# HPE iLO 5 Scripting and Command Line Guide

Part Number: 30-E8969F9F-008
Published: July 2026
Edition: 1

# HPE iLO 5 Scripting and Command Line Guide

## Abstract

This document describes how to use RIBCL XML scripts, the SMASH CLP, IPMI, Secure Shell, and PERL scripting with iLO. This document is for the person who installs, administers, and troubleshoots servers and storage systems. Hewlett Packard Enterprise assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Part Number: 30-E8969F9F-008
Published: July 2026
Edition: 1

© Copyright 2017-2026 Hewlett Packard Enterprise Development LP

## Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance 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 the vendor's standard commercial license.

Links to third-party websites will take you outside of the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for the information outside the Hewlett Packard Enterprise website.

## Acknowledgments

Microsoft®, Azure®, Azure Stack®, Azure Stack Hub®, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

Google™ is a trademark of Google Inc.

Google Chrome™ browser is a trademark of Google Inc.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

VMware® is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

Intel® and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

SD is a trademark or registered trademark of SD-3C in the United States, other countries or both.

Thales® and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries.

All third-party marks are property of their respective owners.

# Table of contents


Scripting and command line guide overview....18
Scripting and command-line utilities described in this guide....18
Required utility versions....19
Other scripting and command-line utilities....20
HPQLOCFG....21
Configuring for unauthenticated XML queries....22
Creating a system collection in HPE SIM....24
Launch applications with HPE SIM custom tools....25
Batch processing using HPQLOCFG....26
HPQLOCFG command-line parameters....26
Using quote characters....26
Command line switches....27
Using variables and name value pairs with HPQLOCFG....29
LOCFG.PL....29
LOCFG.PL requirements....30
LOCFG.PL command line switches....30
HPONCFG....31
HPONCFG requirements....32
Installing HPONCFG....32
Windows server installation....33
Linux server installation....33
VMware installation....34
Using HPONCFG on Windows servers....35
HPONCFG command line parameters....35
Using HPONCFG on Linux servers....37
Obtaining the basic configuration....39
Obtaining a specific configuration....40
Setting a configuration....42
Using variable substitution....43
Capturing and restoring a configuration....44
SMASH CLP....44
IPMI....45
The IPMI utility....45
Basic IPMI tool usage....46

Advanced IPMI tool usage on Linux ... 46
Advanced IPMIutil usage on Windows ... 47
SMASH CLP commands ... 48
SMASH CLP command line overview ... 48
SMASH CLP command line access ... 48
Using the command line ... 49
Escape commands ... 51
Base commands ... 52
Using the NIC auto-selection feature ... 57
Specific commands ... 58
User commands ... 59
HPE SSO settings ... 60
Network commands ... 62
iLO 5 settings ... 65
AlertMail settings ... 69
iLO embedded health settings ... 70
SNMP settings ... 74
License commands ... 76
Directory commands ... 77
Virtual Media commands ... 79
Start and Reset commands ... 82
Firmware commands ... 84
Non-iLO firmware commands ... 85
Eventlog commands ... 86
Blade commands ... 87
Boot commands ... 88
LED commands ... 92
System properties and targets ... 93
Other commands ... 98
RIBCL XML Scripting Language ... 99
Remote Insight Board Command Language ... 99
XML headers ... 100
Data types ... 102
String ... 103
Specific string ... 103
Boolean string ... 103
Response definitions ... 104
RIBCL ... 104

RIBCL parameters....105
RIBCL runtime errors....105
Combining multiple commands in one RIBCL script....105
LOGIN....107
LOGIN parameters....108
LOGIN runtime errors....108
USER_INFO....108
ADD_USER....109
ADD_USER parameters....110
ADD_USER runtime errors....111
Password guidelines....112
DELETE_USER....113
DELETE_USER parameter....113
DELETE_USER runtime errors....113
DEL_USERS_SSH_KEY....114
DEL_SSH_KEY parameters....114
DEL_SSH_KEY runtime errors....115
GET_USER....115
GET_USER parameter....116
GET_USER runtime errors....116
GET_USER return messages....116
MOD_USER....116
MOD_USER parameters....118
MOD_USER runtime errors....119
GET_ALL_USERS....119
GET_ALL_USERS parameters....120
GET_ALL_USERS return messages....120
GET_ALL_USER_INFO....121
GET_ALL_USER_INFO parameters....122
GET_ALL_USER_INFO return messages....122
RIB_INFO....123
RESET_RIB....126
RESET_RIB parameters....126
RESET_RIB runtime errors....126
GET_EVENT_LOG....127
GET_EVENT_LOG parameters....128
GET_EVENT_LOG runtime errors....128
GET_EVENT_LOG return messages....128

CLEAR_EVENTLOG ..... 130
CLEAR_EVENTLOG parameters ..... 130
CLEAR_EVENTLOG runtime errors ..... 131
GET_FEDERATION_MULTICAST ..... 131
GET_FEDERATION_MULTICAST parameters ..... 132
GET_FEDERATION_MULTICAST runtime errors ..... 132
GET_FEDERATION_MULTICAST return messages ..... 132
SET_FEDERATION_MULTICAST ..... 132
SET_FEDERATION_MULTICAST parameters ..... 133
SET_FEDERATION_MULTICAST runtime errors ..... 134
GET_FEDERATION_ALL_GROUPS ..... 134
GET_FEDERATION_ALL_GROUPS parameters ..... 135
GET_FEDERATION_ALL_GROUPS runtime errors ..... 135
GET_FEDERATION_ALL_GROUPS return messages ..... 135
GET_FEDERATION_ALL_GROUPS_INFO ..... 136
GET_FEDERATION_ALL_GROUPS_INFO parameters ..... 137
GET_FEDERATION_ALL_GROUPS_INFO runtime errors ..... 137
GET_FEDERATION_ALL_GROUPS_INFO return messages ..... 137
ADD_FEDERATION_GROUP ..... 138
ADD_FEDERATION_GROUP parameters ..... 139
ADD_FEDERATION_GROUP runtime errors ..... 140
DELETE_FEDERATION_GROUP ..... 140
DELETE_FEDERATION_GROUP parameters ..... 141
DELETE_FEDERATION_GROUP runtime errors ..... 141
GET_FEDERATION_GROUP ..... 141
GET_FEDERATION_GROUP parameters ..... 142
GET_FEDERATION_GROUP runtime errors ..... 142
GET_FEDERATION_GROUP return messages ..... 142
MOD_FEDERATION_GROUP ..... 143
MOD_FEDERATION_GROUP parameters ..... 144
MOD_FEDERATION_GROUP runtime errors ..... 145
COMPUTER_LOCK_CONFIG ..... 145
COMPUTER_LOCK_CONFIG parameters ..... 146
COMPUTER_LOCK_CONFIG runtime errors ..... 147
GET_NETWORK_SETTINGS ..... 148
GET_NETWORK_SETTINGS parameters ..... 148
GET_NETWORK_SETTINGS runtime errors ..... 148
GET_NETWORK_SETTINGS return messages ..... 149

MOD_NETWORK_SETTINGS ..... 151
MOD_NETWORK_SETTINGS runtime errors ..... 157
MOD_NETWORK_SETTINGS parameters ..... 157
GET_GLOBAL_SETTINGS ..... 163
GET_GLOBAL_SETTINGS parameters ..... 164
GET_GLOBAL_SETTINGS runtime errors ..... 164
GET_GLOBAL_SETTINGS return messages ..... 164
MOD_GLOBAL_SETTINGS ..... 165
MOD_GLOBAL_SETTINGS parameters ..... 168
MOD_GLOBAL_SETTINGS runtime errors ..... 172
BROWNOUT_RECOVERY ..... 174
BROWNOUT_RECOVERY parameters ..... 174
BROWNOUT_RECOVERY runtime errors ..... 174
GET_SNMP_IM_SETTINGS ..... 175
GET_SNMP_IM_SETTINGS parameters ..... 175
GET_SNMP_IM_SETTINGS runtime errors ..... 176
GET_SNMP_IM_SETTINGS return messages ..... 176
MOD_SNMP_IM_SETTINGS ..... 177
MOD_SNMP_IM_SETTINGS parameters ..... 180
MOD_SNMP_IM_SETTINGS runtime errors ..... 182
SEND_SNMP_TEST_TRAP ..... 182
SEND_SNMP_TEST_TRAP runtime errors ..... 183
SEND_SNMP_TEST_TRAP return messages ..... 183
MOD_ENCRYPT_SETTINGS ..... 183
MOD_ENCRYPT_SETTINGS parameters ..... 184
MOD_ENCRYPT_SETTINGS runtime errors ..... 185
GET_ENCRYPT_SETTINGS ..... 185
GET_ENCRYPT_SETTINGS parameters ..... 186
GET_ENCRYPT_SETTINGS runtime errors ..... 186
GET_ENCRYPT_SETTINGS return messages ..... 186
UPDATE_RIB_FIRMWARE and UPDATE_FIRMWARE ..... 187
UPDATE_FIRMWARE parameters ..... 188
UPDATE_FIRMWARE runtime errors ..... 188
UPDATE_LANG_PACK ..... 189
UPDATE_LANG_PACK parameters ..... 190
UPDATE_LANG_PACK runtime errors ..... 190
GET_FW_VERSION ..... 191
GET_FW_VERSION parameters ..... 191

GET_FW_VERSION runtime errors....192
GET_FW_VERSION return messages....192
LICENSE....192
LICENSE parameters....193
LICENSE runtime errors....193
INSERT_VIRTUAL_MEDIA....194
INSERT_VIRTUAL_MEDIA parameters....194
INSERT_VIRTUAL_MEDIA runtime errors....195
EJECT_VIRTUAL_MEDIA....196
EJECT_VIRTUAL_MEDIA parameters....196
EJECT_VIRTUAL_MEDIA runtime errors....197
GET_VM_STATUS....197
GET_VM_STATUS parameters....198
GET_VM_STATUS runtime errors....198
GET_VM_STATUS return messages....198
SET_VM_STATUS....199
SET_VM_STATUS parameters....200
SET_VM_STATUS runtime errors....202
CERTIFICATE_SIGNING_REQUEST....202
CERTIFICATE_SIGNING_REQUEST parameters (for custom CSR)....203
CERTIFICATE_SIGNING_REQUEST errors....203
IMPORT_CERTIFICATE....204
IMPORT_CERTIFICATE parameters....205
IMPORT_CERTIFICATE errors....205
AHS_CLEAR_DATA....206
AHS_CLEAR_DATA parameters....206
AHS_CLEAR_DATA runtime errors....206
GET_AHS_STATUS....207
GET_AHS_STATUS parameters....207
GET_AHS_STATUS runtime errors....207
SET_AHS_STATUS....208
SET_AHS_STATUS parameters....208
SET_AHS_STATUS runtime errors....209
TRIGGER_BB_DATA....209
TRIGGER_BB_DATA parameters....209
TRIGGER_BB_DATA runtime errors....210
DISABLE_ERS....210
DISABLE_ERS parameters....210

DISABLE_ERS runtime errors....211
GET_ERS_SETTINGS....211
GET_ERS_SETTINGS parameters....211
GET_ERS_SETTINGS runtime errors....212
SET_ERS_IRS_CONNECT....212
SET_ERS_IRS_CONNECT parameters....212
SET_ERS_IRS_CONNECT runtime errors....213
TRIGGER_L2_COLLECTION....213
TRIGGER_L2_COLLECTION parameters....213
TRIGGER_L2_COLLECTION runtime errors....214
TRIGGER_TEST_EVENT....214
TRIGGER_TEST_EVENT parameters....214
TRIGGER_TEST_EVENT runtime errors....215
SET_LANGUAGE....215
SET_LANGUAGE parameters....215
SET_LANGUAGE runtime errors....216
GET_LANGUAGE....216
GET_LANGUAGE parameters....217
GET_LANGUAGE runtime errors....217
GET_ALL_LANGUAGES....217
GET_ALL_LANGUAGES parameters....218
GET_ALL_LANGUAGES runtime errors....218
GET_ASSET_TAG....218
GET_ASSET_TAG parameters....218
GET_ASSET_TAG runtime errors....219
SET_ASSET_TAG....219
SET_ASSET_TAG parameters....220
SET_ASSET_TAG runtime errors....220
GET_SECURITY_MSG....221
GET_SECURITY_MSG parameters....221
GET_SECURITY_MSG return messages....221
GET_SECURITY_MSG runtime errors....222
SET_SECURITY_MSG....222
SET_SECURITY_MSG parameters....223
SET_SECURITY_MSG runtime errors....223
HOTKEY_CONFIG....223
HOTKEY_CONFIG parameters....224
HOTKEY_CONFIG runtime errors....225

GET_HOTKEY_CONFIG ... 226
GET_HOTKEY_CONFIG parameters ... 226
GET_HOTKEY_CONFIG runtime errors ... 226
GET_HOTKEY_CONFIG return messages ... 226
PROFILE_APPLY ... 227
PROFILE_APPLY parameters ... 227
PROFILE_APPLY runtime errors ... 228
PROFILE_APPLY_GET_RESULTS ... 229
PROFILE_APPLY_GET_RESULTS parameters ... 230
PROFILE_APPLY_GET_RESULTS runtime errors ... 230
PROFILE_DELETE ... 230
PROFILE_DELETE parameters ... 231
PROFILE_DELETE runtime errors ... 231
PROFILE_LIST ... 232
PROFILE_LIST parameters ... 233
PROFILE_LIST runtime errors ... 233
PROFILE_DESC_DOWNLOAD ... 233
PROFILE_DESC_DOWNLOAD parameters ... 234
PROFILE_DESC_DOWNLOAD runtime errors ... 235
FIPS_ENABLE ... 236
FIPS_ENABLE parameters ... 237
FIPS_ENABLE runtime errors ... 237
GET_FIPS_STATUS ... 237
GET_FIPS_STATUS parameters ... 238
GET_FIPS_STATUS runtime errors ... 238
GET_FIPS_STATUS return messages ... 238
GET_ALL_LICENSES ... 238
GET_ALL_LICENSES parameters ... 239
GET_ALL_LICENSES runtime errors ... 239
GET_ALL_LICENSES return messages ... 239
FACTORY_DEFAULTS ... 240
FACTORY_DEFAULTS parameters ... 240
FACTORY_DEFAULTS runtime errors ... 240
IMPORT_SSH_KEY ... 241
IMPORT_SSH_KEY parameters ... 242
IMPORT_SSH_KEY runtime errors ... 242
LOCK_CONFIGURATION ... 242
LOCK_CONFIGURATION parameters ... 243

LOCK_CONFIGURATION runtime errors 243
DIR_INFO 243
GET_DIR_CONFIG 244
GET_DIR_CONFIG parameters 245
GET_DIR_CONFIG runtime errors 245
GET_DIR_CONFIG return messages 245
MOD_DIR_CONFIG 248
MOD_DIR_CONFIG parameters 254
MOD_DIR_CONFIG runtime errors 256
IMPORT_LDAP_CA_CERTIFICATE 256
GET_LDAP_CA_CERTIFICATE_STATUS 257
MOD_KERBEROS 258
START_DIR_TEST 258
START_DIR_TEST parameters 259
START_DIR_TEST runtime errors 260
ABORT_DIR_TEST 260
ABORT_DIR_TEST runtime errors 260
GET_DIR_TEST_RESULTS 261
GET_DIR_TEST_RESULTS runtime errors 261
RACK_INFO 261
GET_RACK_SETTINGS 262
GET_RACK_SETTINGS parameters 263
GET_RACK_SETTINGS runtime errors 263
GET_RACK_SETTINGS return messages 263
BLADESYSTEM_INFO 263
GET_OA_INFO 264
GET_OA_INFO parameters 264
GET_OA_INFO runtime errors 265
GET_OA_INFO return messages 265
SERVER_INFO 265
GET_TPM_STATUS 268
GET_TPM_STATUS parameters 268
GET_TPM_STATUS runtime errors 268
GET_TPM_STATUS return messages 269
GET_CURRENT_BOOT_MODE 269
GET_CURRENT_BOOT_MODE parameters 270
GET_CURRENT_BOOT_MODE runtime errors 270
GET_CURRENT_BOOT_MODE return messages 270

GET_PENDING_BOOT_MODE....270
GET_PENDING_BOOT_MODE parameters....271
GET_PENDING_BOOT_MODE runtime errors....271
GET_PENDING_BOOT_MODE return messages....271
SET_PENDING_BOOT_MODE....271
SET_PENDING_BOOT_MODE parameters....272
SET_PENDING_BOOT_MODE runtime errors....272
GET_PERSISTENT_BOOT....272
GET_PERSISTENT_BOOT return messages....273
SET_PERSISTENT_BOOT (Legacy)....274
SET_PERSISTENT_BOOT parameters....275
SET_PERSISTENT_BOOT runtime errors....275
SET_PERSISTENT_BOOT (UEFI)....276
SET_PERSISTENT_BOOT parameters....277
SET_PERSISTENT_BOOT runtime errors....278
GET_ONE_TIME_BOOT....278
GET_ONE_TIME_BOOT return messages....278
SET_ONE_TIME_BOOT....280
SET_ONE_TIME_BOOT parameters....280
SET_ONE_TIME_BOOT runtime errors....281
GET_SDCARD_STATUS....282
GET_SDCARD_STATUS return messages....282
GET_SUPPORTED_BOOT_MODE....283
GET_SUPPORTED_BOOT_MODE return messages....283
GET_SUPPORTED_BOOT_MODE runtime errors....284
GET_SERVER_NAME....284
GET_SERVER_NAME return message....285
GET_SERVER_NAME runtime errors....285
SERVER_NAME....285
SERVER_NAME parameters....286
SERVER_NAME return message....286
SERVER_NAME runtime errors....286
GET_SERVER_FQDN....287
GET_SERVER_FQDN....287
GET_SERVER_FQDN....287
SERVER_FQDN....288
SERVER_FQDN parameters....288
SERVER_FQDN return messages....288

SERVER_FQDN runtime errors....288
GET_PRODUCT_NAME....289
GET_PRODUCT_NAME runtime errors....289
GET_PRODUCT_NAME return messages....289
GET_EMBEDDED_HEALTH....290
GET_EMBEDDED_HEALTH parameters....291
GET_EMBEDDED_HEALTH return messages....291
GET_POWER_READINGS....293
GET_POWER_READINGS parameters....293
GET_POWER_READINGS return messages....293
GET_PWREG....294
GET_PWREG parameters....295
GET_PWREG return messages....295
GET_PWREG runtime errors....295
SET_PWREG....296
SET_PWREG parameters....296
SET_PWREG runtime errors....297
GET_PS_DATA....297
GET_PS_DATA parameters....298
GET_PS_DATA return messages....298
GET_POWER_CAP....298
GET_POWER_CAP parameters....299
GET_POWER_CAP return messages....299
SET_POWER_CAP....299
SET_POWER_CAP parameters....300
SET_POWER_CAP runtime errors....300
SET_CRITICAL_TEMP_REMAIN_OFF....301
SET_CRITICAL_TEMP_REMAIN_OFF parameters....301
SET_CRITICAL_TEMP_REMAIN_OFF runtime errors....301
GET_CRITICAL_TEMP_REMAIN_OFF....302
GET_CRITICAL_TEMP_REMAIN_OFF return messages....302
GET_HOST_POWER_SAVER_STATUS....302
GET_HOST_POWER_SAVER_STATUS parameters....303
GET_HOST_POWER_SAVER_STATUS runtime errors....303
GET_HOST_POWER_SAVER_STATUS return messages....303
SET_HOST_POWER_SAVER....304
SET_HOST_POWER_SAVER parameters....305
SET_HOST_POWER_SAVER runtime errors....305

GET_HOST_POWER_STATUS ..... 306
GET_HOST_POWER_STATUS parameters ..... 306
GET_HOST_POWER_STATUS runtime errors ..... 306
GET_HOST_POWER_STATUS Return Messages ..... 307
SET_HOST_POWER ..... 307
SET_HOST_POWER Parameters ..... 308
SET_HOST_POWER Runtime Errors ..... 308
GET_HOST_PWR_MICRO_VER ..... 308
GET_HOST_PWR_MICRO_VER parameters ..... 309
GET_HOST_PWR_MICRO_VER runtime errors ..... 309
GET_HOST_PWR_MICRO_VER return messages ..... 310
RESET_SERVER ..... 310
RESET_SERVER error messages ..... 311
RESET_SERVER parameters ..... 311
PRESS_PWR_BTN ..... 311
PRESS_PWR_BTN parameters ..... 312
PRESS_PWR_BTN runtime errors ..... 312
HOLD_PWR_BTN ..... 312
HOLD_PWR_BTN parameters ..... 313
HOLD_PWR_BTN runtime errors ..... 313
COLD_BOOT_SERVER ..... 314
COLD_BOOT_SERVER parameters ..... 314
COLD_BOOT_SERVER runtime errors ..... 314
WARM_BOOT_SERVER ..... 315
WARM_BOOT_SERVER parameters ..... 315
WARM_BOOT_SERVER runtime errors ..... 315
SERVER_AUTO_PWR ..... 316
SERVER_AUTO_PWR parameters ..... 317
SERVER_AUTO_PWR runtime errors ..... 317
GET_SERVER_AUTO_PWR ..... 317
GET_SERVER_AUTO_PWR parameters ..... 318
GET_SERVER_AUTO_PWR return message ..... 318
GET_UID_STATUS ..... 319
GET_UID_STATUS parameters ..... 319
GET_UID_STATUS response ..... 320
UID_CONTROL ..... 320
UID_CONTROL parameters ..... 321
UID_CONTROL errors ..... 321

SET_PERS_MOUSE_KEYBOARD_ENABLED....321
SET_PERS_MOUSE_KEYBOARD_ENABLED parameters....322
SET_PERS_MOUSE_KEYBOARD_ENABLED runtime errors....322
GET_PERS_MOUSE_KEYBOARD_ENABLED....322
GET_PERS_MOUSE_KEYBOARD_ENABLED parameters....323
GET_PERS_MOUSE_KEYBOARD_ENABLED return messages....323
GET_SERVER_POWER_ON_TIME....323
GET_SERVER_POWER_ON_TIME parameters....324
GET_SERVER_POWER_ON_TIME return message....324
SSO_INFO....324
GET_SSO_SETTINGS....325
GET_SSO_SETTINGS parameters....326
GET_SSO_SETTINGS return messages....326
MOD_SSO_SETTINGS....327
MOD_SSO_SETTINGS parameters....328
MOD_SSO_SETTINGS runtime errors....329
SSO_SERVER....329
SSO_SERVER parameters....331
SSO_SERVER runtime errors....332
DELETE_SERVER....332
DELETE_SERVER parameters....333
DELETE_SERVER runtime errors....333
Secure Shell....333
SSH overview....334
Supported SSH features....334
Using Secure Shell....335
SSH key authorization....336
Tool definition files....336
Mxagentconfig utility....336
Importing SSH keys from PuTTY....337
Importing SSH keys generated using ssh-keygen....338
PERL scripting....338
Using PERL with the XML scripting interface....339
XML enhancements....339
Opening an SSL connection....340
Sending the XML header and script body....341
iLO ports....343
Enabling the Shared Network Port feature through XML scripting....343

Re-enabling the dedicated NIC management port ..... 344
Sample script and command reference ..... 345
Sample return for GET_EMBEDDED_HEALTH ..... 351
Websites ..... 377
HPE Compute Software and Firmware Product Documentation Quick Links ..... 379
HPE iLO Documentation Quick Links ..... 381
Support and other resources ..... 381
Accessing Hewlett Packard Enterprise Support ..... 381
HPE product registration ..... 382
Accessing updates ..... 382
Remote support ..... 383
Warranty information ..... 383
Regulatory information ..... 384
Documentation feedback ..... 384

# Scripting and command line guide overview

HPE iLO 5 provides multiple ways to configure, update, and operate supported servers. This guide describes the syntax and tools available for using iLO 5 through a command-line or scripted interface.

