, 198
- TRIGGER\_BB\_DATA, 118
- TRIGGER\_L2\_COLLECTION, 120
  - parameters, 120
  - runtime errors, 120
- TRIGGER\_TEST\_EVENT, 120
  - parameters, 121
  - runtime errors, 121

## U

- UID\_CONTROL, 180
- UPDATE\_FIRMWARE, 107
  - parameters, 108
  - runtime errors, 108
- user settings, CLP, 38
- USER\_INFO
  - command block, 69

## V

- variable substitution, HPONCFG, 29
- virtual media commands, CLP, 51

## W

- WARM\_BOOT\_SERVER, 177
  - parameters, 178
  - runtime errors, 178
- Windows server installation, 25

## X

- XML (Extensible Markup Language)
  - using PERL with the XML scripting interface, 193
  - XML header, 64
- XML header, 64
  - Sending the XML header and script body, 194
- XML query, unauthenticated, 17
- XML, general guidelines, 193