- The scripting tools and the RIBCL XML scripts help to configure multiple iLO systems and to control servers and subsystems.
- The command-line tools provide quick and easy methods to send commands to the iLO firmware and host servers.

Sample RIBCL XML scripts downloaded from the Hewlett Packard Enterprise website contain commands for all iLO firmware. Unless otherwise specified, the examples in this guide are for iLO 5 version 1.20 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 Hewlett Packard Enterprise **website**.

Starting with iLO 5, some features and capabilities available in the iLO web interface are not supported by the RIBCL XML scripts or the CLI. Hewlett Packard Enterprise recommends using the iLO RESTful API, particularly for setting iLO security states and extended user privileges. The iLO RESTful API is the preferred programmatic interface for Gen10 and later systems, and the preferred CLI or scripting tool is the RESTful Interface Tool (iLOREST).

For more information, see **http://www.hpe.com/info/redfish**.

### Subtopics

**Scripting and command-line utilities described in this guide**
**Other scripting and command-line utilities**

# Scripting and command-line utilities described in this guide

### HPQLOCFG

A Windows command-line utility that sends XML configuration and control scripts over the network to iLO.

For more information, see HPQLOCFG.

### LOCFG.PL

A PERL script that provides functionality similar to the HPQLOCFG utility.

For more information, see LOCFG.PL.

**HPONCFG**

An online configuration tool used to set up and configure iLO from within supported operating systems.

For more information, see HPONCFG.

**SMASH CLP**

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

For more information, see SMASH CLP.

**IPMI**

The IPMI specification defines a standardized interface for platform management. IPMI commands are sent to iLO by using a third-party or open-source utility. Some examples of these utilities are IPMItool, IPMIUTIL, OpenIPMI, and FreeIPMI.

For more information, see IPMI and the HPE iLO 5 IPMI User Guide.

**Subtopics**

**Required utility versions**

# Required utility versions

**Table 1. iLO 5scripting and command-line utility version requirements**

| Utility | Version |
|---|---|
| HPQLOCFG | 6.0.0 |
| HPE Lights-Out XML PERL Scripting Sample for Linux (includes LOCFG.PL) | 6.00.0 |
| HPE Lights-Out XML Scripting Sample for Windows | 6.00.0 |
| HPONCFG for Windows | 6.0.0 |
| HPONCFG for Linux | 6.0.0 |

| Utility | Version |
|---|---|
| HPLOMIG | 6.0.0 |



**NOTE**

RIBCL and the scripting tools including HPQLOCFG, HPE Lights-Out XML PERL Scripting Sample for Linux (includes LOCFG.PL), HPE Lights-Out XML Scripting Sample for Windows, HPONCFG for Windows, HPONCFG for Linux, and HPLOMIG have entered the sustenance stage. HPE will now provide only critical bugs and security fixes for RIBCL and the scripting tools. Hewlett Packard Enterprise recommends using the iLOREST Tool (**Download Pages** and **User Guide**) or iLO RESTful API.

## Other scripting and command-line utilities

The following scripting and command-line tools are described in other guides.

**Scripting Tools for Windows PowerShell: iLO cmdlets**

These cmdlets enable you to do the following:

- Use PowerShell scripts to manage and configure iLO on supported servers.
- Simplify script writing by using the native PowerShell interface.
- Automate tasks from a Windows Management workstation directly to the iLO of servers you are administering.

For more information, see **https://www.hpe.com/info/powershell/docs**.

**iLO RESTful API and RESTful Interface Tool**

iLO includes the iLO RESTful API, which is Redfish API conformant. The iLO RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring tasks by sending basic HTTPS operations (GET, PUT, POST, DELETE, and PATCH) to the iLO web server.

The RESTful Interface Tool (iLOREST) is a scripting tool that allows you to automate Hewlett Packard Enterprise server management tasks. It provides a set of simplified commands that take advantage of the iLO RESTful API. You can install the tool on your computer for remote use or install it locally on a server with Windows or Linux. The iLO RESTful API offers an interactive mode, a scriptable mode, and a file-based mode similar to CONREP to help decrease automation times.

For more information, see **https://www.hpe.com/support/restfulinterface/docs**.

# HPQLOCFG

HPQLOCFG is a Windows-based command-line 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. To run the same script on many iLO devices, run this utility manually from a Windows command prompt or create a batch file.

Download HPQLOCFG from the Hewlett Packard Enterprise **website**.

### Using HPQLOCFG with SIM

HPQLOCFG integrates with HPE SIM for easy launching of the same script on multiple devices. 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 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\Systems 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.
  ```

### HPQLOCFG OS and .NET Framework requirements

If a security state higher than Production is enabled in iLO 5, you must install a supported version of the Microsoft .NET Framework. Additionally, verify that the OS supports enhanced security protocols such as TLS v1.1 and TLS v1.2.

| OS | .NET Framework version | HPQLOCFG with iLO 5 security set to Production | HPQLOCFG with higher security settings [1] |
|---|---|---|---|
| Windows Server 2008 [2] | v4.0 or earlier | ✔ | X |
| | v4.5 or later | ✔ | X |
| Windows 7 and Windows Server 2008 R2 | v4.0 or earlier | ✔ | X |

| OS | .NET Framework version | HPQLOCFG with iLO 5 security set to Production | HPQLOCFG with higher security settings [1] |
|---|---|---|---|
| | v4.5 or later | ✔ | ✔ |
| Windows 8 and Windows Server 2012 | v4.0 or earlier | ✔ | X |
| | v4.5 or later | ✔ | ✔ |
| Windows 10 | v4.6 or later | ✔ | ✔ |
| Windows Server 2016 | v4.6 or later | ✔ | ✔ |
| Windows Server 2019 | v4.7 or later | ✔ | ✔ |

1 An environment in which the iLO 5 security state is set to High Security, FIPS, or CNSA.
2 Certain operating systems, such as Windows Server 2008, do not support TLS v1.1 and TLS v1.2, even with .NET Framework v4.5 or later installed.

**Subtopics**

**Configuring for unauthenticated XML queries**
**Creating a system collection in HPE SIM**
This module describes the process for creating queries in SIM.
**Launch applications with HPE SIM custom tools**
This module describes the process for launching applications using HPE SIM.
**Batch processing using HPQLOCFG**
**HPQLOCFG command-line parameters**

# Configuring for unauthenticated XML queries

**About this task**

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

This setting must be enabled to successfully perform device discoveries with HPE SIM.

**Procedure**

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

   This feature is called **Anonymous Data** in the iLO web interface. You can configure it in the **Network** section on the **Access Settings** page. For more information, see the HPE iLO 5 User Guide.

2. To view unauthenticated identifying information, enter the following command to the iLO web server port:

   **`https://<iloaddress>/xmldata?item=all`**

   You can also view unauthenticated identifying information by clicking **View XML** in the iLO web interface. For more information, see the HPE iLO 5 User Guide.

   A typical response follows:

```
<RIMP>
    <HSI>
        <SBSN>ABC12345678</SBSN>
        <SPN>ProLiant BL460c</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 5 (iLO 5)</PN>
        <FWRI>1.15</FWRI>
        <CID>0x0</CID>
        <BBLK/>
        <HWRI>ASIC: 19</HWRI>
        <SN>ILOdl360genten2345</SN>
        <UUID>ILO679119dl360gente</UUID>
        <IPM>1</IPM>
        <SSO>1</SSO>
        <PWRM>UNKNOWN</PWRM>
        <ERS>0</ERS>
        <EALERT>1</EALERT>
    </MP>
    <HEALTH>
        <STATUS>2</STATUS>
    </HEALTH>
</RIMP>
```

## Creating a system collection in HPE SIM

This module describes the process for creating queries in SIM.

**About this task**

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.

**Procedure**

1. To create a custom group of all iLO devices (or by iLO version), create a system collection.
2. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
3. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections appear.
4. Click **New**. The New Collection section appears.
5. Select **Choose members by attributes**.
6. In the **Search for** dropdown list, select **systems** .
7. In the **where** dropdown, select **system sub type**, and select **is** from the inclusion/exclusion dropdown.
8. Select an Integrated Lights-Out choice from the system sub type dropdown at the right.
9. 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 HPE SIM custom tools

This module describes the process for launching applications using HPE SIM.

Use custom tools in 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 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 HPE Integrated Lights-Out 5 board
REM Repeat line for each board to be updated
REM
HPQLOCFG -S ILO1 -F C:\...SCRIPT.XML -L ILO1LOG.TXT -V
HPQLOCFG -S ILO2 -F C:\...SCRIPT.XML -L ILO2LOG.TXT -V
HPQLOCFG -S ILO3 -F C:\...SCRIPT.XML -L ILO3LOG.TXT -V
.
.
.
HPQLOCFG -S ILO<N> -F C:\...SCRIPT.XML -L ILO<N>LOG.TXT -V
```

HPQLOCFG overwrites any existing log files.

# HPQLOCFG command-line parameters

For information about the syntax of the XML data files, see RIBCL XML Scripting Language.

Download sample XML scripts from the Hewlett Packard Enterprise website: **https://www.hpe.com/support/ilo5**.

### Subtopics

**Using quote characters**
**Command line switches**

# 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 delimeters 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.

When using LOCFG, to enter a username or password containing the exclamation symbol (!) on the command line, use single quotes.

For example:

`'admin!admin'`

## Command line switches

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

**Table 1. 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>).<br>**NOTE**<br>Do not use this switch if you are launching from SIM. 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` [1] | 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.<br>**NOTE**<br>Do not use this switch if launching from SIM.<br>The output values may need to be modified to match the RIBCL syntax. |
| `-V` | 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. |

[1] The `-L` and `-V` switches might or might not be set depending on the IT administrator preferences.

**Subtopics**

**Using variables and name value pairs with HPQLOCFG**

## Using variables and name value pairs with HPQLOCFG

See the scripts below for examples of successfully using name value pairs.

**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.exe -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 50 variables are supported in an XML file. The maximum length of a variable or value is 255 characters.

## LOCFG.PL

The LOCFG.PL scripting utility is a PERL script that provides functionality similar to 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.

LOCFG.PL is included in the HPE Lights-Out XML PERL Scripting Sample for Linux.

**Subtopics**

**LOCFG.PL requirements**
**LOCFG.PL command line switches**

## LOCFG.PL requirements

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

- `Net::SSLeay`
- `IO::Socket::SSL`

You must have a valid iLO user account and password for each XML script. To process the request, your account must have the required iLO privileges.

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

For example:

```
perl locfg.pl -s {servername|ipaddress}[:port] [-l logfilename]
-f input_filename
[-u username -p password] [ilo5]
```

## LOCFG.PL command line switches

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

**Table 1. LOCFG.PL command line switches**

| Switch | Effect |
|---|---|
| `-s servername` or `ipaddress` | servername: DNS name of target server. Do not use this switch if launching from SIM. |
| | ipaddress: IP address of the target server. Do not use this switch if launching from SIM. |
| `:port` | If a port is not specified, the port defaults to `:443`. |
| `-l logfilename` | 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 SIM. |
| `-f input_filename` | Filename containing the RIB commands. |
| `-u username` | Command line user name. Entering this at the command line overrides the user login name from the script. |

| Switch | Effect |
|---|---|
| `-p password` [1] | 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. |
| `-ilo5` | Specifies the type of targeted management processor. This flag is optional. Without this flag, LOCFG.PL detects the iLO type automatically. The iLO 5 firmware performs better when this flag is present. |

[1] Use `-u` and `-p` with caution, because command line options are visible on Linux systems.

For more information, see RIBCL XML Scripting Language.

# HPONCFG

HPONCFG is an online command-line tool you can use to set up and configure iLO from within Windows and Linux operating systems without rebooting the server OS. HPONCFG has both Windows and Linux versions. A limited graphical interface is available for servers that use Windows operating systems. You can download HPONCFG from the Hewlett Packard Enterprise website: **https://www.hpe.com/support/ilo5**.

Typical usage is to select a script that is similar to the required functionality and modify it for your specific requirements. For example, you can use an HPONCFG script to configure iLO to use a standard configuration at the end of the server deployment process.

When you run HPONCFG from the host operating system, you must be logged in to the host server using an Administrator (Windows) or root level (Linux) user account.

An iLO username and password are not required when iLO security is set to Production. However, when you use HPONCFG with iLO security set to any security state higher than Production, a username and password are required.

The **Require Host Authentication** access setting has the following effects on host-based configuration utilities:

- Enabled—Valid credentials are required for using the host-based configuration utilities with all iLO security states.

- Disabled—Valid credentials are not required when iLO is configured to use the Production or High Security security state.

  The **Require Host Authentication** setting cannot be disabled when the FIPS or CNSA security state is used.

Regardless of the authentication requirement, the XML syntax requires that the USER_LOGIN and PASSWORD tags are present in the LOGIN tag, and that these fields contain data.

HPONCFG returns an error message if the user is not assigned sufficient privileges.

**Subtopics**

**HPONCFG requirements**
**Installing HPONCFG**
This module introduces the HPONCFG utility installation instructions for iLO.
**Using HPONCFG on Windows servers**
**Using HPONCFG on Linux servers**
**Obtaining the basic configuration**
**Obtaining a specific configuration**
This module describes the process for obtaining a specific configuration.
**Setting a configuration**
This module describes setting a configuration with HPONCFG.
**Using variable substitution**
**Capturing and restoring a configuration**
This module describes capturing and restoring an HPONCFG configuration.

## HPONCFG requirements

- When using HPONCFG with iLO security set to any state higher than Production, a username and password are required. An error message will be returned by HPONCFG if the user is not assigned sufficient privileges.
- Windows-based servers—The iLO 5 Channel Interface Driver must be loaded on the server.
- Linux-based servers—The `hpilo` driver is required.

## Installing HPONCFG

This module introduces the HPONCFG utility installation instructions for iLO.

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).

Download SPP at **http://www.hpe.com/servers/spp/download**.

**Subtopics**


**Windows server installation**
**Linux server installation**
**VMware installation**


## Windows server installation

HPONCFG installs automatically when the SPP is installed. To install HPONCFG manually, run the self-extracting executable.

HPONCFG creates a directory at:

```
%Program files%\Hewlett Packard Enterprise\HPONCFG
```

Download SPP at **https://www.hpe.com/servers/spp/download**.

## Linux server installation

HPONCFG is installed automatically when the SPP is installed.

You can download the HPONCFG RPM package for Linux distributions from the Hewlett Packard Enterprise 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 6 by entering the following command:

```
rpm -ivh hponcfg-5.x.x-x.x86_64.rpm
```

**IMPORTANT**

The following Linux commands must be installed and working before attempting to use HPONCFG 5.1.0-0 or later on Linux:

- `strings`
- `which`
- `awk`
- `grep`
- `sort`
- `head`
- `ldconfig`
- `xsltproc`

OpenSSL v1.0.x or later is required with iLO 5. If you manually compile and install OpenSSL, or you intentionally relocate `/usr/bin/openssl`, you must set the `PATH` environment variable to direct HPONCFG to the correct version of OpenSSL.

After installation, the HPONCFG executable is located in the `/sbin` directory. Make sure that the appropriate driver is loaded. For more information, see HPONCFG requirements.

## VMware installation

HPONCFG is included with the Hewlett Packard Enterprise custom VMware ESXi 6.5, 6.7, or 7.0 image.

You can download the HPE VMware ESXi Offline Bundles from the following website: **https://vibsdepot.hpe.com/**.

The `hpilo` driver is included in the image (either Hewlett Packard Enterprise custom or standard VMware).

# Using HPONCFG on Windows servers

### About this task

Start the HPONCFG configuration utility from the command line. When using Windows, open a command window by selecting **Start > Run** and entering `cmd`. Change to the `%Program files%\Hewlett Packard Enterprise\HPONCFG` directory and then enter the your commands. Enter `HPONCFG` with no parameters to display a usage page. HPONCFG accepts a correctly formatted XML script.

For more information about formatting XML scripts, see RIBCL XML Scripting Language.

The command line format is:

```
hponcfg /help
hponcfg /m firmwarelevel
hponcfg /reset [/m firmwarelevel][/u username][/p password]
hponcfg /iLO_reboot [/m firmwarelevel][/u username][/p password]
hponcfg /f filename [/l filename][/s namevaluepairs][/u username]
                    [/p password][/m firmwarelevel][/v]
hponcfg /i [/l filename][/s namevaluepairs][/u username][/p password]
           [/m firmwarelevel][/v]
hponcfg [/a] /w filename [/m firmwarelevel][/u username][/p password]
hponcfg /get_hostinfo [/m firmwarelevel][/u username][/p password]
hponcfg /mouse [/dualcursor][/allusers]
hponcfg /display [/allusers]
```

### Subtopics

**HPONCFG command line parameters**
This module describes the status summary parameters.

# HPONCFG command line parameters

This module describes the status summary parameters.

HPONCFG accepts the following command line parameters:

**Table 1. HPONCFG command line parameters in Windows**

| Parameter | Effect |
|---|---|
| `/help` or `/?` | Displays the help page. |
| `/reset` | Resets the iLO to factory default values. |

| Parameter | Effect |
|---|---|
| `/iLO_reboot` | Reboots the iLO without changing any settings. |
| `/f filename` | Sets and receives the iLO configuration from the information given in the XML input file that has name `filename` |
| `/i` | Sets and receives iLO configuration from XML input received through the standard input stream. |
| `/w filename` | Writes the iLO configuration obtained from the device to the XML output file named `filename` |
| `/a` or `/all` | Capture the complete configuration of iLO to a file. Must be used with /w command line parameter. |
| `/l filename` | Logs replies to the text log file that has name `filename` |
| `/v` or `/xmlverbose` | Display all the responses from iLO. |
| `/s namevaluepairs` | Substitutes variables present in the input config file with values specified in `name valuepairs` |
| `/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, HP ONCFG returns an error without performing any additional action |
| `/u` | iLO username. |
| `/p` | iLO password. |
| `/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. |
| `/mouse /dualcursor` | Optimizes mouse handling as suited for remote console dual-cursor mode. |
| `/mouse /allusers` | Optimizes mouse handling for all users in the local registry. |
| `/mouse /dualcursor /allusers` | Optimizes mouse handling as suited for remote console dual-cursor mode for all users in the local registry. |
| `/display` | Configures Windows display parameters to optimize graphical remote console display performance. |

| Parameter | Effect |
| --- | --- |
| `/display /all users` | Configures Windows display parameters to optimize graphical remote console display performance for all users in the local registry. |

These parameters must be preceded by a slash ( `/` ) in as specified in the usage string.

For example:

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

## Using HPONCFG on Linux servers

### About this task

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  -b [-m minFw]
hponcfg  [-a] -w filename [-m minFw]
hponcfg  -g [-m minFw]
hponcfg  -f filename [-l filename] [-s namevaluepair] [-v] [-m minFw]
                     [-u username] [-p password]
hponcfg  -i [-l filename] [-s namevaluepair] [-v] [-m minFw]
            [-u username] [-p password]
```

**Table 1. HPONCFG Linux command line parameters**

| Parameter | Effect |
| --- | --- |
| `-h`<br>`--help`<br>`-?` | Display the help page. |
| `-r`<br>`--reset` | Reset the Management Processor to factory default values. |
| `-b`<br>`--reboot` | Reboots the Management Processor without changing any settings. |

| Parameter | Effect |
|---|---|
| `-f filename`<br>`--file filename` | Sets and receives the Management Processor configuration from the information given in the XML input file that has name *filename*. [1] |
| `-i`<br>`--input` | Sets and receives Management Processor configuration from XML input received through the standard input stream. [1] |
| `-w filename`<br>`--writeconfig filename` | Writes the Management Processor configuration obtained from the device to the XML output file named *filename*. |
| `-a`<br>`--all` | Capture the complete configuration of the Management Processor to a file. Must be used with -w command line parameter. |
| `-l filename`<br>`--log filename` | Logs replies to the text log file that has name *filename*. |
| `-v`<br>`--xmlverbose` | Display all the responses from the Management Processor. |
| `-s namevaluepair`<br>`--substitute namevaluepair` | Substitutes variables present in the input config file with values specified in *namevaluepair*. |
| `-g`<br>`--get_hostinfo` | Receives the host information. Returns the server name and server serial number. |
| `-m`<br>`--minfwlevel` | 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. |
| `-u`<br>`--username` | The iLO username credential of the user initiating the action. [1] |
| `-p`<br>`--password` | The iLO password credential of the user initiating the action. [1] |

[1] When entity processing tags are used inside XML that is passed through the -f or -i option, in addition to using -u and -p to send username and password in high security states, do not use entity substitution for the username and password in the command line. For example, `hponcfg -f filename.xml -u admin -p admin&123`. Do not use `admin&123`.

# Obtaining the basic configuration

### About this task

Use HPONCFG to obtain a basic configuration from iLO 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 of a typical output file, the utility indicates that it obtained the data successfully and wrote the data to the output file:

```
<!-- HPONCFG VERSION = "5.1.0.0" -->
<!-- Generated 09/01/2017 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"/>
    <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 = "hpe.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

This module describes the process for obtaining a specific configuration.

### About this task

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"/>
    <IPMI_DCMI_OVER_LAN_ENABLED VALUE="Y"/>
    <REMOTE_SYSLOG_ENABLE VALUE="N"/>
    <REMOTE_SYSLOG_PORT VALUE="514"/>
    <REMOTE_SYSLOG_SERVER_ADDRESS VALUE="192.0.2.20"/>
    <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>
```

**NOTE**

The key designation in the two parameters F8_PROMPT_ENABLED and F8_LOGIN_REQUIRED refer to previously assigned function keys for starting UEFI/RBSU in previous generations of HPE systems. For Gen10, the key to press for this function has changed to F9. To ensure backward compatibility, the parameter names have not been changed.

## Setting a configuration

This module describes setting a configuration with HPONCFG.

### About this task

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="Username"
        USER_LOGIN="Userlogin"
        PASSWORD="password">
    <ADMIN_PRIV value ="No"/>
    <REMOTE_CONS_PRIV value ="Yes"/>
    <RESET_SERVER_PRIV value ="No"/>
    <VIRTUAL_MEDIA_PRIV value ="No"/>
    <CONFIG_ILO_PRIV value="Yes"/>
    </ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

The specified user is added to the device.

# Using variable substitution

### About this task

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="2.1">
<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="2.1">
<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>
```

### Procedure

- 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

This module describes capturing and restoring an HPONCFG configuration.

### About this task

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 HPE RIBCL format.

### Procedure

1. To capture a configuration, you must specify the name and location of the output file on the command line.

   See Obtaining the basic configuration 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.

2. 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
   ```

## 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.

On iLO, SMASH CLP is accessed through the SSH port.

For more information, see SMASH CLP commands.

# 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 by using a third-party or open-source utility. Some examples of these utilities are IPMItool, IPMIUTIL, OpenIPMI, and FreeIPMI.

You must be familiar with IPMI specifications when issuing raw commands. For additional information, see the **IPMI specification** on the Intel website.

**Subtopics**

**The IPMI utility**
This module describes the IPMI utility.
**Basic IPMI tool usage**
This module describes the Linux IPMI tool utility.
**Advanced IPMI tool usage on Linux**
This module describes advanced IPMI tool usage on Linux
**Advanced IPMIutil usage on Windows**
This module describes the advanced IPMI util usage on windows

# The IPMI utility

This module describes 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 based on your Linux version:

- RHEL6, SLES10, SLES11: `service ipmi start`
- RHEL7, RHEL8, SLES12, RHEL15: `systemctl start ipmi.service`

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

This module describes the Linux IPMI tool utility.

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

This module describes 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 -P password mc info
```

- To power on the ProLiant Server, enter:

```
# ipmitool -H IP Address or FQDN -I lanplus -U user name -P password chassis power on
```

- To turn on the ProLiant Server UID, enter:

```
# ipmitool -H IP Address or FQDN -I lanplus -U user name -P password 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:

`-I lanplus`

## Advanced IPMIutil usage on Windows

This module describes the advanced IPMI util 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 ProLiant server on, enter:

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

- To power the ProLiant server off, enter:

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

- To turn on the ProLiant server UID, enter:

```
C:\> ipmiutil.exe leds -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.

# SMASH CLP commands

**Subtopics**

**SMASH CLP command line overview**
This module describes the overview of SMASH CLP.
**SMASH CLP command line access**
This module describes SMASH CLP access.
**Using the command line**
This module describes HPONCFG utility.
**Escape commands**
**Base commands**
This module describes CLP escape commands.
**Specific commands**
**Other commands**

## SMASH CLP command line overview

This module describes the overview of SMASH CLP.

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

This module describes SMASH CLP access.

The iLO 5 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. Access the iLO CLI by entering `ESC (`
- A network using SSH. This enables multiple 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.

The SSH session starts after authentication. The maximum length of login name is 127 characters and the password length is limited to 63 characters.

> **NOTE**
>
> Enable the **Serial Command Line Interface Status** on the **Security > Access Settings** screen of the iLO 5 web interface before attempting to connect using a serial port connection.

#### Security states and privileges in iLO 5

SMASH CLP does not support the following:

- Setting iLO security states.
- The extended user privileges available from the iLO 5 web interface.
- iLO 5 CNSA/SuiteB security state.

For more information about setting iLO security states or extended user privileges, see the HPE iLO 5 User Guide at **http://www.hpe.com/support/ilo-docs**.

## Using the command line

This module describes HPONCFG utility.

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=INVALID OPTION
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

Escape key commands are shortcuts to popular tasks.

**`ESC R ESC r ESC R`**

Resets the system.

**`ESC ^`**

Powers on the system.

**`ESC ESC`**

Erases the current line.

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

# Base commands

This module describes CLP escape 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 subtargets (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 `/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 namespace.

**`delete`**

Removes instances of the MAP in the namespace.

**`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:

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

SM-CLP Version 1.0
```

### `oemhpe_ping`

The command determines if an IP address is reachable from the current iLO session.

For example:

```
hpiLO-> oemhpe_ping 192.168.1.1
```

Where `192.168.1.1` is the IP address you are testing.

### `oemhpe_clearRESTAPIstate`

The command clears any data cache stored by the HPE RESTful interface.

For example:

```
hpiLO-> oemhpe_clearRESTAPIstate
```

### `oemhpe_ip6`

The command displays the iLO IPv6 settings and allows settings to be changed.

Syntax:

```
oemHPE_ip6 OBJECT [COMMAND [args]] [dev n]
```

| OBJECTS | Explanation |
|---|---|
| addr | Specifies an IPv6 address/prefix for the NIC. |
| route | Specifies an IPv6 route via a gateway. |
| gateway | Specifies an IPv6 address for a gateway. |
| dns | Specifies an IPv6 address for a DNS server. |
| options | Options can be set to yes or no:<br>• IPV6_ACTIVE<br>• SLAAC_ADDR_CFG<br>• DHCPV6_ADDR_CFG<br>• DHCPV6_OTHER_CFG<br>• DHCPV6_RAPID_COMMIT<br>• USE_DHCPV6_DNS<br>• USE_DHCPV6_DOMAIN<br>• USE_DHCPV6_NTP<br>• IPV6_PREFERRED<br>• IPV6_ENABLE_DDNS |
| dev <0\|1> | Specifies the NIC. A value of 1 specifies the sideband NIC. A value of 0 ( zero) specifies the dedicated NIC. If the dev is not specified, the currently active interface will be the target of the command. |

| COMMANDS | Explanation |
|---|---|
| add | Adds the OBJECT. |
| del | Deletes the OBJECT. |
| set | Sets an OPTION to the specified value. |
| default | Returns an OPTION to the default value. |

**NOTE**

The command `set` can only be used when OBJECT=options. The command `default` can be used when OBJECT=options, or can be used alone( `oemHPE_ip6 default` ) to return all IPv6 settings to default. Entering an OBJECT without a COMMAND displays the OBJECT status. Entering just oemhpe_ip6 displays the status for all IPv6 settings related to the active Ethernet device.

For example:

```
</>hpiLO-> oemHPE_ip6 addr  {add | del} <address6/prefix>
</>hpiLO-> oemHPE_ip6 route {add | del} <dest_addr6/prefix> via
<gw_addr6>
</>hpiLO-> oemHPE_ip6 dns   {add | del} <address6>
</>hpiLO-> oemHPE_ip6 gateway {add | del} <address6>
</>hpiLO-> oemHPE_ip6 options <set opt_name>=<value>
</>hpiLO-> oemHPE_ip6 options <default {opt_name | IPV6_ALL}>
</>hpiLO-> oemHPE_ip6 default
```

## `oemhpe_nicautosel`

The command allows iLO to automatically select between either the shared or dedicated network ports at startup. The feature looks for network activity on the ports, and the first port found with network activity is selected for use. Any changes to this setting do not take effect until the iLO is reset.

Syntax:

```
oemhpe_nicautosel Method [sbvlan= <0-4094>] [sbport= <1-2>]
[sbport_limit=<0 or 2>]
[delay=<90-1800>]
```

| Argument | Effect |
|---|---|
| sbvlan | Optional. Specifies the VLAN tag to be used for the shared NIC port. A value of zero disables the VLAN tag. |

| Argument | Effect |
|---|---|
| sbport | Optional. Specifies which port of the shared NIC will be shared with iLO. Verify your server and network adapter can support any values greater than 1. |
| sbport_limit | Optional. Specifies when shared NIC ports will be tested by NIC Auto-selection in addition to the dedicated NIC. Value must be 0 or 2:<br>• 0 = Test only the currently configured port<br>• 2 = Auto mode, tests both shared NIC ports 1 and 2<br>The default is 0. |
| delay | Optional. Specifies the number of seconds to test each NIC connection before moving to the next while searching. Default is 90 seconds. |
| **Methods** | |
| disabled | Disables NIC auto-selection. |
| linkact | Enables NIC auto-selection for any activity detection. |
| rcvdata | Enables NIC auto-selection for received data packet activity detection. |
| dhcp | Enables NIC auto-selection for DHCP address assignment. |

For example:

```
hpilLO-> oemhpe_nicautosel rcvdata
```

This command enables the feature for received data packet activity detection.

**oemHPE_nicfailover**

The command configures the NIC failover feature.

Syntax:

```
oemHPE_nicfailover Method [delay=<30-3600>]
```

| Methods | Effect |
|---|---|
| disabled | Disables NIC failover. |
| linkact | Enables NIC failover to a NIC with any activity detection. |
| rcvdata | Enables NIC failover to a NIC with received data packet activity detection. |
| dhcp | Enables NIC failover to a NIC with a DHCP address assignment. |

| Methods | Effect |
|---|---|
| Argument | |
| delay | Optional. Specifies the number of seconds to test each NIC connection before moving to the next while searching. Default is 300 seconds. |

**NOTE**

The command oemHPE_nicautosel must also be enabled for oemHPE_nicfailover to operate. If not already configured, oemHPE_nicautosel will be enabled for the same Method with a default delay value.

**Subtopics**

**Using the NIC auto-selection feature**

# Using the NIC auto-selection feature

### About this task

To enable the NIC auto-selection feature, do the following:

### Procedure

1. Configure both iLO network ports.

**CAUTION**

If any of the physical NICs are connected to an unsecured network, unauthorized access attempts might occur when iLO is alternating between the iLO network ports. Hewlett Packard Enterprise strongly recommends that whenever iLO is connected to any network:

- Use strong passwords for iLO access.
- Never connect the iLO Dedicated Network Port to an unsecured network.
- If the iLO Shared Network Port is connected to an unsecured network, use VLAN tagging on the iLO portion of the shared NIC, and make sure that the VLAN is connected to a secure network.

2. Before enabling and using the NIC auto-selection feature, both iLO network ports must be configured for their respective network environments.
3. Enable the feature using the CLI command `oemhpe_nicautosel` or by adding the command to the MOD_NETWORK_SETTINGS script.
4. If DHCP Address Assignment is being used for activity detection (`oemhpe_nicautosel dhcp`), then it should be enabled on at least one port with appropriate DHCP options. Either or both of IPv4 or IPv6 address assignment methods can be used. When both IPv4 and IPv6 DHCP is enabled, either protocol being assigned an address will be considered success during searching using DHCP Address Assignment detection.
5. Arrange server cabling as desired, and then reset iLO.
6. The change to NIC auto-selection does not take effect until iLO is reset.

# Specific commands

**Subtopics**

**User commands**
**HPE SSO settings**
**Network commands**
This module describes network commands.
**iLO 5 settings**
This module describes iLO settings.
**AlertMail settings**
**iLO embedded health settings**
**SNMP settings**
**License commands**
**Directory commands**
**Virtual Media commands**
**Start and Reset commands**
This module describes start and reset commands.
**Firmware commands**
**Eventlog commands**
**Blade commands**
**Boot commands**
**LED commands**
**System properties and targets**

# User commands

User commands enable you to view and modify user settings. User settings are available 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 1. User Command Properties**

| Property | Access | Description |
|---|---|---|
| `username` | 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 user name property. |
| `password` | read/write | Corresponds to the password for the current user. |
| `name` | read/write | Corresponds to the iLO login name. |
| `group` | read/write | Specifies the privilege level. The valid values are as follows:<br>• `admin`<br>• `config`<br>• `oemHPE_power`<br>• `oemHPE_rc`<br>• `oemHPE_vm`<br>If you do not specify a group, no privileges are assigned to the user.<br>**NOTE**<br>For backwards compatibility, `oemhp_` is accepted in place of `oemHPE_`. |

### For example

The current path is:

`/map1/accounts1`

- In this example, `username` corresponds to the login name:

  ```
  create username=lname1 password=password
  ```

- In this example, `lname1` is the login name of the user:

  ```
  create /map1/accounts1 username=<lname1> password=<pwd12345>
  name=<dname1> group=<admin,config,oemhpe_vm,oemhpe_rc,oemhpe_power>
  ```

## HPE SSO settings

HPE SSO settings commands are accessed using:

`/map1/oemHPE_ssocfg1`

You must have the Configure iLO Settings privilege to change these properties. SSO is only supported for browser access from trusted SIM servers. SSO is a licensed feature. For more information, see the HPE iLO 5 User Guide at the following website: **http://www.hpe.com/support/ilo-docs**.

### Targets

None

**Table 1. HPE SSO Properties**

| Property | Access | Description |
|---|---|---|
| `oemHPE_ssotrust` | Read/write | The Single Sign-On required trust level. Valid values are :<br>• `disabled`<br>• `all`<br>• `name`<br>• `certificate` |
| `oemHPE_ssouser` | Read/write | The privileges associated with the user role. Valid valu es are:<br>• `login`<br>• `oemHPE_rc`<br>• `oemHPE_power`<br>• `oemHPE_vm`<br>• `config` |

| Property | Access | Description |
|---|---|---|
| | | • `admin` |
| `oemHPE_ssooperator` | Read/write | The privileges associated with the operator role. Valid values are:<br>• `login`<br>• `oemHPE_rc`<br>• `oemHPE_power`<br>• `oemHPE_vm`<br>• `config`<br>• `admin` |
| `oemHPE_ssoadministrator` | Read/write | The privileges associated with the administrator role. Valid values are:<br>• `login`<br>• `oemHPE_rc`<br>• `oemHPE_power`<br>• `oemHPE_vm`<br>• `config`<br>• `admin` |
| `oemHPE_ssoserver` | Read | Contains 0 or more HPE 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/oemHPE_ssocfg1 oemHPE_ssotrust=certificate
  ```

- To assign user roles the Login privilege:

  ```
  </>hpiLO-> set /map1/oemHPE_ssocfg1 oemHPE_ssouser=login
  ```

- To assign the operator role Login, Remote Console, Virtual Power and Reset, and Virtual Media privileges:

  ```
  </>hpiLO-> set /map1/oemHPE_ssocfg1 oemHPE_ssooperator=login,oemHPE_rc,oemHPE_power,oemHPE_vm
  ```

- To Add a SIM Trusted Server name record:

  ```
  </>hpiLO-> cd map1/oemHPE_ssocfg1
  ```

`</map1/oemHPE_ssocfg1>hpiLO-> create hpsim1.corp.net`

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

  `</map1/oemHPE_ssocfg1>hpiLO-> load http://<HPE SIM name or network address>:280/GetCertificate?certtype=sso`

  Or:

  `</map1/oemHPE_ssocfg1>hpiLO-> load https://<HPE SIM name or network address>:50000/GetCertificate?certtype=sso`

- To delete oemHPE_ssoserver with index 5:

  `</map1/oemHPE_ssocfg1>hpiLO-> delete 5`

- To display the complete iLO SSO configuration:

  `</>hpiLO-> cd map1/oemHPE_ssocfg1`

  `</map1/oemHPE_ssocfg1>hpiLO-> show`

## Network commands

This module describes network commands.

The network subsystems are located at:

- `/map1/enetport1`
- `/map1/dhcpendpt1`
- `/map1/dnsendpt1`
- `/map1/gateway1`
- `/map1/dnsserver1`
- `/map1/dnsserver2`
- `/map1/dnsserver3`
- `/map1/settings1`
- `/map1/vlan1`

See also `oemhpe_nicautosel` in Base commands.

**Table 1. /map1/enetport1**

| Targets | Properties |
|---|---|
| lanendpt1 | • `Autosense`<br>• `PermanentAddress`<br>• `LinkTechnology`<br>• `Speed`<br>• `SystemName`<br>• `Fullduplex` |

**For example**

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

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

**Table 2. /map1/dhcpendpt1**

| Targets | Properties |
|---|---|
| None | • `EnabledState`<br>• `OtherTypeDescription` |

**Table 3. /map1/dnsendpt1**

| Targets | Properties |
|---|---|
| None | • `EnabledState`<br>• `HostName`<br>• `DomainName`<br>• `OtherTypeDescription` |

**Table 4. /map1/gateway1**

| Targets | Properties |
|---|---|
| None | • `AccessInfo`<br>• `AccessContext`<br>• `DHCPOptionToUse` |

**Table 5. /map1/dnsserver1, dnsserver2, dnsserver3**

| Targets | Properties |
|---|---|
| None | • `AccessInfo`<br>• `AccessContext` |

**Table 6. /map1/settings1**

| Targets | Properties |
|---|---|
| DNSSettings1 | • `DNSServerAddress`<br>• `RegisterThisConnection`<br>• `DomainName`<br>• `DHCPOptionToUse`<br>• `oemHPE_UseDHCPv4DomainName` |
| WINSSettingData1 | • `WINSServerAddress`<br>• `RegisterThisConnection`<br>• `DHCPOptionToUse` |
| StaticIPSettings1 | • `oemHPE_SRoute1Address`<br>• `oemHPE_Mask1Address`<br>• `oemHPE_Gateway1Address`<br>• `oemHPE_SRoute2Address`<br>• `oemHPE_Mask2Address`<br>• `oemHPE_Gateway2Address`<br>• `oemHPE_SRoute3Address`<br>• `oemHPE_Mask3Address`<br>• `oemHPE_Gateway3Address`<br>• `DHCPOptionToUse` |

**Table 7. /map1/vlan1**

| Targets | Properties |
|---|---|
| None | • `EnabledState` |

| Targets | Properties |
| --- | --- |
| | • `VLANID` |



**NOTE**

Verbs

Network commands are compatible with the following verbs:

- `cd`
- `version`
- `exit`
- `show`
- `set`

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 5 settings

This module describes iLO settings.

The iLO 5 settings commands enable you to view or modify iLO 5 settings. The iLO 5 settings are in `/map1/config1`.

**Targets**

No targets

**Properties**

> **NOTE**
> All iLO properties listed are Read/Write access.

**Table 1. iLO Properties**

| Property | Description |
|---|---|
| oemHPE_mapenable | Enables or disables iLO. Boolean values are accepted. |
| oemHPE_timeout | Displays or modifies idle timeout setting, in minutes. Valid values are 15, 30, 60, and 120. |
| oemHPE_rbsuenable | Enables or disables RBSU prompt during POST. Boolean val ues are accepted. |
| oemHPE_rbsulogin | Enables or disables login requirement for accessing RBSU. Boolean values are accepted. |
| oemHPE_rbsushowip | Enables or disables iLO IP address display during POST. Boolean values are accepted. |
| oemHPE_vsp_log_enable | Enables or disables capture of virtual serial port output fro m the server. |
| oemHPE_httpport | Sets the HTTP port value. |
| oemHPE_sslport | Sets the SSL port value. |
| oemHPE_rcport | Sets remote console port value. |
| oemHPE_vmport | Sets virtual media port value. |
| oemHPE_sshport | Sets the SSH port value. |
| oemHPE_sshstatus | Enables or disables SSH. Boolean values are accepted. |
| oemHPE_serialclistatus | Displays or modifies serial port CLI status setting. Boolean values are accepted. |
| oemHPE_serialcliauth | Displays or modifies serial port CLI authorization status set ting. Boolean values are accepted. |
| oemHPE_serialclispeed | Displays or modifies serial port CLI speed setting. |
| oemHPE_minpwdlen | Displays or modifies minimum password length setting. |

| Property | Description |
| --- | --- |
| oemHPE_enforce_aes | Displays or modifies AES encryption configuration. Valid va lues are 'yes' or 'no'. This setting requires a forced logout fo r the changes to take place.<br>**NOTE**<br>This command is deprecated for iLO 5 1.20 . Instead, use the HPE RESTful API Security State setting. |
| oemHPE_authfailurelogging | Displays or modifies authentication failure logging setting. |
| oemHPE_computer_lock | Displays or modifies Remote Console Computer Lock confi guration. |
| oemHPE_hotkey_ctrl_t,<br>oemHPE_hotkey_ctrl_u,<br>oemHPE_hotkey_ctrl_v,<br>oemHPE_hotkey_ctrl_w,<br>oemHPE_hotkey_ctrl_x,<br>oemHPE_hotkey_ctrl_y | Displays or modifies remote console hotkey configuration. |
| oemHPE_irc_trust_enable | Displays or modifies iLO Trusted Certificate check for Integ rated Remote Console. |
| oemHPE_snmp_access | Displays or modifies SNMP Access. |
| oemHPE_snmp_port | Displays or modifies SNMP port setting. |
| oemHPE_snmp_trapport | Displays or modifies SNMP Trap port setting. |
| oemHPE_fips_enable | Displays or modifies FIPS mode setting. |
| oemHPE_ipmi_dcmi_overlan_enable | Displays or modifies IPMI status setting. Valid values are `yes` or `no`. |
| oemHPE_ipmi_dcmi_overlan_port | Displays or modifies IPMI port setting. Valid value is betwe en `1` and `65535`. |
| oemHPE_ribcl_status | Displays or modifies RIBCL status setting. Valid values are `yes` or `no`. |

| Property | Description |
|---|---|
| oemHPE_webserver_status | Displays or modifies WEB Server status setting. Valid values are `yes` or `no`. |
| oemHPE_webgui_status | Displays or modifies WEB GUI status setting. Valid values are `yes` or `no`. |
| oemHPE_virtual_media_status | Displays or modifies Virtual Media status setting. Valid values are `yes` or `no`. |
| oemHPE_remote_console_status | Displays or modifies Remote Console status setting. Valid values are `yes` or `no`. |

**Verbs**

- cd
- version
- exit
- show
- set
- oemHPE_loadSSHkey
- oemHPE_resetHotkeys
- vsp

**For example**

```
set /map1/config1 oemHPE_mapenable=yes oemHPE_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 oemHPE_computer_lock=windows
```

```
set /map1/config1 oemHPE_computer_lock=custom,l_gui,l
```

```
set /map1/config1 oemHPE_computer_lock=disabled
```

For a list of all `oemHPE_computer_lock` custom keys, see the iLO User Guide on the Hewlett Packard Enterprise website at **http://www.hpe.com/support/ilo-docs**. Keys with a space must have the space replaced with an underscore.

For example:

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

## AlertMail settings

AlertMail settings commands enable you to view and configure the AlertMail feature. These settings are available at: `/map1/oemHPE_alertmail1`

### Targets

None

### Properties

> **NOTE**
> All command properties are Read/Write access.

| Property | Description |
|---|---|
| `oemHPE_alertmail_enable` | Enables or disables the AlertMail function. Values can be **`yes`** (enabled) or **`no`** (disabled). |
| `oemHPE_alertmail_email` | Sets the AlertMail recipient address. Value must be a valid email address. |
| `oemHPE_alertmail_sender_domain` | Sets the domain for the AlertMail recipient. |
| `oemHPE_alertmail_smtp_server` | Sets the server address for the AlertMail recipient. |
| `oemHPE_alertmail_smtp_port` | Sets the port for AlertMail. Valid port values include port **`25`** (unauthenticated) and **`587`** (authenticated). |
| `oemHPE_alertmail_smtp_secure_enable` | Enables or disables secure AlertMail. Values can be **`yes`** (enabled) or **`no`** (disabled). |
| `oemHPE_alertmail_smtp_auth_enable` | Enables or disables authentication for secure AlertMail. Values can be **`yes`** (enabled) or **`no`** (disabled). |
| `oemHPE_alertmail_smtp_auth_username` | Sets the username for authentication when AlertMail authentication is enabled. |
| `oemHPE_alertmail_smtp_auth_password` | Sets the password for authentication when AlertMail authentication is enabled. |

**Verbs**

- cd
- version
- exit
- show
- set
- oemHPE_sendTestAlertmail

> **NOTE**
>
> HPE suggests sending a test AlertMail to confirm proper setup.

**For example**

The following commands set various AlertMail properties:

- `set /map1/oemHPE_alertmail1 oemHPE_alertmail_enable=yes`
- `set oemHPE_alertmail_email=name@domain.com`
- `set oemHPE_alertmail_sender_domain=domain.com`
- `set oemHPE_alertmail_smtp_server=smtp.domain.com`
- `set oemHPE_alertmail_smtp_port=587`
- `set oemHPE_alertmail_smtp_secure_enable=yes`
- `set oemHPE_alertmail_smtp_auth_enable=yes`
- `set oemHPE_alertmail_smtp_auth_username=`*`username`*
- `set oemHPE_alertmail_smtp_auth_password=`*`password`*

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.

# iLO embedded health settings

iLO embedded health commands enable you to display system-embedded health information for fans, temperature sensors, voltage sensors, and power supplies.

Use the following commands to view the details for the specified target:

- `show /system1/<target>(N)`—Displays detailed information for the specified target instance, where `(N)` is a numeric identifier. Examples include `fan1`, `fan2`, `sensor3`, and similar target instances.
- `show -all /system1/<target>*` or `show -a /system1/<target>*`—Displays detailed information for all the instances of the specified target.

Use `*` character only with `show -all` or `show -a` options to get the detailed information for all the instances of the specified target type.



**NOTE**

Enter a target from the **Supported Targets** list in `<target>`. For targets that support multiple instances, enter the corresponding numeric identifier in `(N)`.

**Supported Targets**

- Fan(N)
- Sensor(N)
- Powersupply(N)
- firmware1
- bootconfig1
- log1
- led1
- network1
- oemHPE_vsp1
- oemHPE_power1
- cpu1
- memory(N)
- slot(N)
- swid(N)

**Table 1. 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 the 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 |
| `oemHPE_CautionValue` | Read | Displays temperature sensor caution value |
| `oemHPE_CriticalValue` | Read | Displays temperature sensor critical value |



**NOTE**

All available embedded health properties from all targets are shown in Table: Embedded Health properties. The actual properties returned depend on the command.

**For example**

The following command displays the system fan1 properties: `show /system1/fan1`.

```
show /system1/fan1
  Targets
  Properties
    DeviceID=Fan 1
    ElementName=System
    OperationalStatus=Not Installed
    VariableSpeed=Yes
    DesiredSpeed=0 percent
    HealthState=Not Installed
```

VRM power supplies are mapped to the sensor targets.

The following command displays the VRM1 properties: `show /system1/sensor15`.

```
show /system1/sensor15
  Targets
  Properties
    DeviceID=15-P/S 1 Inlet
    ElementName=Power Supply
    OperationalStatus=Ok
    RateUnits=Celsius
    CurrentReading=30
    SensorType=Temperature
    HealthState=Ok
    oemHPE_CautionValue=Not Applicable
    oemHPE_CriticalValue=Not Applicable
```

Other sensor targets show system temperatures.

The following command displays one of the temperature zone properties: `show /system1/sensor38`.

```
show /system1/sensor38
  Targets
  Properties
    DeviceID=38-PCI 3 Zone
    ElementName=I/O Board
    OperationalStatus=Ok
    RateUnits=Celsius
    CurrentReading=28
    SensorType=Temperature
    HealthState=Ok
    oemHPE_CautionValue=90
    oemHPE_CriticalValue=95
```

The following command displays all the Powersupply target properties: `show -a /system1/powersupply*`.

```
show -a /system1/powersupply*

/system1/powersupply1
  Targets
  Properties
    ElementName=Power Supply
    OperationalStatus=Ok
    HealthState=Good, In Use
  Verbs
```

```
    cd version exit show

/system1/powersupply2
  Targets
  Properties
    ElementName=Power Supply
    OperationalStatus=Unknown
    HealthState=Unknown
  Verbs
    cd version exit show
```

## SNMP settings

SNMP settings commands enable you to view and modify SNMP settings. SNMP settings are available at: `/map1/snmp1`.

### Targets

None

### Properties



**NOTE**

All SNMP command properties are Read/Write access.

**Table 1. SNMP Command Properties**

| Property | Description |
|---|---|
| `accessinfo<n>` | Sets the SNMP trap destination address, where *<n>* is `1`, `2`, or `3`. |
| `readcom<n>` | Displays or modifies the SNMP read community address when Agentless Management is enabled. The value *<n>* is `1`, `2`, or `3`. |
| `trapcom<n>` | Displays or modifies SNMP trap community address, where *<n>* is `1`, `2`, or `3`. |
| `oemHPE_iloalert` | Enables or disables iLO SNMP alerts. Boolean values accepted. |
| `oemHPE_systemlocation` | Displays or modifies SNMP System Location when Agentless Management is enabled. |

| Property | Description |
| --- | --- |
| `oemHPE_systemcontact` | Displays or modifies SNMP System Contact when Agentless Management is enabled. |
| `oemHPE_systemrole` | Displays or modifies SNMP System Role information when Agentless Management is enabled. |
| `oemHPE_systemroledetail <n>` | Displays or modifies SNMP System Role detail when Agentless Management is enabled, where *<n>* is `1` to `5`. |
| `oemHPE_imdatalevel` | Displays or modifies level of data returned to Insight Manager. Boolean values accepted. |
| `oemHPE_coldstarttrap` | Displays or modifies the SNMP Cold Start Trap Broadcast. Boolean values accepted. |
| `oemHPE_trapsource` | Displays or modifies the SNMP trap source setting. |

**NOTE**

The command properties `oemhp_agentalert`, `oemhp_snmppassthru`, `oemhp_imagenturl` and `oemhp_agentlessenable` properties are deprecated in iLO 5.

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

**For example**

The following commands set various SNMP properties:

- `set /map1/snmp1 accessinfo1=192.168.0.50 oemHPE_imdatalevel=Enabled`
- `set readcom1="public1"`
- `set trapcom1="trapcomm1"`
- `set oemHPE_systemlocation="HPE Data Center, Hockley, TX"`

- `set oemHPE_systemcontact="Mr. System Administrator"`
- `set oemHPE_systemrole="Brief Role Description [60 characters]"`
- `set oemHPE_systemroledetail1="Extended role description [100 characters]"`
- Showing multiple lines for `oemHPE_systemroledetail`:
  - `set oemHPE_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. License commands are available at: `/map1/`.

For more information see the HPE iLO Licensing Guide at: **http://www.hpe.com/support/iLOLicenseGuide-en**.

**Targets**

None

**Commands**

**Table 1. 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. Directory command settings are available at: `/map1/oemHPE_dircfg1`.

### Targets

**Table 1. Directory Command Targets**

| Target | Description |
|---|---|
| `/map1/oemHPE_dircfg1/oemHPE_keytab1` | Contains a load verb used to load the binary keytab file from a given URL. Keytab files up to 1,024 bytes in length are supported. |

### Properties

**Table 2. Directory Command Properties**

| Property | Access | Description |
|---|---|---|
| `oemHPE_dirauth` | Read/Write | Enables or disables directory authentication. Valid settings are as follows:<br>• `extended_schema`—Uses the Hewlett Packard Enterprise extended schema.<br>• `default_schema`—Uses schema-free directories.<br>• `disabled`—Directory-based authentication is disabled. |
| `oemHPE_localacct` | Read/Write | Enables or disables local account authentication. This property can be disabled only if directory authentication is enabled. Boolean values accepted. |
| `oemHPE_dirsrvaddr` | Read/Write | Sets the directory server IP address or DNS name. The schema-free directory configuration requires a DNS name. |
| `oemHPE_dir_generic_ldap_enabled` | Read/Write | Displays or modifies the iLO 5 generic LDAP setting for directory default schema configurations. Valid values are `yes` and `no`. This property can be configured only when directory a |

| Property | Access | Description |
|---|---|---|
| | | uthorization is configured to use the default sc hema. |
| `oemHPE_ldapport` | Read/Writ e | Sets the directory server port. |
| `oemHPE_dirdn` | Read/Writ e | Displays the LOM object distinguished name. This field is ignored when the schema-free dire ctory configuration is used. |
| `oemHPE_usercntxt1, 2 ...` (up to 15) | Read/Writ e | Displays the directory user login search contex t. This field is not necessary when the schema -free directory configuration is used. |
| `oemHPE_group(n)_name`, where `n` = 1..6 | Read/Writ e | Displays security group distinguished name. U sed within the schema-free directory configura tion only. |
| `oemHPE_group(n)_priv`, where `n` = 1..6 | Read/Writ e | The privileges associated with a group. Valid values are:<br>• `login`<br>• `oemHPE_rc`<br>• `oemHPE_power`<br>• `oemHPE_vm`<br>• `config`<br>• `admin` |
| `oemHPE_dir_kerberos_enabled` | Read/Writ e | Enables or disables Kerberos authentication. Boolean values are accepted. |
| `oemHPE_dir_kerberos_kdc_port` | Read/Writ e | Specifies the port number used to connect to the domain controller. The Kerberos port num ber is 88, but the domain controller can be conf igured for a different port number. |
| `oemHPE_dir_kerberos_kdc_addre ss` | Read/Writ e | The location of the domain controller. The dom ain controller location is specified as an IP add ress or DNS name. |
| `oemHPE_dir_kerberos_realm` | Read/Writ e | Specifies the Kerberos realm for which the do main controller is configured. By convention, t he Kerberos realm name for a given domain is the domain name converted to uppercase. |

**For example**

- `set /map1/oemHPE_dircfg1`
- `set /map1/oemHPE_dircfg1 oemHPE_dirauth=default_schema oemHPE_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 feature is supported through the CLP. The virtual media subsystem is available at: `/map1/oemHPE_vm1`.

For more information, see the HPE iLO 5 User Guide on the Hewlett Packard Enterprise website at: **http://www.hpe.com/support/ilo-docs**.

### Targets

**Table 1. Virtual Media Command Targets**

| Target | Description |
|---|---|
| `/map1/oemHPE_vm1/floppydr1` | Virtual floppy or key drive device |
| `/map1/oemHPE_vm1/cddr1` | Virtual CD-ROM device |

**Table 2. Virtual Media Command Properties**

| Property | Access | Description |
|---|---|---|
| `oemHPE_image` | Read/Write | The image path and name for virtual media access. The value is a URL with a maximum length of 80 characters. |
| `oemHPE_connect` | Read | Displays if a virtual media device is already connected through the CLP or scriptable virtual media. |
| `oemHPE_boot` | Read/Write | Sets the boot flag. The valid values are:<br>• `Never`<br>Do not boot from the device. The value appears as `No_Boot`. |

| Property | Access | Description |
|---|---|---|
| | | • `Once`<br>Boot from the device only once. The value appears as `Once`.<br>• `Always`<br>Boot from the device each time the server is rebooted. The value i s displayed as `Always`.<br>• `Connect`<br>Connect the virtual media device. Sets `oemHPE_connect` to `Yes` and `oemHPE_boot` to `Always`.<br>• `Disconnect`<br>Disconnects the virtual media device and sets the `oemHPE_bo ot` to `No_Boot`. |
| `oemHPE_wp` | Read/Write | Enables or disables the write-protect flag. Boolean values accepted. |
| `vm_applet` | Read/Write | Displays whether an iLO virtual media device is connected through a remote console. Requires an iLO license. |

**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. It uses the same format as the scriptable virtual media image location.

URL example:

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

- `protocol` —Mandatory (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 oemHPE_image=http://imgserver.company.com/image/dosboot.bin`

- `set oemHPE_image=http://john:abc123@imgserver.company.com/VMimage/installDisk.iso`

**Tasks**

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

  ```
  cd /map1/oemHPE_vm1/floppydr1
  show
  set oemHPE_image=http://my.imageserver.com/floppyimg.bin
  set oemHPE_boot=connect
  show
  ```

  This example executes the following commands:

  - Changes the current context to the floppy or key drive.
  - Shows the status to verify that the media is not in use.
  - Inserts the specified 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/oemHPE_vm1/floppydr1
  set oemHPE_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 `oemHPE_image`.

- To insert a CD-ROM image into the virtual CD-ROM, enter:

  ```
  cd /map1/oemHPE_vm1/cddr1
  show
  set oemHPE_image=http://my.imageserver.com/ISO/install_disk1.iso
  set oemHPE_boot=connect
  show
  ```

  This example executes the following commands:

  - Changes the current context to the CD-ROM drive.
  - Shows the status to verify that the media is not in use.
  - Inserts the specified 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/oemHPE_vm1/cddr1
set oemHPE_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 `oemHPE_image`.

- To insert a CD-ROM image and set for single boot, enter:

```
cd /map1/oemHPE_vm1/cddr1
set oemHPE_image=http://my.imageserver.com/ISO/install_disk1.iso
set oemHPE_boot=connect
set oemHPE_boot=once
show
```

This example executes the following commands:

- Changes the current context to the CD-ROM drive.
- Shows the status to verify that the media is not in use.
- Inserts the specified 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/oemHPE_vm1/cddr1 oemHPE_boot=disconnect`. If you attempt to disconnect when the drive is not connected, you receive an error.

## Start and Reset commands

This module describes start and reset commands.

Start and reset commands enable you to power on and reboot the server containing iLO or reboot just iLO itself. Start and Reset Commands shows the Start and Reset command properties.

**Table 1. Start and Reset Commands**

| Command | Description |
|---|---|
| `start` | Turns on server power |
| `stop` | Turns off server power |

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

**Table 2. Manual Reset Command**

| Property | Access | Description |
|---|---|---|
| manual_iLO_reset | Read/Write | Allows a delay to iLO resets, which is useful when changin g multiple properties. Valid values are **`yes`** (enabled) or **`no`** (disabled). When enabled, the iLO will reset only wh en a user logs out, is disconnected from iLO, or issues a 'res et/map1' command. |

**For example**

The following commands are supported if the current target is:

`/system1`

- `start`
- `stop`
- `reset hard`

The following commands are supported if the current target is:

`/map1`

- `reset`
- `reset soft`

Set the status of the manual_iLO_reset property using the following commands in /map1:

- set /map1/ manual_ilo_reset=yes
- set /map1/ manual_ilo_reset=no

# Firmware commands

Firmware commands enable you to display and modify the iLO firmware version. Firmware settings are available at: `/map1/firmware1`.

### Targets

No targets

**Table 1. Firmware Update Properties**

| Property | Access | Description |
|---|---|---|
| `version` | read | Displays the current firmware version. |
| `date` | read | Displays the release date of the current firmware version. |
| `name` | read | Displays the iLO firmware name. |

### Command format - source

`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, 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. Confirm visually that the URL is valid. For example:

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

**WARNING**

If a Hewlett Packard Enterprise 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.

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

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` is displayed. If iLO firmware is flashed, then an iLO reset occurs.

**Command format - Target**

The [`target`] value is: `/map1/firmware1` —This field is optional if it is already the current target.

**Subtopics**

**Non-iLO firmware commands**

## Non-iLO firmware commands

Non-iLO firmware commands support system firmware updates, available at: `/system1/swid<N>`, where `<N>` is a number or a wildcard (*). Use a wildcard to show every firmware version installed on the system (including iLO). The list helps to identify the software ID number of the firmware you want to load.

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

```
</system1>hpiLO-> show swid*
status=0
status_tag=COMMAND COMPLETED
Thu May 25 09:28:25 2017

/system1/swid1
  Targets
  Properties
    name=iLO 5
    VersionString=1.20 Jan 09 2018
    oemHPE_VersionStrings=1.20 Jan 09 2018
  Verbs
    cd version exit show load
```

```
/system1/swid2
  Targets
  Properties
    name=System ROM
    VersionString=U33 v1.20 (07/01/2017)
    oemHPE_VersionStrings=U33 v1.20 (07/01/2017)
  Verbs
    cd version exit show load

.
.
.
```

When loading non-iLO firmware, a manual system reset might be required for the changes to be applied.

Follow the command format described in Firmware commands. For example:

```
load -source http://192.168.1.1/images/fw/<firmware_filename>
```

The following firmware types are supported:

- ProLiant System ROM
- System Programmable Logic Device
- SL Chassis Firmware
- Power Management Controller Firmware and FW Bootloader
- Innovation Engine (IE) Firmware
- Ethernet Adapter

Download the server firmware files at: **https://www.hpe.com/support/hpesc**.

## Eventlog commands

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

Eventlog settings are available at:

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

**Targets**

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

**Table 1. 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/record`*n* —Displays record *n* from the Integrated Management log.
- `show /map1/log1/record`*n* —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. These values are available at: `/system1/map1/blade1`.

**Table 1. Blade Command Targets**

| Target | Description |
|---|---|
| `/map1/blade1/rack` | Displays and modifies the blade rack settings. |
| `/map1/blade1/rack/enclosure` | Displays and modifies the blade enclosure settings. |

**Table 2. 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. |
| `ip_address` | Read | Displays the IP address |
| `mac_address` | Read | Displays the MAC address |
| `sys_health` | Read | Displays the system health status |

## Boot commands

Boot commands enable you to modify the boot order of the system. 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.

For systems with UEFI BIOS, the values for `bootsource` are:

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

For systems with legacy BIOS, the values for `bootsource` are:

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

- `bootsource5: BootFmNetwork`

> **NOTE**
>
> If no bootable network device is enabled on the system, the `BootFmNetwork` boot source might not show up in the list of targets.

**Table 1. 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 following example output shows `bootsource3` (`BootfmDrive`) is 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
    bootdevice=BootFmCd
  Verbs
    cd version exit show set

/system1/bootconfig1/bootsource2
  Targets
  Properties
    bootorder=3
    bootdevice=BootFmFloppy
```

```
  Verbs
    cd version exit show set

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

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

/system1/bootconfig1/bootsource5
  Targets
  Properties
    bootorder=5
    bootdevice=BootFmNetwork
  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/oemHPE_bootmode
```

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

```
show /system1/bootconfig1/oemHPE_pendingbootmode
```

**UEFI enabled systems**

When configuring the UEFI `bootorder`, 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 following example output shows `oemHPE_uefibootsource1` is configured as the primary boot device, because it has a `bootorder=1`

```
/system1/bootconfig1
  Targets
    oemHPE_uefibootsource1
    oemHPE_uefibootsource2
  Properties
    oemHPE_bootmode=UEFI
    oemHPE_secureboot=no
    oemHPE_pendingbootmode=UEFI
  Verbs
    cd version exit show set

/system1/bootconfig1/oemHPE_uefibootsource1
  Targets
  Properties
    bootorder=1
    oemHPE_description=Windows Boot Manager
  Verbs
    cd version exit show set

/system1/bootconfig1/oemHPE_uefibootsource2
  Targets
  Properties
    bootorder=2
    oemHPE_description=Embedded SATA Port 3 HDD : GB0160CAABV
```

```
  Verbs
    cd version exit show set
```

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

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

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

```
set /system1/bootconfig1/oemHPE_uefibootsource2 bootorder=1
```

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

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

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

```
show /system1/bootconfig1/oemHPE_secureboot
```

## LED commands

LED commands are used to change the state of the UID light on the server. LED settings are available at: `/system1/led1` .

**Table 1. LED Command Properties**

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

**For example**

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

**iLO CLI support**

Simple UID CLI commands are supported:

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

- `uid off` —Turns off the UID.

The CLP format is supported as well:

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

## System properties and targets

The properties and targets described in this section provide information about the server. System properties settings are available at: `/system1`.

**Table 1. System Properties**

| Property | Access | Description |
|---|---|---|
| `name` | Read | Displays the system name. |
| `number` | Read | Displays the system serial number. |
| `oemHPE_server_name` | 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. |
| `oemHPE_server_fqdn` | Read | Displays the host server fully qualified domain name. |
| `enabledstate` | Read | Appears if the server is powered up. |
| `processor_number` | Read | Displays the number of logical processors in the system. |

**For example**

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

**CPU properties**

The CPU property is a target of `/system1` and displays information about the system processor. The properties are available at: `/system1/cpun`, where `n` is the processor number.

**Table 2. System CPU Properties**

| Property | Access | Description |
|---|---|---|
| `name` | Read | Displays manufacturer information about the processor. |
| `status` | Read | Displays status information. |
| `number_cores` | Read | Displays the number of processor cores. |
| `active_cores` | Read | Displays the number of active logi cal processors within a CPU. |
| `threads` | Read | Displays the number of logical th reads within a CPU. |
| `speed` | Read | Displays the processor speed. |
| `memory_technology` | Read | Displays the bit level technology o f the memory. |
| `cachememory1` | Read | Displays the size of the processor l evel-1 cache. |
| `cachememory2` | Read | Displays the size of the processor l evel-2 cache. |
| `cachememory3` | Read | Displays the size of the processor l evel-3 cache. |

`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
```

### System memory properties

The `memory` property displays information about the system memory.

The properties are available at: `/system1/memoryn`, where `n` is the memory DIMM number.

**Table 3. System Memory Properties**

| Property | Access | Description |
|---|---|---|
| `size` | Read | Displays the memory size. |
| `frequency` | Read | Displays the memory speed. |
| `location` | Read | Displays the location of the memory. |
| `technology` | Read | Displays information about the system memory technology type. |

### System slot properties

The `Slot` property displays information about the system slots.

The properties are available at: `/system1/slotn`, where *n* is the slot number.

**Table 4. System Slot Properties**

| Property | Access | Description |
|---|---|---|
| `type` | Read | Displays the slot type. |
| `width` | Read | Displays the slot width. |
| `name` | Read | Display the slot name. |

### System firmware properties

The `Firmware` property displays information about the system ROM.

The properties are available at:

`/system1/firmware1`

**Table 5. 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=U33
    date=12/04/2016
  Verbs
    cd version exit show load
```

### System power properties

The `oemHPE_power1` property displays information about the system power.

The properties are available at: `/system1/oemHPE_power1`

**Table 6. oemHPE_power1 properties**

| Target | Description |
|---|---|
| `oemHPE_powerreg` | Displays and modifies the Power Regulator for ProLiant state. Valid values a re **dynamic**, **max**, **min**, or **os**. |
| `oemHPE_pwrcap` | Displays and modifies the server power cap setting (watts). A value of zero indicates that power capping is disabled. The value must be an integer cap value that is greater than or equal to `oemHPE_serverminpower`. It m ust be less than or equal to `oemHPE_powersupplycapacity`. |
| `oemHPE_PresentPowe r` | Displays the average power reading from the last sample. |
| `oemHPE_AvgPower` | Displays the average power reading from the past 24 hours. |
| `oemHPE_MaxPower` | Displays the greatest peak power reading from the past 24 hours. |
| `oemHPE_MinPower` | Displays the minimum average power reading from the past 24 hours. |
| `oemHPE_powersupply capacity` | Displays the total power supply capacity in Watts. |
| `oemHPE_servermaxpo wer` | Displays the maximum server power capacity in Watts. |

| Target | Description |
| --- | --- |
| `oemHPE_serverminpower` | Displays the minimum server power capacity in Watts. |
| `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. |
| `oemHPE_power_micro_ver` | Displays the firmware version number for the Power Micro Controller. |
| `oemHPE_auto_pwr` | Displays and modifies the Server Automatic Power On setting. Valid values are on, 15, 30, 45, 60, random, restore, and off. **On** turns on automatic power on with minimum delay. Time-delayed automatic power on settings or a **random** time delay can be enabled (time starts after iLO boots). **Restore** restores the last power state. **Off** turns off automatic power on.<br><br>The Restore option is supported on nonblade servers only.<br><br>The 15, 30, 45, and 60 second delay values are not supported on c-Class blade servers or Synergy compute modules. These server types are managed by external products such as OA, HPE OneView, or the Frame Link Module. iLO will try to power on the servers based on the configured power-on delay setting, but external factors might affect the actual startup time. |

**Verbs**

- cd
- version
- exit
- show
- set

For example:

- `show /system1/oemHPE_power1 oemHPE_powerreg`
- `set /system1/oemHPE_power1 oemHPE_powerreg=<dynamic|max|min|os>`
- `show /system1/oemHPE_power1 oemHPE_pwrcap`
- `set /system1/oemHPE_power1 oemHPE_pwrcap=0`
- `show /system1/oemHPE_power1 oemHPE_power_micro_ver`

## Other commands

Other commands include the following:

**`start /system1/oemHPE_vsp1`**

Starts a virtual serial port session. Press **Esc (** to return to the CLI session. This command includes a single property, `enabled_state`, which must be set to `enabled` or `disabled`.

**`show /system1/oemHPE_vsp1`**

Displays the status of a virtual serial port session. If VSP is currently running, then `enabled_state` property will be set to `enabled`. If VSP is currently not running, then `enabled_state` property will be set to `disabled`.

**`power`**

This command is used to change the server power state. The Virtual Power and Reset privilege is required to use this command.

**`onetimeboot`**

This command is used to access the one-time boot settings on the server.

**`nmi server`**

Generates and sends an NMI to the server. The Virtual Power and Reset privilege is required to use this command.

**`language`**

This command sets and gets the default language.

**`textcons`**

This command initiates a text console session.

**`testtrap`**

Send a test SNMP trap to the configured alert destinations.

#### Online help

For information about how to use these commands, enter **`help`** ***`command name`***.

For example:

```
</>hpiLO-> help onetimeboot

status=0
status_tag=COMMAND COMPLETED
Wed Aug 12 16:15:53 2020
```

```
ONETIMEBOOT: The ONETIMEBOOT command is used to access the One-Time Boot
settings on the server.  The supported settings are a subset of
settings found in other interfaces.
Usage:
  onetimeboot               -- Displays the current state on the server.
  onetimeboot usb           -- Set to USB.
  onetimeboot ip            -- Set to Intelligent Provisioning.
  onetimeboot smartstartLX  -- Set to IP Smart Start Linux PE.
  onetimeboot netdev1       -- Set to Network Device 1.
  onetimeboot none          -- Disable One-Time Boot.
```

# RIBCL XML Scripting Language

**Subtopics**

**Remote Insight Board Command Language**
**RIBCL**
This module describes the RIBCL command.
**LOGIN**
This module describes the LOGIN command.
**USER_INFO**
This module describes the USER_INFO command.
**RIB_INFO**
This module describes the RIB_INFO command.
**DIR_INFO**
This module describes the DIR_INFO command.
**RACK_INFO**
**BLADESYSTEM_INFO**
**SERVER_INFO**
This module describes the SERVER_INFO command.
**SSO_INFO**

# Remote Insight Board Command Language

The Remote Insight Board Command Language (RIBCL) enables you to write XML scripts to configure and manage:

- iLO configuration settings
- User accounts
- Directory settings
- Server settings
- SSO settings

Download the sample scripts from the Hewlett Packard Enterprise **website**.

Before using the XML sample scripts, read the firmware support information in each sample script. The information helps you tailor the script for the intended firmware and version.

When writing 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 for iLO 5 firmware version 1.20 and later.

**Subtopics**

**XML headers**
**Data types**
This module describes the xml header used with HPQLOCFG.exe.
**Response definitions**
This module describes iLO command response conventions.

# XML headers

The following XML header must be present in every script, which ensures an XML connection and not an HTTP connection:

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

Two other headers can be added in RIBCL scripts:

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

  Added to a RIBCL script or in a response, this header takes the following entities in a quoted string and changes them to symbol equivalents:

**Table 1. Accepted script entities**

| Entity | Symbol |
|---|---|
| < | < |
| > | > |

| Entity | Symbol |
|---|---|
| & | & |
| ' | ' |
| " | " |

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

This header will accept entities (see Table: Accepted script entities) along with changing output to minimal response.

**Table 2. XMLILO output (GET_FW_VERSION)**

**Output with header**

```
#> perl locfg.pl -s <ilo ip> -f get_fw_version.xml -u admin -p admin123
```

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">

<GET_FW_VERSION
   FIRMWARE_VERSION = "1.20"
   FIRMWARE_DATE = "Feb 5 2018"
   MANAGEMENT_PROCESSOR = "iLO5"
   LICENSE_TYPE = "iLO Advanced"
    />
</RIBCL>
```

**Output without header**

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

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

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

<?xml version="1.0"?>
<RIBCL VERSION="2.23">
```

| Output with header | Output without header |
| --- | --- |
| | <RESPONSE<br>STATUS="0x0000"<br>MESSAGE='No error'<br>/><br><GET_FW_VERSION<br>FIRMWARE_VERSION = "1.20"<br>FIRMWARE_DATE = "Feb 5 2018"<br>MANAGEMENT_PROCESSOR = "iLO5"<br>LICENSE_TYPE = "iLO Advanced"<br>/><br></RIBCL><br><br><?xml version="1.0"?><br><RIBCL VERSION="2.23"><br><RESPONSE<br>STATUS="0x0000"<br>MESSAGE='No error'<br>/><br></RIBCL><br><br><?xml version="1.0"?><br><RIBCL VERSION="2.23"><br><RESPONSE<br>STATUS="0x0000"<br>MESSAGE='No error'<br>/><br></RIBCL> |

## Data types

This module describes the xml header used with HPQLOCFG.exe.

The three data types allowed in the parameter are:

- String
- Specific string
- Boolean string

**Subtopics**

**String**
This module describes the text strings in the context of RIBCL.
**Specific string**
This module describes specific strings in the context of RIBCL.
**Boolean string**
This module describes Boolean strings in the context of RIBCL.

# String

This module describes the text strings in the context of RIBCL.

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.



**NOTE**

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

This module describes specific strings in the context of RIBCL.

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

This module describes Boolean strings in the context of RIBCL.

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

This module describes iLO command response conventions.

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 module describes the RIBCL command.

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>
```

**Subtopics**

**RIBCL parameters**
This module describes the RIBCL VERSION string.
**RIBCL runtime errors**
**Combining multiple commands in one RIBCL script**

## RIBCL parameters

This module describes the RIBCL VERSION string.

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 errors 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.

**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>
```

**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

This module describes the LOGIN command.

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`

### Subtopics

**LOGIN parameters**
This module describes the LOGIN command.

**LOGIN runtime errors**
This module describes the LOGIN command.

## LOGIN parameters

This module describes the LOGIN command.

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must not be blank. The maximum length of the login name is 39 characters.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The maximum length of the password is 39 characters.

## LOGIN runtime errors

This module describes the LOGIN command.

Possible runtime error messages include:

- `User login name was not found.`
- `Logged-in user does not have required privilege for this command.`

## USER_INFO

This module describes the USER_INFO command.

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>
```

**Subtopics**

**ADD_USER**
This module describes the ADD_USER command.
**DELETE_USER**
This module describes the DELETE_USER command.
**DEL_USERS_SSH_KEY**
**GET_USER**
This module describes the GET_USER command.
**MOD_USER**
This module describes the MOD_USER command.
**GET_ALL_USERS**
This module describes the GET_ALL_USERS command.
**GET_ALL_USER_INFO**
This module describes the GET_ALL_USER_INFO command.

# ADD_USER

This module describes the ADD_USER command.

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>
```



**NOTE**

ADD_USER has not been enhanced to support the extended user privileges available from the iLO 5 web interface. For more information about setting user privileges in iLO 6, see the HPE iLO 6 User Guide.

**Subtopics**

**ADD_USER parameters**
**ADD_USER runtime errors**
This module describes the ADD_USER command runtime errors.
**Password guidelines**

## 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 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

This module describes the ADD_USER command 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.`

# Password guidelines

Hewlett Packard Enterprise recommends that you follow these password guidelines when you create and update user accounts.

- When working with passwords:
  - Do not write down or record passwords.
  - Do not share passwords with others.
  - Do not use passwords that are made up of words found in a dictionary.
  - Do not use passwords that contain obvious words. Examples include the company name, product name, user name, or login name.
  - Change passwords regularly.
  - Keep the iLO default credentials in a safe place.
- Use strong passwords with at least three of the following characteristics:
  - At least one uppercase ASCII character
  - At least one lowercase ASCII character
  - At least one ASCII digit
  - At least one other type of character (for example, a symbol, special character, or punctuation).

  If you enable the **Password complexity** setting on the **Access Settings** page, iLO enforces these password characteristics when you create or edit a user account.
- The minimum length for a user account password is set on the **Access Settings** page. Depending on the configured **Minimum Password Length** value, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. Hewlett Packard Enterprise recommends using a **Minimum Password Length** of eight or more characters. The default value is eight characters.

  **IMPORTANT**

  Do not set the **Minimum Password Length** to fewer than eight characters unless you have a physically secure management network that does not extend outside the secure data center.

# DELETE_USER

This module describes the DELETE_USER command.

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>
```

**Subtopics**

**DELETE_USER parameter**

**DELETE_USER runtime errors**

This module describes the DELETE_USER command runtime errors.

# DELETE_USER parameter

USER_LOGIN is the login name of the user account. This parameter is not case-sensitive, and must not be blank.

# DELETE_USER runtime errors

This module describes the DELETE_USER command 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 left 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 5.00 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>
```

### Subtopics

**DEL_SSH_KEY parameters**
**DEL_SSH_KEY runtime errors**

## 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

This module describes the GET_USER command.

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 read or write.

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>
```

### Subtopics

**GET_USER parameter**
This module describes the GET_USER parameters.
**GET_USER runtime errors**
This module describes the GET_USER runtime errors.
**GET_USER return messages**
This module describes the GET_USER return messages

## GET_USER parameter

This module describes the GET_USER parameters.

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

## GET_USER runtime errors

This module describes the GET_USER runtime errors.

Possible GET_USER error messages include:

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

## GET_USER return messages

This module describes the 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

This module describes the MOD_USER command.

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.

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>
```

**NOTE**

MOD_USER has not been enhanced to support the extended user privileges available from the iLO 5 web interface. For more information about setting user privileges in iLO 5, see the HPE iLO 5 User Guide in the HPE Information LIbrary at **http://www.hpe.com/support/ilo-docs**.

**Subtopics**

**MOD_USER parameters**
This module describes the MOD_USER command parameters.
**MOD_USER runtime errors**
This module describes the MOD_USER runtime errors.

# MOD_USER parameters

This module describes the MOD_USER command 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

This module describes the 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

This module describes the GET_ALL_USERS command.

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>
```

**Subtopics**

**GET_ALL_USERS parameters**
This module describes the GET_ALL_USERS command parameters.
**GET_ALL_USERS return messages**
This module describes the GET_ALL_USERS command return messages.

## GET_ALL_USERS parameters

This module describes the GET_ALL_USERS command parameters.

None

## GET_ALL_USERS return messages

This module describes the GET_ALL_USERS command 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

This module describes the GET_ALL_USER_INFO command.

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>
```

**NOTE**

GET_ALL_USER_INFO has not been enhanced to support the extended user privileges available from the iLO 5 web interface. For more information about setting user privileges in iLO 5, see the HPE iLO 5 User Guide in the HPE Information LIbrary at **http://www.hpe.com/support/ilo-docs**.

**Subtopics**

**GET_ALL_USER_INFO parameters**
This module describes the GET_ALL_USER_INFO command parameters.
**GET_ALL_USER_INFO return messages**

# GET_ALL_USER_INFO parameters

This module describes the GET_ALL_USER_INFO command parameters.

None

# 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

This module describes the RIB_INFO command.

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>
```

### Subtopics

**RESET_RIB**

This module describes the RESET_RIB command.

**GET_EVENT_LOG**

This module describes the GET_EVENT_LOG command.

**CLEAR_EVENTLOG**

This module describes the CLEAR_EVENT_LOG command.

**GET_FEDERATION_MULTICAST**

This module describes the GET_FEDERATION_MULTICAST command

**SET_FEDERATION_MULTICAST**

This module describes the SET_FEDERATION_MULTICAST command

**GET_FEDERATION_ALL_GROUPS**

This module describes the GET_FEDERATION_ALL_GROUPS command

**GET_FEDERATION_ALL_GROUPS_INFO**

**ADD_FEDERATION_GROUP**

**DELETE_FEDERATION_GROUP**

This module describes the DELETE_FEDERATION_GROUP command

**GET_FEDERATION_GROUP**

**MOD_FEDERATION_GROUP**

**COMPUTER_LOCK_CONFIG**

This module describes the COMPUTER_LOCK_CONFIG command.

**GET_NETWORK_SETTINGS**

This module describes the GET_NETWORK_SETTINGS command.

**MOD_NETWORK_SETTINGS**

This module describes the MOD_NETWORK_SETTINGS command.

**GET_GLOBAL_SETTINGS**

This module describes the GET_GLOBAL_SETTINGS command.

**MOD_GLOBAL_SETTINGS**

This module describes the MOD_GLOBAL_SETTINGS command.

**BROWNOUT_RECOVERY**

This module describes the BROWNOUT_RECOVERY command.

**GET_SNMP_IM_SETTINGS**

This module describes the GET_SNMP_IM_SETTINGS command.

**MOD_SNMP_IM_SETTINGS**

This module describes the MOD_SNMP_IM_SETTINGS command.

**SEND_SNMP_TEST_TRAP**

**MOD_ENCRYPT_SETTINGS**

**GET_ENCRYPT_SETTINGS**

**UPDATE_RIB_FIRMWARE and UPDATE_FIRMWARE**

This module describes the UPDATE_FIRMWARE command.

**UPDATE_LANG_PACK**

**GET_FW_VERSION**

This module describes the GET_FW_VERSION command.

**LICENSE**

This module describes the LICENSE command.

**INSERT_VIRTUAL_MEDIA**
This module describes the INSERT_VIRTUAL_MEDIA command.
**EJECT_VIRTUAL_MEDIA**
**GET_VM_STATUS**
This module describes the GET_VM_STATUS command.
**SET_VM_STATUS**
**CERTIFICATE_SIGNING_REQUEST**
This module describes the CERTIFICATE_SIGNING_REQUEST command.
**IMPORT_CERTIFICATE**
This module describes the IMPORT_CERTIFICATE command.
**AHS_CLEAR_DATA**
**GET_AHS_STATUS**
**SET_AHS_STATUS**
This module describes the SET_AHS_STATUS command.
**TRIGGER_BB_DATA**
**DISABLE_ERS**
**GET_ERS_SETTINGS**
**SET_ERS_IRS_CONNECT**
**TRIGGER_L2_COLLECTION**
This module describes the TRIGGER_L2_COLLECTION command.
**TRIGGER_TEST_EVENT**
This module describes the TRIGGER_TEST_EVENT command.
**SET_LANGUAGE**
**GET_LANGUAGE**
This module describes the GET_LANGUAGE command.
**GET_ALL_LANGUAGES**
This module describes the GET_ALL_LANGUAGES command.
**GET_ASSET_TAG**
This module describes the GET_ASSET_TAG command.
**SET_ASSET_TAG**
This module describes the SET_ASSET_TAG command.
**GET_SECURITY_MSG**
**SET_SECURITY_MSG**
**HOTKEY_CONFIG**
**GET_HOTKEY_CONFIG**
**PROFILE_APPLY**
**PROFILE_APPLY_GET_RESULTS**
**PROFILE_DELETE**
**PROFILE_LIST**
**PROFILE_DESC_DOWNLOAD**
**FIPS_ENABLE**
**GET_FIPS_STATUS**
**GET_ALL_LICENSES**
**FACTORY_DEFAULTS**
**IMPORT_SSH_KEY**

**LOCK_CONFIGURATION**

# RESET_RIB

This module describes the RESET_RIB command.

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>
```

**Subtopics**

**RESET_RIB parameters**
This module describes the RESET_RIB command parameters.
**RESET_RIB runtime errors**
This module describes the RESET_RIB command runtime errors.

# RESET_RIB parameters

This module describes the RESET_RIB command parameters.

None

# RESET_RIB runtime errors

This module describes the RESET_RIB command runtime errors.

The possible RESET_RIB error message include:

```
User does not have correct privilege for action. CONFIG_ILO_PRIV req
uired.
```

# GET_EVENT_LOG

This module describes the GET_EVENT_LOG command.

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>
```

### Subtopics

**GET_EVENT_LOG parameters**
This module describes the GET_EVENT_LOG command parameters.
**GET_EVENT_LOG runtime errors**
This module describes the GET_EVENT_LOG command runtime errors.

**GET_EVENT_LOG return messages**
This module describes the GET_EVENT_LOG command return messages.

## GET_EVENT_LOG parameters

This module describes the GET_EVENT_LOG command parameters.

None

## GET_EVENT_LOG runtime errors

This module describes the GET_EVENT_LOG command 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

This module describes the GET_EVENT_LOG command 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.
- EVENT_CODE is a unique identifier for an event within a given event class displayed in hexadecimal format.

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

```
<EVENT_LOG DESCRIPTION="iLO 5 Event Log">
 <EVENT
  SEVERITY="Informational"
  CLASS="iLO 5"
  LAST_UPDATE="01/20/2017 07:33:00"
  INITIAL_UPDATE="01/20/2017 07:33:00"
  COUNT="1"
  DESCRIPTION="Event log cleared by: admin."
  EVENT_CODE="0x0087"
 />
</EVENT_LOG>
```

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

```
<EVENT_LOG DESCRIPTION="Integrated Management Log">
 <EVENT
  SEVERITY="Informational"
  CLASS="Maintenance"
  LAST_UPDATE="11/14/2016 20:18:28"
  INITIAL_UPDATE="11/14/2016 20:18:28"
  COUNT="1"
  DESCRIPTION="IML Cleared (iLO 5 user: Administrator)"
  EVENT_CLASS="0x0021"
  EVENT_CODE="0x0001"
```

```
 />
</EVENT_LOG>
```

# CLEAR_EVENTLOG

This module describes the CLEAR_EVENT_LOG command.

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>
```

**Subtopics**

**CLEAR_EVENTLOG parameters**
This module describes the CLEAR_EVENT_LOG command parameters.
**CLEAR_EVENTLOG runtime errors**
This module describes the CLEAR_EVENT_LOG command runtime errors.

# CLEAR_EVENTLOG parameters

This module describes the CLEAR_EVENT_LOG command parameters.

None

# CLEAR_EVENTLOG runtime errors

This module describes the CLEAR_EVENT_LOG command runtime errors.

The possible CLEAR_EVENTLOG error messages are:

- `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_FEDERATION_MULTICAST

This module describes the GET_FEDERATION_MULTICAST command

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>
```

### Subtopics

**GET_FEDERATION_MULTICAST parameters**
This module describes the GET_FEDERATION_MULTICAST command parameters
**GET_FEDERATION_MULTICAST runtime errors**
This module describes the GET_FEDERATION_MULTICAST command runtime errors
**GET_FEDERATION_MULTICAST return messages**
This module describes the GET_FEDERATION_MULTICAST command return messages

## GET_FEDERATION_MULTICAST parameters

This module describes the GET_FEDERATION_MULTICAST command parameters

None

## GET_FEDERATION_MULTICAST runtime errors

This module describes the GET_FEDERATION_MULTICAST command runtime errors

None

## GET_FEDERATION_MULTICAST return messages

This module describes the GET_FEDERATION_MULTICAST command 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'
     />
    <MULTICAST_FEDERATION_ENABLED VALUE="Yes"/>
    <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

This module describes the SET_FEDERATION_MULTICAST command

Use SET_FEDERATION_MULTICAST to enable or disable iLO Federation, and to set the iLO Federation multicast options, including Multicast Discovery, Multicast Announcement Interval, IPv6 Multicast Scope, and Multicast TTL.

For example:

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

**NOTE**

Disabling multicast discovery or announcements disables the iLO Federation features.

All devices in an iLO Federation group must have the same scope and TTL to properly enable peer discovery.

**Subtopics**

**SET_FEDERATION_MULTICAST parameters**
This module describes the SET_FEDERATION_MULTICAST command parameters
**SET_FEDERATION_MULTICAST runtime errors**
This module describes the SET_FEDERATION_MULTICAST command runtime errors

# SET_FEDERATION_MULTICAST parameters

This module describes the SET_FEDERATION_MULTICAST command parameters

MULTICAST_FEDERATION_ENABLED enables or disables iLO Federation. The value must be either `Yes` (enabled) or `No` (disabled). When disabled, iLO federation management features are unavailable.

MULTICAST_DISCOVERY_ENABLED enables or disables multicast discovery. The value must be either `Yes` (enabled) or `No` (disabled). When enabled, this parameter makes the iLO discoverable as federated on the network. When disabled, iLO Federation 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 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 an iLO Federation 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. Valid values are between **`1`** and **`255`**. All devices in a federated group must have the same TTL to properly enable peer discovery.

## SET_FEDERATION_MULTICAST runtime errors

This module describes the SET_FEDERATION_MULTICAST command runtime errors

Some possible SET_FEDERATION_MULTICAST error messages include the following:

- `The MULTICAST_ANNOUNCEMENT_INTERVAL VALUE is invalid. The valid values are "Disabled", "30", "60", "120", "300", "600", "900", and "1800".`
- `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

This module describes the GET_FEDERATION_ALL_GROUPS command

Use the GET_FEDERATION_ALL_GROUPS command to retrieve a list of all iLO 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>
```

**Subtopics**

**GET_FEDERATION_ALL_GROUPS parameters**
This module describes the GET_FEDERATION_ALL_GROUPS command parameters
**GET_FEDERATION_ALL_GROUPS runtime errors**
This module describes the GET_FEDERATION_ALL_GROUPS command runtime errors
**GET_FEDERATION_ALL_GROUPS return messages**
This module describes the GET_FEDERATION_ALL_GROUPS command return messages

# GET_FEDERATION_ALL_GROUPS parameters

This module describes the GET_FEDERATION_ALL_GROUPS command parameters

None

# GET_FEDERATION_ALL_GROUPS runtime errors

This module describes the GET_FEDERATION_ALL_GROUPS command runtime errors

None

# GET_FEDERATION_ALL_GROUPS return messages

This module describes the GET_FEDERATION_ALL_GROUPS command 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 iLO Federation group names and the associated privileges for each group. To retrieve the privileges of a specific group, use GET_FEDERATION_GROUP. In addition to the group name, the returned group privileges include:

- User Account Administration (ADMIN_PRIV)
- Remote Console Access (REMOTE_CONS_PRIV)
- Virtual Power and Reset (RESET_SERVER_PRIV)
- Virtual Media (VIRTUAL_MEDIA_PRIV)
- iLO Setting Configuration (CONFIG_ILO_PRIV)
- Login Privilege (LOGIN_PRIV)



**NOTE**

GET_FEDERATION_ALL_GROUPS_INFO has not been enhanced to support the extended group privileges available from the iLO 5 web interface. For more information about setting group privileges in iLO 5, see the HPE iLO 5 User Guide.

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>
```

**Subtopics**

**GET_FEDERATION_ALL_GROUPS_INFO parameters**
This module describes the GET_FEDERATION_ALL_GROUPS_INFO command parameters
**GET_FEDERATION_ALL_GROUPS_INFO runtime errors**
This module describes the GET_FEDERATION_ALL_GROUPS_INFO command runtime errors
**GET_FEDERATION_ALL_GROUPS_INFO return messages**
This module describes the GET_FEDERATION_ALL_GROUPS_INFO command returns messages

# GET_FEDERATION_ALL_GROUPS_INFO parameters

This module describes the GET_FEDERATION_ALL_GROUPS_INFO command parameters

None.

# GET_FEDERATION_ALL_GROUPS_INFO runtime errors

This module describes the GET_FEDERATION_ALL_GROUPS_INFO command runtime errors

None

# GET_FEDERATION_ALL_GROUPS_INFO return messages

This module describes the GET_FEDERATION_ALL_GROUPS_INFO command returns 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>
```

## ADD_FEDERATION_GROUP

Use ADD_FEDERATION_GROUP to create a new iLO Federation group, or to include an iLO in an existing group membership while setting the privileges of that group on the iLO. The command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to `write`.



**NOTE**

ADD_FEDERATION_GROUP has not been enhanced to support the extended group privileges available from the iLO 5 web interface. For more information about setting group privileges in iLO 5, see the HPE iLO 5 User Guide.

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**

A single iLO can belong to up to a maximum of 10 iLO Federation groups. To remove an iLO system from an iLO Federation group, use DELETE_FEDERATION_GROUP.

**Subtopics**


**ADD_FEDERATION_GROUP parameters**
This module describes the ADD_FEDERATION_GROUP command parameters
**ADD_FEDERATION_GROUP runtime errors**
This module describes the ADD_FEDERATION_GROUP command runtime errors


# ADD_FEDERATION_GROUP parameters

This module describes the ADD_FEDERATION_GROUP command 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 for the group to be added. The password can be from the configured minimum password length to 31 characters long. If **Password Complexity** is enabled on the iLO system, the group key must meet the password complexity requirements.

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

This module describes the ADD_FEDERATION_GROUP command runtime errors

Some possible ADD_FEDERATION_GROUP error messages include the following:

- `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.`
- `The GROUP_KEY is too short. Use a longer key.`
- `Group membership already exists.`
- `Cannot add group membership. Maximum number of memberships reached : 10.`

# DELETE_FEDERATION_GROUP

This module describes the DELETE_FEDERATION_GROUP command

Use DELETE_FEDERATION_GROUP to remove the iLO from an iLO 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>
```

### Subtopics

**DELETE_FEDERATION_GROUP parameters**
This module describes the DELETE_FEDERATION_GROUP command parameters
**DELETE_FEDERATION_GROUP runtime errors**
This module describes the DELETE_FEDERATION_GROUP command errors

## DELETE_FEDERATION_GROUP parameters

This module describes the DELETE_FEDERATION_GROUP command parameters

GROUP_NAME—The name of the iLO 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

This module describes the DELETE_FEDERATION_GROUP command errors

Some possible runtime errors returned by DELETE_FEDERATION_GROUP include the following:

- 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.`

## 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. In addition to the group name, the return includes the following group privileges:

- User Account Administration (ADMIN_PRIV)
- Remote Console Access (REMOTE_CONS_PRIV)
- Virtual Power and Reset (RESET_SERVER_PRIV)
- Virtual Media (VIRTUAL_MEDIA_PRIV)
- iLO Setting Configuration (CONFIG_ILO_PRIV)
- Login Privilege (LOGIN_PRIV)

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>
```

**NOTE**

GET_FEDERATION_GROUP has not been enhanced to support the extended group privileges available from the iLO 5 web interface. For more information about setting group privileges in iLO 5, see the HPE iLO 5 User Guide.

**Subtopics**


**GET_FEDERATION_GROUP parameters**
This module describes the GET_FEDERATION_GROUP command parameters
**GET_FEDERATION_GROUP runtime errors**
This module describes the GET_FEDERATION_GROUP command runtime errors
**GET_FEDERATION_GROUP return messages**
This module describes the GET_FEDERATION_GROUP command return messages


## GET_FEDERATION_GROUP parameters

This module describes the GET_FEDERATION_GROUP command 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

This module describes the GET_FEDERATION_GROUP command 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

This module describes the GET_FEDERATION_GROUP command 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>
```

## MOD_FEDERATION_GROUP

Use MOD_FEDERATION_GROUP to modify an existing iLO 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 iLO Federation property that is 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>
```



**NOTE**

MOD_FEDERATION_GROUP has not been enhanced to support the extended group privileges available from the iLO 5 web interface. For more information about setting group privileges in iLO 5, see the HPE iLO 5 User Guide.

**Subtopics**

**MOD_FEDERATION_GROUP parameters**
This module describes the MOD_FEDERATION_GROUP command parameters
**MOD_FEDERATION_GROUP runtime errors**
This module describes the MOD_FEDERATION_GROUP command runtime errors

# MOD_FEDERATION_GROUP parameters

This module describes the MOD_FEDERATION_GROUP command 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 can be from the configured minimum password length to 31 characters long. If **Password Complexity** is enabled on the iLO system, the group key must meet the password complexity requirements.

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

This module describes the MOD_FEDERATION_GROUP command runtime errors

Some possible MOD_FEDERATION_GROUP error messages include the following:

- `The GROUP_NAME must not be left blank.`

  **NOTE**

  This error appears only 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.`

# COMPUTER_LOCK_CONFIG

This module describes the COMPUTER_LOCK_CONFIG command.

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 iLO User Guide on the Hewlett Packard Enterprise website at: **http://www.hpe.com/support/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,l"/>
            -->

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

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

**Subtopics**

**COMPUTER_LOCK_CONFIG parameters**
This module describes the COMPUTER_LOCK_CONFIG command parameters.
**COMPUTER_LOCK_CONFIG runtime errors**
This module describes the COMPUTER_LOCK_CONFIG command runtime errors.

## COMPUTER_LOCK_CONFIG parameters

This module describes the COMPUTER_LOCK_CONFIG command 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

This module describes the COMPUTER_LOCK_CONFIG command runtime errors.

Possible COMPUTER_LOCK_CONFIG error messages include:

- `iLO 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

This module describes the GET_NETWORK_SETTINGS command.

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.

For example:

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

**Subtopics**

**GET_NETWORK_SETTINGS parameters**
This module describes the GET_NETWORK_SETTINGS command parameters.
**GET_NETWORK_SETTINGS runtime errors**
This module describes the GET_NETWORK_SETTINGS command runtime errors.
**GET_NETWORK_SETTINGS return messages**

# GET_NETWORK_SETTINGS parameters

This module describes the GET_NETWORK_SETTINGS command parameters.

None

# GET_NETWORK_SETTINGS runtime errors

This module describes the GET_NETWORK_SETTINGS command 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="0"/>
    <SPEED_AUTOSELECT VALUE="Y"/>
    <NIC_SPEED VALUE="Automatic"/>
    <FULL_DUPLEX VALUE="Automatic"/>
    <DHCP_ENABLE VALUE="N"/>
    <DHCP_GATEWAY VALUE="N"/>
    <DHCP_DNS_SERVER VALUE="N"/>
    <DHCP_WINS_SERVER VALUE="N"/>
    <DHCP_STATIC_ROUTE VALUE="N"/>
    <DHCP_DOMAIN_NAME VALUE="N"/>
    <DHCP_SNTP_SETTINGS VALUE="N"/>
    <REG_WINS_SERVER VALUE="N"/>
    <REG_DDNS_SERVER VALUE="Y"/>
    <PING_GATEWAY VALUE="N"/>
    <MAC_ADDRESS VALUE="9c:8e:99:18:07:52"/>
    <IP_ADDRESS VALUE="192.168.1.14"/>
    <SUBNET_MASK VALUE="255.255.255.0"/>
    <GATEWAY_IP_ADDRESS VALUE="0.0.0.0"/>
    <DNS_NAME VALUE="foghat"/>
    <DOMAIN_NAME VALUE="nexus.ilotest.com"/>
    <PRIM_DNS_SERVER VALUE="192.168.1.5"/>
    <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="192.168.1.2"/>
    <SNTP_SERVER2 VALUE=""/>
    <TIMEZONE VALUE="Greenwich"/>
    <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="2001:2:1::14"
                PREFIXLEN="64"
                ADDR_SOURCE="STATIC"
                ADDR_STATUS="ACTIVE"/>
<IPV6_ADDRESS   VALUE="fe80::9e8e:99ff:fe18:752"
                PREFIXLEN="64"
                ADDR_SOURCE="SLAAC"
                ADDR_STATUS="ACTIVE"/>
<IPV6_ADDRESS   VALUE="2001:2:1:0:9e8e:99ff:fe18:752"
                PREFIXLEN="64"
                ADDR_SOURCE="SLAAC"
                ADDR_STATUS="ACTIVE"/>
<IPV6_STATIC_ROUTE_1
                IPV6_DEST="2001:2:2::20"
                PREFIXLEN="64"
                IPV6_GATEWAY="fe80::1:2:3"
                ADDR_STATUS="ACTIVE"/>
<IPV6_STATIC_ROUTE_2
                IPV6_DEST="::"
                PREFIXLEN="0"
                IPV6_GATEWAY="::"
                ADDR_STATUS="INACTIVE"/>
<IPV6_STATIC_ROUTE_3
                IPV6_DEST="2001:1001:2002:3003::"
                PREFIXLEN="64"
                IPV6_GATEWAY="fe80::1:2:3"
                ADDR_STATUS="ACTIVE"/>
<IPV6_PRIM_DNS_SERVER VALUE="2001:1:2::5"/>
<IPV6_SEC_DNS_SERVER VALUE="2001:2:1::5"/>
<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_DOMAIN_NAME VALUE="N"/>
<DHCPV6_SNTP_SETTINGS VALUE="N"/>
<DHCPV6_DNS_SERVER VALUE="N"/>
<ILO_NIC_AUTO_SELECT VALUE="LINKACT"/>
<ILO_NIC_AUTO_SNP_SCAN VALUE="0"/>
```

```
    <ILO_NIC_AUTO_DELAY VALUE="90"/>
    <ILO_NIC_FAIL_OVER VALUE="DISABLED"/>
    <ILO_NIC_FAIL_OVER_DELAY VALUE="300"/>
    <SNP_PORT VALUE="1"/>
</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 values of `PENDING`, `ACTIVE`, or `FAILED` for each address. Pending indicates that the Duplicate Address Detection (DAD) test is still in progress. Failed indicates that a duplicate address was found and it is not currently in use by iLO. 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`, `SLAAC`, or `DHCPv6`, 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 that the route was accepted by the networking stack and is in use. Failed indicates that the route was rejected by the networking stack. Typically the rejection is due to a `No route to source` error for the specified gateway. In this case, iLO periodically retries setting the static route as long as it remains configured. A route to the gateway might be discovered in the future through router advertisements or further iLO address configuration.

# MOD_NETWORK_SETTINGS

This module describes the MOD_NETWORK_SETTINGS command.

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.

iLO reboots in response to changes made to the following:

- All IPv4 settings
- Some settings for IPv6, including the following (if the parameter change requires a reboot):
  - IPV6_PREFERRED_PROTOCOL
  - IPV6_ADDR_AUTOCFG
  - DHCPv6 (all)
- Settings for SNTP and time zone, including the following (only if the parameter change requires a reboot):
  - DHCP_SNTP_SETTINGS
  - DHCPv6_SNTP_SETTINGS
  - SNTP_SERVER1
  - SNTP_SERVER2
  - TIMEZONE

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="Greenwich(GMT)"/>
            <!-- 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"/>
            <!--            iLO 5 - All versions.
-->
            <!--            iLO 4 - Version 1.20 or later.
-->
            <!--            iLO 3 - Version 1.50 or later.
-->
            <!--  VALUES "DISABLED" "LINKACT" "RCVDATA" "DHCP"
-->
            <ILO_NIC_AUTO_SELECT VALUE="DISABLED"/>
            <SNP_PORT VALUE="1"
            <ILO_NIC_AUTO_SNP_SCAN VALUE="0"/>
            <ILO_NIC_AUTO_DELAY VALUE="90"/>
            <ILO_NIC_FAIL_OVER VALUE="DISABLED"/>
            <ILO_NIC_FAIL_OVER_DELAY VALUE="300"/>
        </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" />
    <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:

**NOTE**

While you can add shared network commands to the sample script MOD_NETWORK_SETTINGS.xml, shared network port configuration is included in the sample script `Shared_Network_Port.xml`.

```
<RIBCL version="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="WRITE" >
   <MOD_NETWORK_SETTINGS>
    <SHARED_NETWORK_PORT VALUE="N"/>
           <!--            iLO 5 - All versions                    -->
           <!--            iLO 4 - Version 2.00 and later.         -->
           <!--  VALUES "", "1", "2"                               -->
           <!--
           <SNP_PORT VALUE="1"/>
            -->
   </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. Uncommend the parameters as needed to enable them, and disable (comment out) the equivalent IPv4 parameters. See "IPv6 MOD_NETWORK_SETTINGS parameters" in 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::13"/>
            <!--            Support for the following 5 tags:
-->
            <!--            iLO 5 - All versions.
-->
            <!--            iLO 4 - Version 1.30 and later.
-->
            <!--            iLO 3 - Version 1.60 and later.
-->
            <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"/>
            <!--            iLO 5 - All versions.
-->
            <!--            iLO 4 - Version 1.50 and later.
-->
            <!--            iLO 3 - Version 1.80 and later.
-->
            <DHCPV6_DOMAIN_NAME VALUE="Y"/>
```

**Subtopics**

**MOD_NETWORK_SETTINGS runtime errors**
This module describes the MOD_NETWORK_SETTINGS runtime errors.
**MOD_NETWORK_SETTINGS parameters**
This module describes the MOD_NETWORK_SETTINGS parameters.

# MOD_NETWORK_SETTINGS runtime errors

This module describes the MOD_NETWORK_SETTINGS runtime errors.

Possible MOD_NETWORK_SETTINGS error messages include:

- `iLO information is open for read-only access. Write access is required for this operation.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`
- `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.
- `iLO Shared Network Port is not properly configured.`
  This message is sent if you attempt to modify the value for ILO_NIC_AUTO_SELECT when the iLO dedicated network port is configured. This value can be set only when the iLO shared network port is configured.

# MOD_NETWORK_SETTINGS parameters

This module describes the 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. Not all values, (such as `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.

VLAN_ENABLED—Enables Shared Network Port VLAN ID tagging. The possible values are `Yes` or `No`.

VLAN_ID—Sets the VLAN ID value. Values must be between 1 and 4094.

REG_DDNS_SERVER VALUE instructs iLO to register the management port with a DDNS server. The possible values are `Yes` or `No`.

PING_GATEWAY—When set to `Y`, this causes iLO to send four ICMPv4 echo request packets to the IPv4 gateway when iLO initializes. This keeps the ARP cache entry for iLO updated on the router responsible for routing packets for iLO.

DHCP_DOMAIN_NAME—When set to `Y`, iLO uses the domain name provided by the DHCPv4 server. If both DHCP_DOMAIN_NAME and DHCPV6_DOMAIN_NAME are set to `N`, iLO uses a static value for the domain name, which is set in DOMAIN_NAME.

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`, `1000`, 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. The value can be from 1 to 49 characters. If an empty string is entered, the current value is deleted. Note that other interfaces this is referred to as the Hostname.

DOMAIN_NAME is used to specify the domain name for the network where iLO resides. The value can be from 1 to 64 characters. If an empty string is entered, the current value is deleted. If both DHCP_DOMAIN_NAME and DHCPV6_DOMAIN_NAME are set to `N`, iLO uses the static value from DOMAIN_NAME.

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 whether the iLO NIC must be registers with a WINS server. The possible values are `Yes` or `No`. The parameter value is case sensitive.

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. Your entry for TIMEZONE in RIBCL must match exactly with an item from the Time Zone list in the iLO 5 web interface. To view a list of time zones, in the iLO 5 web interface, navigate to the **SNTP** tabs of either the **iLO Dedicated Network Port** or the **iLO Shared Network Port** pages. View the **Time Zone** list in the **SNTP Settings** section. Note that you cannot open the Time Zone list if either of the settings for **Use DHCPv4 Supplied Time Settings** or **Use DHCPv6 Supplied Time Settings** are enabled.

ILO_NIC_AUTO_SELECT allows iLO to automatically select between either the shared or dedicated network ports at startup. The feature looks for network activity on the ports, and the first port found with network activity is selected for use. Any changes to this setting do not take effect until the iLO is reset. This value can only be set successfully when the shared network port is configured. Valid values include DISABLED, LINKACT, RCVDATA, and DHCP.



**NOTE**

When iLO is searching the NICs for activity, it periodically switches between the available physical NICs. If any of the physical NICs are connected to an unsecured network it may be possible for unauthorized access attempts to occur. Hewlett Packard Enterprise strongly recommends that whenever iLO is connected to any network:

- Use strong passwords for iLO access
- Never connect the ILO dedicated NIC to an unsecured network
- If the server NIC that is shared with iLO is connected to an unsecured network, use VLAN tagging on the iLO portion of the shared NIC and make sure that VLAN is connected to a secure network only.

ILO_NIC_AUTO_SNP_SCAN scans multiple SNP ports during NIC auto-selection when supported by hardware. Valid values are 0 and 2. When the value is set to 0, iLO scans currently configured SNP port. When the value is set to 2, iLO scans the SNP ports 1 and 2. If an empty string is entered, iLO scans the currently configured port.

ILO_NIC_AUTO_DELAY specifies the number of seconds to test each NIC connection before moving to the next while scanning. Valid values are 90 to 1800. If not specified, the delay will default to 90 seconds. Empty string is invalid.

ILO_NIC_FAIL_OVER configures NIC Fail-over feature. Valid values are DISABLED, LINKACT, RCVDATA and DHCP. Empty string disables the feature. To enable this feature, ILO_NIC_AUTO_SELECT tag must also be present and must be a value other than DISABLED.

ILO_NIC_FAIL_OVER_DELAY specifies the number of seconds to monitor each NIC connection before considering the connection as failed and switching to the next NIC. Valid values are 30 to 3600. If not specified, the delay will default to 300 seconds. Empty string is invalid.

SNP_PORT selects which physical NIC port to be used by the iLO Shared Network Port connection, if a port other than 1 is supported. Valid values are `1` and `2`. If port 2 is chosen but not supported, port 1 is selected automatically. Note that even if more than 2 ports are available, for example with a LOM adapter, the iLO shared network port could only be mapped to the either of the first two ports (if supported.)

**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_PREFFERED_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 analagous 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_STATEFULL_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 adresses are used. Value must be either `Y` (enabled) or `N` (disabled).

DHCPV6_DOMAIN_NAME—Determines whether iLO uses the domain name provided by the DHCPv6 server. Value must be either `Y` (enabled) or `N` (disabled). If both DHCP_DOMAIN_NAME and DHCPV6_DOMAIN_NAME are set to `N`, iLO uses a static value for the domain name, which is set in DOMAIN_NAME.

# GET_GLOBAL_SETTINGS

This module describes the GET_GLOBAL_SETTINGS command.

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`.

For example:

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

### Subtopics

**GET_GLOBAL_SETTINGS parameters**
This module describes the GET_GLOBAL_SETTINGS command parameters.

**GET_GLOBAL_SETTINGS runtime errors**
This module describes the GET_GLOBAL_SETTINGS command runtime errors.

# GET_GLOBAL_SETTINGS parameters

This module describes the GET_GLOBAL_SETTINGS command parameters.

None

# GET_GLOBAL_SETTINGS runtime errors

This module describes the GET_GLOBAL_SETTINGS command runtime errors.

None

# GET_GLOBAL_SETTINGS return messages

A possible GET_GLOBAL_SETTINGS return message is as follows:

```
<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"/>
    <RIBCL_STATUS VALUE="Y"/>
    <WEBSERVER_STATUS VALUE="Y"/>
    <WEBGUI_STATUS VALUE="Y"/>
    <REMOTE_CONSOLE_STATUS VALUE="Y"/>
    <VIRTUAL_MEDIA_STATUS VALUE="Y"/>
    <HTTPS_PORT VALUE="443"/>
    <HTTP_PORT VALUE="80"/>
    <REMOTE_CONSOLE_PORT VALUE="17990"/>
    <VIRTUAL_MEDIA_PORT VALUE="17988"/>
    <SNMP_ACCESS_ENABLED VALUE="N"/>
    <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="Y"/>
    <MIN_PASSWORD VALUE="8"/>
    <AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
    <AUTHENTICATION_FAILURE_DELAY_SECS VALUE="10"/>
    <AUTHENTICATION_FAILURES_BEFORE_DELAY VALUE="1"/>
    <RBSU_POST_IP VALUE="Y"/>
    <ENFORCE_AES VALUE="N"/>
    <IPMI_DCMI_OVER_LAN_ENABLED VALUE="Y"/>
    <REMOTE_SYSLOG_ENABLE VALUE="Y"/>
    <REMOTE_SYSLOG_PORT VALUE="514"/>
    <REMOTE_SYSLOG_SERVER_ADDRESS VALUE="172.1.1.1"/>
    <ALERTMAIL_ENABLE VALUE="Y"/>
    <ALERTMAIL_EMAIL_ADDRESS VALUE="user@domain.com"/>
    <ALERTMAIL_SENDER_DOMAIN VALUE="domain.com"/>
    <ALERTMAIL_SMTP_PORT VALUE="25"/>
    <ALERTMAIL_SMTP_SERVER VALUE="smtp.domain.com"/>
    <ALERTMAIL_SMTP_SECURE_ENABLE VALUE="Y"/>
    <ALERTMAIL_SMTP_AUTH_ENABLE VALUE="Y"/>
    <ALERTMAIL_SMTP_AUTH_USERNAME VALUE="username"/>
    <PROPAGATE_TIME_TO_HOST VALUE="Y"/>
    <IPMI_DCMI_OVER_LAN_PORT VALUE="623"/>
</GET_GLOBAL_SETTINGS>
```

## MOD_GLOBAL_SETTINGS

This module describes the MOD_GLOBAL_SETTINGS command.

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. To re-enable iLO functionality, use the UEFI System Utilities. For more information, see the UEFI System Utilities User Guide at **http://www.hpe.com/info/UEFI/docs**.

Use `HPQLOCFG.EXE` version 5.00 or later with the following scripts.

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"/>
            <!--  Firmware support information for next 5 tags:      -->
              <!--      iLO 5 - All versions.                          -->
            <RIBCL_STATUS VALUE="Y"/>
            <WEBSERVER_STATUS VALUE="Y"/>
            <WEBGUI_STATUS VALUE="Y"/>
            <REMOTE_CONSOLE_STATUS VALUE="Y"/>
            <VIRTUAL_MEDIA_STATUS VALUE="Y"/>
            <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"/>
            <!--  Firmware support information for next tag:         -->
              <!--      iLO 4 - All versions.                          -->
              <!--      iLO 3 - All versions.                          -->
            <LOCK_CONFIGURATION value="N"/>
            <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 2 tags:      -->
              <!--      iLO 5 - All versions.                          -->
              <!--      iLO 4 - Version 2.30 and later.                -->
            <!-- <AUTHENTICATION_FAILURE_DELAY_SECS value="10"/>     -->
            <!-- <AUTHENTICATION_FAILURES_BEFORE_DELAY value="1"/>   -->
            <!--  Firmware support information for next 3 tags:      -->
              <!--      iLO 5 - All versions.                          -->
              <!--      iLO 4 - 1.10 or later.                         -->
            <SNMP_ACCESS_ENABLED value = "No"/>
            <SNMP_PORT value="161"/>
            <SNMP_TRAP_PORT value="162"/>
            <!--  Firmware support information for next 7 tags:      -->
```

```
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 1.20 or later.                         -->
          <REMOTE_SYSLOG_ENABLE VALUE="Yes"/>
          <REMOTE_SYSLOG_PORT VALUE="514"/>
          <REMOTE_SYSLOG_SERVER_ADDRESS VALUE="172.20.60.152"/>
          <ALERTMAIL_ENABLE VALUE="yes"/>
          <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 4 tags: -->
          <!-- iLO 5 - 1.30 or later. -->
          <!-- iLO 4 - None. -->
          <!-- iLO 3 - None. -->
          <!-- iLO 2 - None. -->
          <ALERTMAIL_SMTP_SECURE_ENABLE VALUE="Y"/>
          <ALERTMAIL_SMTP_AUTH_ENABLE VALUE="N"/>
          <ALERTMAIL_SMTP_AUTH_USERNAME VALUE=""/>
          <ALERTMAIL_SMTP_AUTH_PASSWORD VALUE=""/>
          <!--  Firmware support information for next tag:         -->
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 1.30 or later.                         -->
          <ALERTMAIL_SMTP_PORT VALUE="25"/>
          <!--  Firmware support information for next tag:         -->
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 1.20 or later.                         -->
            <!--      iLO 3 - 1.55 or later.                         -->
          <IPMI_DCMI_OVER_LAN_ENABLED value="y"/>
          <!--  Firmware support information for next tag:         -->
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 2.50 or later.                         -->
          <IPMI_DCMI_OVER_LAN_PORT value="623"/>
          <!--  Firmware support information for next tag:         -->
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 1.20 or later.                         -->
          <VSP_LOG_ENABLE VALUE="yes" />
          <!--  Firmware support information for next tag:         -->
            <!--      iLO 5 - All versions.                          -->
            <!--      iLO 4 - 1.30 or later.                         -->
            <!--      iLO 3 - 1.60 or later.                         -->
          <PROPAGATE_TIME_TO_HOST VALUE="Y" />
      </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
```

```
   </LOGIN>
</RIBCL>
```

**NOTE**

- The parameters F8_PROMPT_ENABLED and F8_LOGIN_REQUIRED refer to previously assigned function keys for starting UEFI/RBSU in earlier generations of HPE systems. For iLO 5, the key to press for this function has changed to F9 (System Utilities). To ensure backward compatibility, the RIBCL parameter names have not been changed.
- The ENFORCE_AES tag is deprecated for iLO 5. Instead, use the HPE RESTful API Security State setting.

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:

```
<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>
```

**Subtopics**


**MOD_GLOBAL_SETTINGS parameters**
This module describes the MOD_GLOBAL_SETTINGS command parameters.
**MOD_GLOBAL_SETTINGS runtime errors**
This module describes the MOD_GLOBAL_SETTINGS command runtime errors.


# MOD_GLOBAL_SETTINGS parameters

This module describes the MOD_GLOBAL_SETTINGS command 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`.

F8_LOGIN_REQUIRED—Determines if login credentials are required to access the RBSU for iLO. The possible values are `Yes` or `No`.

> **NOTE**
>
> The parameters F8_PROMPT_ENABLED and F8_LOGIN_REQUIRED refer to previously assigned function keys for starting UEFI/RBSU in earlier generations of HPE systems. For iLO 5, the key to press for this function has changed to F9 (System Utilities). To ensure backward compatibility, the RIBCL parameter names have not been changed.

RIBCL_STATUS— Specifies whether RIBCL commands can be used to communicate with iLO. This setting is enabled by default. Valid values are `Yes` or `No`.

WEBSERVER_STATUS— Allows you to enable or disable access through the iLO web server. If you set this value to disabled, iLO will not listen for communication on the Web Server Non-SSL Port or the Web Server SSL port. The following features will not work when the web server is disabled: RIBCL, iLO RESTful API, remote console, iLO Federation, and the iLO web interface. Valid values are `Yes` or `No`.

WEBGUI_STATUS— Specifies whether the iLO web interface can be used to communicate with iLO. This setting is enabled by default. Valid values are `Yes` or `No`.

REMOTE_CONSOLE_STATUS— Allows you to enable or disable access through the iLO remote consoles. Valid values are `Yes` or `No`.

VIRTUAL_MEDIA_STATUS— Allows you to enable or disable the iLO Virtual Media feature. Valid 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.

> **NOTE**
>
> After setting this parameter to `No`, you can use the UEFI System Utilities to re-enable iLO functionality. For more information, see the UEFI System Utilities User Guide for HPE ProLiant Gen10 and Synergy Servers in the HPE Information Library at **http://www.hpe.com/info/UEFI/docs**.

VIRTUAL_MEDIA_PORT—Specifies the port used for virtual media.

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)

AUTHENTICATION_FAILURE_DELAY_SECS—The time, in seconds, that logging in is unavailable when the number of AUTHENTICATION_FAILURES_BEFORE_DELAY is reached.

AUTHENTICATION_FAILURES_BEFORE_DELAY—The number of times authentication can fail before logging in is unavailable for a period of time (set in AUTHENTICAITON_FAILURE_DELAY_SECS).

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 to iLO. 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 IP address is displayed during server POST process. The valid values are `Y` or `1` (enabled) and `N` or `0` (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 252 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 can support unauthenticated and authenticated SMTP connections on port 25 or 587.

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

ALERTMAIL_SMTP_SECURE_ENABLE—Specifies whether to use a secure SMTP connection. Valid values are `Y` (for enabled) and `N` (for disabled).

ALERTMAIL_SMTP_AUTH_ENABLE—Specifies whether to enable authentication on the secure SMTP connection. Valid values are `Y` (for enabled) and `N` (for disabled).

ALERTMAIL_SMTP_AUTH_USERNAME—Sets the username that should be used to authenticate to the secure SMTP server when ALERTMAIL_SMTP_AUTH_ENABLE is set to `Y` (enabled). The maximum string length is 63 characters. Enter blank to clear the field if ALERTMAIL_SMTP_AUTH_ENABLE is set to `N` (disabled).

ALERTMAIL_SMTP_AUTH_PASSWORD-Sets the password to be used to authenticate to the secure SMTP server when ALERTMAIL_SMTP_AUTH_ENABLE is set to `Y` (enabled). The maximum string length is 63 characters. Enter blank to clear the field if ALERTMAIL_SMTP_AUTH_ENABLE is set to `N` (disabled). The requirements for the password length set by the MIN_PASSWORD parameter do not affect ALERTMAIL_SMTP_AUTH_PASSWORD.

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).

IPMI_DCMI_OVER_LAN_PORT—Sets the port used for IPMI communications. The industry standard (default) IPMI port is 623. Valid value is between 1 and 65535.

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

This module describes the MOD_GLOBAL_SETTINGS command runtime errors.

Possible MOD_GLOBAL_SETTINGS error messages include:

- `The IPMI port value specified is invalid. Values supported are between 1 and 65535.`

- `The IPMI_DCMI_OVER_LAN_PORT value must not be left blank.`
- `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.`
- `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.
- `SMTP account credentials and secure connection (SSL/TLS) are required in order to enable Alertmail SMTP Authentication.`

  This message is sent if ALERTMAIL_SMTP_AUTH_ENABLE is set to **`Y`** (enabled) but the username or password ( ALERTMAIL_SMTP_AUTH_USERNAME or ALERTMAIL_SMTP_AUTH_PASSWORD) are blank or ALERTMAIL_SMTP_SECURE_ENABLE is set to **`N`** (disabled).

A possible MOD_GLOBAL_SETTINGS warning message includes:

- `SNMP_ACCESS is disabled, SNMP_PORT and SNMP_TRAP_PORT will not be changed.`

# BROWNOUT_RECOVERY

This module describes the BROWNOUT_RECOVERY command.

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 5.0 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>
```

**Subtopics**

**BROWNOUT_RECOVERY parameters**
This module describes the BROWNOUT_RECOVERY command parameters.
**BROWNOUT_RECOVERY runtime errors**
This module describes the BROWNOUT_RECOVERY runtime errors.

# BROWNOUT_RECOVERY parameters

This module describes the BROWNOUT_RECOVERY command parameters.

`<BROWNOUT_RECOVERY VALUE="No"/>`—Disables brownout recovery

`<BROWNOUT_RECOVERY VALUE="Yes"/>`—Enables brownout recovery

# BROWNOUT_RECOVERY runtime errors

This module describes the BROWNOUT_RECOVERY runtime errors.

None

# GET_SNMP_IM_SETTINGS

This module describes the GET_SNMP_IM_SETTINGS command.

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.

For example:

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

**Subtopics**

**GET_SNMP_IM_SETTINGS parameters**
This module describes the GET_SNMP_IM_SETTINGS command parameters.
**GET_SNMP_IM_SETTINGS runtime errors**
This module describes the GET_SNMP_IM_SETTINGS command runtime errors.
**GET_SNMP_IM_SETTINGS return messages**

# GET_SNMP_IM_SETTINGS parameters

This module describes the GET_SNMP_IM_SETTINGS command parameters.

None

## GET_SNMP_IM_SETTINGS runtime errors

This module describes the GET_SNMP_IM_SETTINGS command 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_ROCOMMUNITY VALUE=""/>
    <SNMP_ADDRESS_2_ROCOMMUNITY VALUE=""/>
    <SNMP_ADDRESS_3_ROCOMMUNITY VALUE=""/>
    <SNMP_ADDRESS_1 VALUE=""/>
    <SNMP_ADDRESS_1_TRAPCOMMUNITY VERSION="" VALUE=""/>
    <SNMP_ADDRESS_1_TRAP_PROTOCOL VALUE=""/>
    <SNMP_ADDRESS_2 VALUE=""/>
    <SNMP_ADDRESS_2_TRAPCOMMUNITY VERSION="" VALUE=""/>
    <SNMP_ADDRESS_2_TRAP_PROTOCOL VALUE=""/>
    <SNMP_ADDRESS_3 VALUE=""/>
    <SNMP_ADDRESS_3_TRAPCOMMUNITY VERSION="" VALUE=""/>
    <SNMP_ADDRESS_3_TRAP_PROTOCOL VALUE=""/>
    <SNMP_V3_ENGINE_ID VALUE=""/>
    <SNMP_PORT VALUE="161"/>
    <SNMP_TRAP_PORT VALUE="162"/>
    <TRAP_SOURCE_IDENTIFIER VALUE="iLO Hostname"/>
    <RIB_TRAPS VALUE="N"/>
    <OS_TRAPS VALUE="N"/>
    <COLD_START_TRAP_BROADCAST VALUE="N"/>
    <SNMP_PASSTHROUGH_STATUS VALUE="N"/>
    <WEB_AGENT_IP_ADDRESS VALUE=""/>
    <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

This module describes the MOD_SNMP_IM_SETTINGS command.

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"/>
       <!--   Firmware support information for the next 2 tags:      -->
       <!--     iLO 3 - All versions.                                 -->
       <!--     iLO 4 - All versions.                                 -->
```

```
       <OS_TRAPS value="Yes"/>
       <SNMP_PASSTHROUGH_STATUS value="No"/>
       <RIB_TRAPS value="No"/>
       <CIM_SECURITY_MASK value="3"/>
           <!--   Firmware support information for the below tags:   -->
           <!--     iLO 5 - All versions.                             -->
           <!--     iLO 4 - All versions.                             -->
       <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="HPE 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 5 - All versions.                             -->
           <!--     iLO 4 - 1.10 or later.                            -->
           <!--   Acceptable values for TRAP_SOURCE_IDENTIFIER:       -->
           <!--     iLO Hostname, OS Hostname                         -->
       <TRAP_SOURCE_IDENTIFIER value = "iLO Hostname"/>
           <!--   Firmware support information for next tags:        -->
           <!--     iLO 5 - All versions.                             -->
           <!--     iLO 4 - 1.20 or later.                            -->
           <!--    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 = "Yes"/>
       <SNMP_PORT value="161"/>
       <SNMP_TRAP_PORT value="162"/>
       <!--   Firmware support information for next tag:   -->
       <!--     iLO 5 - 1.20 or later UNSUPPORTED          -->
       <SNMP_V1_TRAPS VALUE="Yes"/>
       <SNMP_V3_ENGINE_ID VALUE="0x12345678"/>
       <SNMP_USER_PROFILE INDEX = "1">
         <SECURITY_NAME VALUE="SecurityName1"/>
         <AUTHN_PROTOCOL VALUE="0"/>
```

```
        <AUTHN_PASSPHRASE VALUE="AuthenticationPassPhrase1"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="PrivacyPassPhrase1"/>
      </SNMP_USER_PROFILE>
      <SNMP_USER_PROFILE INDEX = "2">
        <SECURITY_NAME VALUE="SecurityName2"/>
        <AUTHN_PROTOCOL VALUE="0"/>
        <AUTHN_PASSPHRASE VALUE="AuthenticationPassPhrase2"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="PrivacyPassPhrase2"/>
      </SNMP_USER_PROFILE>
      <SNMP_USER_PROFILE INDEX = "3">
        <SECURITY_NAME VALUE="SecurityName3"/>
        <AUTHN_PROTOCOL VALUE="0"/>
        <AUTHN_PASSPHRASE VALUE="AuthenticationPassPhrase3"/>
        <PRIVACY_PROTOCOL VALUE="0"/>
        <PRIVACY_PASSPHRASE VALUE="PrivacyPassPhrase3"/>
      </SNMP_USER_PROFILE>
      <!--   Firmware support information for next five tags:   -->
      <!--       iLO 5 - 1.20 or later                          -->
      <!--   If trap protocol is SNMPv3trap, then associated    -->
      <!--   SNMP user index should be given                    -->
      <!--   The possible values for profile index are 1,2,3    -->
      <!--   indicating first, second and third snmpv3 user respectively
-->
      <SNMP_ADDRESS_1_TRAP_PROTOCOL value="SNMPv1Trap"/>
      <SNMP_ADDRESS_2_TRAP_PROTOCOL value="SNMPv3Trap"/>
      <SNMP_ADDRESS_3_TRAP_PROTOCOL value="SNMPv3Trap"/>
      <SNMP_ADDRESS_2_USER_PROFILE_INDEX value="1"/>
      <SNMP_ADDRESS_3_USER_PROFILE_INDEX value="2"/>
    </MOD_SNMP_IM_SETTINGS>
  </RIB_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**

**MOD_SNMP_IM_SETTINGS parameters**
This module describes the MOD_SNMP_IM_SETTINGS command parameters.
**MOD_SNMP_IM_SETTINGS runtime errors**
This module describes the MOD_SNMP_IM_SETTINGS command runtime errors.

# MOD_SNMP_IM_SETTINGS parameters

This module describes the MOD_SNMP_IM_SETTINGS command 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.

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.

SNMP_ADDRESS_*<1-3>*_TRAP_PROTOCOL specifies the protocol of the traps to be associated with SNMP_ADDRESS_<1-3>. Valid values include **`SNMPv1Trap`** or **`SNMPv3Trap`**.

SNMP_ADDRESS_*<1-3>*_USER_PROFILE_INDEX specifies the user profile to associate with each SNMP address. Valid values from RIBCL are **`1, 2,`** or **`3`** when there are three user profiles configured. This parameter is ignored when the associated SNMP_ADDRESS_*<1-3>*_TRAP_PROTOCOL is set to **`SNMPv1Trap`**.

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 configure the SNMP trap community string.

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`.

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 0–4. The possible values are:

- **0**—No change
- **1**—None (no data is returned)
- **2, 3, 4**—Enabled (medium — 3)

COLD_START_TRAP_BROADCAST specifies whether to broadcast to the subnet broadcast IP address when no trap destinations are set for SNMP_ADDRESS_<1-3>. 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 communicates.

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`. This parameter is deprecated for iLO 5 1.20 and later.

SNMP_V3_ENGINE_ID sets the unique identifier of an SNMP engine belonging to an 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, and must have no spaces.
- 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 in 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.



**NOTE**

The following tags are valid only for iLO 5 v1.20 and later:

- SNMP_ADDRESS_*<1-3>*_TRAP_PROTOCOL
- SNMP_ADDRESS_*<1-3>*_USER_PROFILE_INDEX

The SNMP_V1_TRAPS tag is deprecated in iLO 5 v1.20 and later.

# MOD_SNMP_IM_SETTINGS runtime errors

This module describes the MOD_SNMP_IM_SETTINGS command 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.`
- `SNMP_V1_TRAPS is not supported in this platform. Enable SNMPv1 traps per destination.`
- `Cannot set user profile index tag when trap protocol is SNMPv1trap.`
- `Cannot set user profile index tag when trap protocol is not SNMPv3 trap.`
- `User profile index is missing.`
- `SNMPv3 user profile is not configured at index : <user index>`

# SEND_SNMP_TEST_TRAP

Use the SEND_SNMP_TEST_TRAP command to send a test SNMP trap to the configured alert destinations. 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.

For example:

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

**Subtopics**

**SEND_SNMP_TEST_TRAP runtime errors**

## SEND_SNMP_TEST_TRAP runtime errors

- `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.`
- `The iLO is not configured for this command.`
- `Internal error.`
- `Error while reading or writing SNMP data.`

## SEND_SNMP_TEST_TRAP return messages

No information is returned other than a `no error` message.

## 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.

**Subtopics**


**MOD_ENCRYPT_SETTINGS parameters**
**MOD_ENCRYPT_SETTINGS runtime errors**


## 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*. 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. If this parameter is empty or left blank then it will clear an already set ESKM primary server address.

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. If this parameter is empty or left blank then it will clear an already set ESKM primary server port.

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_PORT VALUE specified is invalid. Values supported are between 1 and 65535.`
- `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>
```

The following operations are performed to verify the configuration settings before displaying the primary and secondary ESKM server details:

- iLO connects to the primary ESKM server (and secondary ESKM server, if configured) over SSL.
- iLO tries to authenticate to the ESKM by using the configured credentials and account.
- iLO confirms that the version of the ESKM software is compatible with iLO.

If any of the operations fail, the primary and secondary ESKM server details are displayed as NULL even though they are configured in iLO.

**Subtopics**


**GET_ENCRYPT_SETTINGS parameters**
**GET_ENCRYPT_SETTINGS runtime errors**
**GET_ENCRYPT_SETTINGS return messages**


## 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"/>
    <ESKM_ACC_NAME VALUE="ilo-fc15b4975e90"/>
    <ESKM_CERT_ISSUER VALUE=""/>
    <ESKM_CERT_SUB VALUE=""/>
    <ESKM_GRP_NAME VALUE=""/>
</GET_ENCRYPT_SETTINGS>
</RIBCL>
```

## UPDATE_RIB_FIRMWARE and UPDATE_FIRMWARE

This module describes the UPDATE_FIRMWARE command.

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 only the iLO firmware.
- UPDATE_FIRMWARE flashes other components, such as the CPLD, Power PIC, ROM, and more.

> **WARNING**
> 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 5 - All versions. For servers with TPM enabled.    -->
         <!--    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="<path>\<firmware_filename>"/>
```

```
      </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. Hewlett Packard Enterprise 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>
```

**Subtopics**


**UPDATE_FIRMWARE parameters**
This module describes the UPDATE_FIRMWARE command parameters.
**UPDATE_FIRMWARE runtime errors**
This module describes the UPDATE_FIRMWARE command runtime errors.


## UPDATE_FIRMWARE parameters

This module describes the UPDATE_FIRMWARE command 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

This module describes the UPDATE_FIRMWARE command runtime errors.

Possible UPDATE_FIRMWARE error messages include:

- `iLO 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.`



**NOTE**

If an attempt to use this command fails with errors that involve write access operations, syntax, logins, or configuration privileges, wait for at least 60 seconds before trying again.

## 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.



**NOTE**

iLO 5 requires v1.15 or later of the iLO language pack, and you can install multiple language packs. Installing a new language pack of the same language (v1.15 or later) replaces the currently installed v1.15 language pack. Language packs are not supported on servers that do not have NAND flash memory. To continue using language packs on servers without NAND, use iLO 4 2.10 or earlier. When you upgrade from iLO 4 to iLO 5, previously installed language packs are deleted.

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
       <!-- Firmware support information for next tag:            -->
       <!--   iLO 5 - All versions. For servers with TPM enabled.  -->
       <!--   iLO 4 - All versions. For servers with TPM enabled.  -->
       <TPM_ENABLED VALUE="Yes"/>
       <UPDATE_LANG_PACK IMAGE_LOCATION="<path>\<filename>"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**


**UPDATE_LANG_PACK parameters**
**UPDATE_LANG_PACK runtime errors**


## 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.`

> **NOTE**
>
> If an attempt to use this command fails with errors that involve write access operations, syntax, logins, or configuration privileges, wait for at least 60 seconds before trying again.

# GET_FW_VERSION

This module describes the GET_FW_VERSION command.

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>
```

**Subtopics**

**GET_FW_VERSION parameters**
This module describes the GET_FW_VERSION command parameters
**GET_FW_VERSION runtime errors**
This module describes the GET_FW_VERSION runtime errors.
**GET_FW_VERSION return messages**
This module describes the GET_FW_VERSION return messages.

# GET_FW_VERSION parameters

This module describes the GET_FW_VERSION command parameters

None

## GET_FW_VERSION runtime errors

This module describes the GET_FW_VERSION runtime errors.

None

## GET_FW_VERSION return messages

This module describes the 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_TYPE = iLO license type
/>
```

## LICENSE

This module describes the LICENSE command.

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.



**NOTE**

For more information see the **HPE iLO Licensing Guide** at:

**http://www.hpe.com/support/iLOLicenseGuide-en**

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 KEY="11111222223333344444455555"/>
   </LICENSE>
  </RIB_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**

**LICENSE parameters**
This module describes the LICENSE parameters.
**LICENSE runtime errors**
This module describes the LICENSE runtime errors.

## LICENSE parameters

This module describes the LICENSE parameters.

ACTIVATE KEY followed by a valid value signals the activation of the iLO 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

This module describes the 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 module describes the INSERT_VIRTUAL_MEDIA command.

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 5 - All versions. For servers with TPM enabled.-->
    <!--             iLO 4 - All versions.                               -->
    <!--             iLO 3 - All versions.                               -->
    <!--             iLO 2 - All versions.                               -->
    <INSERT_VIRTUAL_MEDIA DEVICE="FLOPPY" IMAGE_URL="http://<URL>" />
  </RIB_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**

**INSERT_VIRTUAL_MEDIA parameters**
This module describes the INSERT_VIRTUAL_MEDIA command parameters.
**INSERT_VIRTUAL_MEDIA runtime errors**
This module describes the INSERT_VIRTUAL_MEDIA command runtime errors.

# INSERT_VIRTUAL_MEDIA parameters

This module describes the INSERT_VIRTUAL_MEDIA command 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 iLO MAC address.
- `%i` expands to the iLO IP address in dotted-quad form.
- `%h` expands to the iLO 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

This module describes the INSERT_VIRTUAL_MEDIA command runtime errors.

The possible INSERT_VIRTUAL_MEDIA error messages include:

- `iLO information is open for read-only access. Write access is required for this operation.`
- `IMAGE_URL must not be left 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. An iLO license is required to use 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>
```

### Subtopics

**EJECT_VIRTUAL_MEDIA parameters**
This module describes the EJECT_VIRTUAL_MEDIA command parameters.
**EJECT_VIRTUAL_MEDIA runtime errors**
This module describes the EJECT_VIRTUAL_MEDIA command runtime errors.

# EJECT_VIRTUAL_MEDIA parameters

This module describes the EJECT_VIRTUAL_MEDIA command 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

This module describes the EJECT_VIRTUAL_MEDIA command runtime errors.

Possible EJECT_VIRTUAL_MEDIA errors are:

- `iLO 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

This module describes the GET_VM_STATUS command.

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 5 - All versions. For servers with TPM
enabled.  -->
         <!--            iLO 4 - All versions.
-->
         <!--            iLO 3 - All versions.
-->
         <!--            iLO 2 - All versions.
-->
         <GET_VM_STATUS DEVICE="FLOPPY"/>
      </RIB_INFO>
   </LOGIN>
</RIBCL>
```

**Subtopics**

**GET_VM_STATUS parameters**
This module describes the GET_VM_STATUS command parameters.
**GET_VM_STATUS runtime errors**
This module describes the GET_VM_STATUS command runtime errors.
**GET_VM_STATUS return messages**
This module describes the GET_VM_STATUS command return messages.

# GET_VM_STATUS parameters

This module describes the GET_VM_STATUS command 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

This module describes the GET_VM_STATUS command runtime errors.

The possible GET_VM_STATUS error is:

```
An invalid Virtual Media option has been given.
```

# GET_VM_STATUS return messages

This module describes the GET_VM_STATUS command 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 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
IMAGE_URL="<URL>"
```

> **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. An iLO license is required to enable this feature.

For example:

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

```
         <SET_VM_STATUS DEVICE="FLOPPY">
            <VM_BOOT_OPTION VALUE="BOOT_ONCE"/>
            <VM_WRITE_PROTECT VALUE="YES" />
         </SET_VM_STATUS>
      </RIB_INFO>
   </LOGIN>
</RIBCL>
```

**Subtopics**

**SET_VM_STATUS parameters**
This module describes the SET_VM_STATUS command parameters
**SET_VM_STATUS runtime errors**
This module describes the SET_VM_STATUS command.

# SET_VM_STATUS parameters

This module describes the SET_VM_STATUS command 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 connection and boot option parameter for the Virtual Media.

CONNECT and DISCONNECT are two possible values for VM_BOOT_OPTION. 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. Before setting any additional boot options as described below, connect the image by setting the VM_BOOT_OPTION value to CONNECT.

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

- 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`

- 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`

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

This module describes the SET_VM_STATUS command.

The possible runtime errors are:

- `iLO 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 module describes the CERTIFICATE_SIGNING_REQUEST command.

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 version 5.00 or later.

Default response:

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

Custom response:

```
<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"/>
         <CSR_ORGANIZATIONAL_UNIT VALUE =""/>
         <CSR_COMMON_NAME VALUE ="test.com"/>
     </CERTIFICATE_SIGNING_REQUEST>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**


**CERTIFICATE_SIGNING_REQUEST parameters (for custom CSR)**
This module describes the CERTIFICATE_SIGNING_REQUEST command.
**CERTIFICATE_SIGNING_REQUEST errors**
This module describes the CERTIFICATE_SIGNING_REQUEST command.


## CERTIFICATE_SIGNING_REQUEST parameters (for custom CSR)

This module describes the CERTIFICATE_SIGNING_REQUEST command.

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

This module describes the CERTIFICATE_SIGNING_REQUEST command.

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

This module describes the IMPORT_CERTIFICATE command.

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 version 5.00 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-----
    <!--  Ceritificate Data         -->
```

```
      -----END CERTIFICATE-----
   </IMPORT_CERTIFICATE>
   <!--  The iLO will be reset after the certificate has been imported.
-->
   <RESET_RIB/>
  </RIB_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**

**IMPORT_CERTIFICATE parameters**
This module describes the IMPORT_CERTIFICATE command parameters.
**IMPORT_CERTIFICATE errors**
This module describes the IMPORT_CERTIFICATE command errors.

# IMPORT_CERTIFICATE parameters

This module describes the IMPORT_CERTIFICATE command parameters.

None

# IMPORT_CERTIFICATE errors

This module describes the IMPORT_CERTIFICATE command errors.

The possible IMPORT_CERTIFICATE error messages include:

- `iLO 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 5.00 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>
```

**Subtopics**

**AHS_CLEAR_DATA parameters**
This module describes the AHS_CLEAR_DATA command parameters.
**AHS_CLEAR_DATA runtime errors**
This module describes the AHS_CLEAR_DATA command runtime errors.

# AHS_CLEAR_DATA parameters

This module describes the AHS_CLEAR_DATA command parameters.

None

# AHS_CLEAR_DATA runtime errors

This module describes the AHS_CLEAR_DATA command 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 5.00 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>
```

**Subtopics**

**GET_AHS_STATUS parameters**
This module describes the GET_AHS_STATUS command parameters.
**GET_AHS_STATUS runtime errors**
This module describes the GET_AHS_STATUS command runtime errors.

# GET_AHS_STATUS parameters

This module describes the GET_AHS_STATUS command parameters.

None

# GET_AHS_STATUS runtime errors

This module describes the GET_AHS_STATUS command runtime errors.

None

# SET_AHS_STATUS

This module describes the SET_AHS_STATUS command.

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 5.00 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 the AHS logging status is changed the status from `Disabled` to `Enabled`. 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>
```

**Subtopics**

**SET_AHS_STATUS parameters**
This module describes the SET_AHS_STATUS command parameters.
**SET_AHS_STATUS runtime errors**
This module describes the SET_AHS_STATUS command runtime errors.

# SET_AHS_STATUS parameters

This module describes the SET_AHS_STATUS command parameters.

SET_AHS_STATUS—Controls AHS logging. Valid values are **`Enable`** or **`Disable`**.

# SET_AHS_STATUS runtime errors

This module describes the SET_AHS_STATUS command runtime errors.

Some possible error messages for SET_AHS_STATUS:

- `AHS is already enabled.`
- `AHS is already disabled.`

# TRIGGER_BB_DATA

Use this script to initiate Active Health System data submission to the Insight Remote Support server. Use HPQLOCFG version 5.00 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>
```

**Subtopics**

**TRIGGER_BB_DATA parameters**
This module describes the ERS_AHS_SUBMIT command parameters.
**TRIGGER_BB_DATA runtime errors**
This module describes the ERS_AHS_SUBMIT runtime errors.

# TRIGGER_BB_DATA parameters

This module describes the ERS_AHS_SUBMIT command 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**.

## TRIGGER_BB_DATA runtime errors

This module describes the ERS_AHS_SUBMIT runtime errors.

None

## DISABLE_ERS

Use this command to unregister the server from HPE remote support. Use HPQLOCFG version 5.00 or later with this command.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Command to unregister the server.   -->
      <DISABLE_ERS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**

**DISABLE_ERS parameters**
This module describes the DISABLE_ERS command parameters.
**DISABLE_ERS runtime errors**
This module describes the DISABLE_ERS command runtime errors.

## DISABLE_ERS parameters

This module describes the DISABLE_ERS command parameters.

None

## DISABLE_ERS runtime errors

This module describes the DISABLE_ERS command runtime errors.

None

## GET_ERS_SETTINGS

Use this command to retrieve the current Insight Remote Support settings. Use HPQLOCFG version 5.00 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>
```

**Subtopics**

**GET_ERS_SETTINGS parameters**
This module describes the GET_ERS_SETTINGS command parameters.
**GET_ERS_SETTINGS runtime errors**
This module describes the GET_ERS_SETTINGS command runtime errors.

## GET_ERS_SETTINGS parameters

This module describes the GET_ERS_SETTINGS command parameters.

None

# GET_ERS_SETTINGS runtime errors

This module describes the GET_ERS_SETTINGS command 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 version 5.00 or later with this command.

```
<RIBCL VERSION="2.23">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
        <RIB_INFO MODE="write">
            <!-- Command to connect ERS to IRS and register the server.-->
            <SET_ERS_IRS_CONNECT>
                <!-- Host name or IPv4/IPv6 address of IRS server-->
                <ERS_DESTINATION_URL value = "192.168.100.1"/>
                <!-- Port of IRS server                  -->
                <ERS_DESTINATION_PORT value = "7906"/>
            </SET_ERS_IRS_CONNECT>
        </RIB_INFO>
    </LOGIN>
</RIBCL>
```

### Subtopics

**SET_ERS_IRS_CONNECT parameters**
This module describes the SET_ERS_IRS_CONNECT command parameters.
**SET_ERS_IRS_CONNECT runtime errors**
This module describes the SET_ERS_IRS_CONNECT command runtime errors.

# SET_ERS_IRS_CONNECT parameters

This module describes the SET_ERS_IRS_CONNECT command parameters.

ERS_DESTINATION_URL—The host name or IP address of IRS server. The IP address format can be either IPv4 or IPv6.

ERS_DESTINATION_PORT—The port number of the IRS server.

# SET_ERS_IRS_CONNECT runtime errors

This module describes the SET_ERS_IRS_CONNECT command runtime errors.

None

# TRIGGER_L2_COLLECTION

This module describes the TRIGGER_L2_COLLECTION command.

Use this command to initiate an L2 data collection submission to the Insight Remote Support server. Use HPQLOCFG version 5.00 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>
```

### Subtopics

**TRIGGER_L2_COLLECTION parameters**
This module describes the TRIGGER_L2_COLLECTION command parameters.
**TRIGGER_L2_COLLECTION runtime errors**
This module describes the TRIGGER_L2_COLLECTION command runtime errors.

# TRIGGER_L2_COLLECTION parameters

This module describes the TRIGGER_L2_COLLECTION command 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

This module describes the TRIGGER_L2_COLLECTION command runtime errors.

None

# TRIGGER_TEST_EVENT

This module describes the TRIGGER_TEST_EVENT command.

Use this command to initiate a test service event submission to the Insight Remote Support server. Use HPQLOCFG version 5.00 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>
```

### Subtopics

**TRIGGER_TEST_EVENT parameters**
This module describes the TRIGGER_TEST_EVENT command parameters.
**TRIGGER_TEST_EVENT runtime errors**
This module describes the TRIGGER_TEST_EVENT command runtime errors.

# TRIGGER_TEST_EVENT parameters

This module describes the TRIGGER_TEST_EVENT command 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

This module describes the TRIGGER_TEST_EVENT command runtime errors.

None

# SET_LANGUAGE

Use this command to set the default language on iLO. Use HPQLOCFG version 5.00 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>
```

**Subtopics**

**SET_LANGUAGE parameters**
This module describes the SET_LANGUAGE command parameters.
**SET_LANGUAGE runtime errors**
This module describes the SET_LANGUAGE command runtime errors.

# SET_LANGUAGE parameters

This module describes the SET_LANGUAGE command parameters.

LANG_ID is the two letter designation for a language. This parameter is not case sensitive, and must not be blank.

Possible values for LANG_ID are:

- EN (English)

- JA (Japanese)
- ZH (Simplified Chinese)

## SET_LANGUAGE runtime errors

This module describes the SET_LANGUAGE command runtime errors.

A possible error message returned for this command is:

- `Could not set the Default Language.`

## GET_LANGUAGE

This module describes the GET_LANGUAGE command.

Use this command to read the default language on iLO. Use HPQLOCFG version 5.00 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>
```

**Subtopics**

**GET_LANGUAGE parameters**
This module describes the GET_LANGUAGE command parameters.
**GET_LANGUAGE runtime errors**
This module describes the GET_LANGUAGE command runtime errors.

# GET_LANGUAGE parameters

This module describes the GET_LANGUAGE command parameters.

None

# GET_LANGUAGE runtime errors

This module describes the GET_LANGUAGE command runtime errors.

None

# GET_ALL_LANGUAGES

This module describes the GET_ALL_LANGUAGES command.

Use this command to read all languages on iLO. Use HPQLOCFG version 5.00 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>
```

**Subtopics**

**GET_ALL_LANGUAGES parameters**
This module describes the GET_ALL_LANGUAGES command parameters.
**GET_ALL_LANGUAGES runtime errors**
This module describes the GET_ALL_LANGUAGES command runtime errors.

# GET_ALL_LANGUAGES parameters

This module describes the GET_ALL_LANGUAGES command parameters.

None

# GET_ALL_LANGUAGES runtime errors

This module describes the GET_ALL_LANGUAGES command runtime errors.

None

# GET_ASSET_TAG

This module describes the GET_ASSET_TAG command.

Use this command to get the asset tag. Use HPQLOCFG version 5.00 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>
```

### Subtopics

**GET_ASSET_TAG parameters**
This module describes the GET_ASSET_TAG command parameters.
**GET_ASSET_TAG runtime errors**
This module describes the GET_ASSET_TAG command runtime errors.

# GET_ASSET_TAG parameters

This module describes the GET_ASSET_TAG command parameters.

None

## GET_ASSET_TAG runtime errors

This module describes the GET_ASSET_TAG command 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

This module describes the SET_ASSET_TAG command.

Use this command to set or clear the asset tag. Use HPQLOCFG version 5.00 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>
```

### Subtopics

**SET_ASSET_TAG parameters**
This module describes the SET_ASSET_TAG command parameters.

**SET_ASSET_TAG runtime errors**
This module describes the SET_ASSET_TAG command runtime errors.

# SET_ASSET_TAG parameters

This module describes the SET_ASSET_TAG command 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

This module describes the SET_ASSET_TAG command 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>
```

**Subtopics**

**GET_SECURITY_MSG parameters**
This module describes the GET_SECURITY_MSG command parameters.
**GET_SECURITY_MSG return messages**
This module describes the returns from GET_SECURITY_MSG. Info added during iLO 4 v1.10 release cycle.
**GET_SECURITY_MSG runtime errors**
This module describes the GET_SECURITY_MSG command runtime errors.

# GET_SECURITY_MSG parameters

This module describes the GET_SECURITY_MSG command parameters.

None

# GET_SECURITY_MSG return messages

This module describes the returns from GET_SECURITY_MSG. Info added during iLO 4 v1.10 release cycle.

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

This module describes the GET_SECURITY_MSG command 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 must have the Configure iLO Setting privileges to change 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>
```

### Subtopics

**SET_SECURITY_MSG parameters**
This module describes the SET_SECURITY_MSG command parameters.
**SET_SECURITY_MSG runtime errors**
This module describes the SET_SECURITY_MSG command runtime errors.

## SET_SECURITY_MSG parameters

This module describes the SET_SECURITY_MSG command 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

This module describes the SET_SECURITY_MSG command runtime errors.

The value for the SECURITY_MESSAGE parameter must a `Y` or an `N`, otherwise the command reports an error:

```
Boolean value not specified.
```

You may also see this error:

```
User does NOT have correct privilege for action. CONFIG_ILO_PRIV required.
```

## 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. Use HPQLOCFG.EXE version 5.00 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>
```

**Subtopics**

**HOTKEY_CONFIG parameters**
**HOTKEY_CONFIG runtime errors**

## 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 | : | I | x | 4 |
| DEL | F7 | < | j | 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:

- `iLO 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 version 5.00 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>
```

**Subtopics**

**GET_HOTKEY_CONFIG parameters**
**GET_HOTKEY_CONFIG runtime errors**
**GET_HOTKEY_CONFIG return messages**

## 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. Use HPQLOCFG.EXE version 5.00 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>
```

### Subtopics


**PROFILE_APPLY parameters**
**PROFILE_APPLY runtime errors**


# 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 alphanumerics 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 version 5.00 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>
```

**Subtopics**


**PROFILE_APPLY_GET_RESULTS parameters**
**PROFILE_APPLY_GET_RESULTS runtime errors**

## 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 version 5.00 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>
```

**Subtopics**


**PROFILE_DELETE parameters**
**PROFILE_DELETE runtime errors**


## 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 or equal to 27 characters long. Only alphanumerics 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 version 5.00 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>
```

**Subtopics**

**PROFILE_LIST parameters**
**PROFILE_LIST runtime errors**

## 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 version 5.00 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>
```

**Subtopics**


**PROFILE_DESC_DOWNLOAD parameters**
**PROFILE_DESC_DOWNLOAD runtime errors**


## 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 fewer than 27 characters long. Only alphanumerics 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 alphanumerics and underscores are accepted; spaces, periods, and slashes are

invalid. Hewlett Packard Enterprise 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 mode. Use HPQLOCFG version 5.00 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>
```

**NOTE**

To disable FIPS, use the FACTORY_DEFAULTS command.

**Subtopics**

**FIPS_ENABLE parameters**
**FIPS_ENABLE runtime errors**

## 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.
```

> **NOTE**
>
> This tag may not take effect when the iLO 5 security state is set to SuiteB/CNSA. For more information on security states, see the iLO 5 user guide.

# GET_FIPS_STATUS

Use this script to retrieve the current FIPS mode status. Use HPQLOCFG version 5.00 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>
```

### Subtopics


**GET_FIPS_STATUS parameters**
**GET_FIPS_STATUS runtime errors**
**GET_FIPS_STATUS return messages**

## 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. Use HPQLOCFG version 5.00 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>
```

**Subtopics**


**GET_ALL_LICENSES parameters**
**GET_ALL_LICENSES runtime errors**
**GET_ALL_LICENSES return messages**

## 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="2.23">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
    />
<GET_ALL_LICENSES>
    <LICENSE>
         <LICENSE_TYPE VALUE= "iLO Advanced"/>
         <LICENSE_KEY VALUE= "<advanced license key value>"/>
                     <LICENSE_INSTALL_DATE VALUE="Tue Jan 17 15:57:30
2017"/>
         <LICENSE_CLASS VALUE="FQL"/>
         <LICENSE_STATE VALUE="<State>"/>
         <LICENSE_TIER VALUE="<Tier>"/>
    </LICENSE>
</GET_ALL_LICENSES>
</RIBCL>
```

# FACTORY_DEFAULTS

Use this command to set the iLO device to factory default settings. Use HPQLOCFG version 5.00 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 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.



**NOTE**

You must reboot the host operating system after setting the iLO to factory defaults.

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

**Subtopics**


**FACTORY_DEFAULTS parameters**
**FACTORY_DEFAULTS runtime errors**


## FACTORY_DEFAULTS parameters

None

## FACTORY_DEFAULTS runtime errors

None

# IMPORT_SSH_KEY

The IMPORT_SSH_KEY command imports an SSH_KEY and associated iLO username into iLO. This command requires HPQLOCFG version 5.00 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:

   `ssh-dss .`

2. At the end of the key, append a space and the name of a valid iLO 5 username as displayed on the Modify User page. For example:

   `xxx_some-text_xxx ASmith`

The username is case-sensitive and must match the iLO 5 username to associate the SSH key with the correct user.

```
<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+aKqFjlfO1NjszHrFN26H1AhWOjY2bEwj2wlJzBMAhXwnPQelQsCnJDf+
zCzbDn+5Va86+qWxm0lsDEChvZPM6wpjkXvHwuInjxTzOGQTq++vmYlo1/AAAAFQC1M
FaZjE995QhX9H1DaDzpsVTXvwAAAIA6ec/hAkas2N762jtlHvSuvZaQRzu49DOtjXVI
pNdJAhTC8O2505PzkGLf5qhrbDnusclCvoH7DuxyHjeOUVxbC5wFQBcGF4VnpYZ8nGQ
Gt9TQ0iUV+NRwn4CR5ESoi63zTJIvKIYZDT2ISeXhF2iU6txjZzdeEm7vQz3slaY3dg
AAAIAQ46i6FBzJAYXziF/qmWMt4y6SlylOQDAsxPKk7rpxegv8RlTeon/aeL7ojb9GQ
2xnEN5gobaNZxKz2d4/jwg3+qgTDT6V1G+b7+nEI/XHIc717/7oqgiOv4VE3WxN+HE9
JWsv2jwUpAzRGqJOoojRG/CCru0K+jgTOf/di1o0sw== ASmith
-----END SSH KEY-----
   </IMPORT_SSH_KEY>
  </RIB_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**

**IMPORT_SSH_KEY parameters**
This module describes the IMPORT_SSH_KEYcommand parameters.
**IMPORT_SSH_KEY runtime errors**
This module describes the IMPORT_SSH_KEYcommand runtime errors.

## IMPORT_SSH_KEY parameters

This module describes the IMPORT_SSH_KEYcommand parameters.

None

## IMPORT_SSH_KEY runtime errors

This module describes the IMPORT_SSH_KEYcommand runtime errors.

A possible IMPORT_SSH_KEY error message includes:

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

## LOCK_CONFIGURATION

The LOCK_CONFIGURATION command enables or disables the **Require Host Authentication** access setting. 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 5.0 or later. 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_GLOBAL_SETTINGS>
     <LOCK_CONFIGURATION value="Y"/>
   </MOD_GLOBAL_SETTINGS>
```

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

**Subtopics**


**LOCK_CONFIGURATION parameters**
**LOCK_CONFIGURATION runtime errors**


## LOCK_CONFIGURATION parameters

`<LOCK_CONFIGURATION value="N"/>` —Disables the **Require Host Authentication** access setting.

`<LOCK_CONFIGURATION value="Y"/>` —Enables the **Require Host Authentication** access setting.

## LOCK_CONFIGURATION runtime errors

None

## DIR_INFO

This module describes the DIR_INFO command.

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>
```

**Subtopics**


**GET_DIR_CONFIG**
This module describes the GET_DIR_CONFIG command.
**MOD_DIR_CONFIG**
**IMPORT_LDAP_CA_CERTIFICATE**
**GET_LDAP_CA_CERTIFICATE_STATUS**
**MOD_KERBEROS**
**START_DIR_TEST**
**ABORT_DIR_TEST**
**GET_DIR_TEST_RESULTS**


# GET_DIR_CONFIG

This module describes the GET_DIR_CONFIG command.

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>
```



**NOTE**

The information returned by GET_DIR_CONFIG has not been enhanced to support the extended group privileges available from the iLO 5 web interface. For more information about user and group privileges in iLO 5, see the HPE iLO 5 User Guide in the HPE Information Library at **http://www.hpe.com/support/ilo-docs**.

**Subtopics**

**GET_DIR_CONFIG parameters**
This module describes the GET_DIR_CONFIG command parameters.
**GET_DIR_CONFIG runtime errors**
This module describes the GET_DIR_CONFIG command runtime errors.
**GET_DIR_CONFIG return messages**
This module describes the GET_DIR_CONFIG command return messages.

# GET_DIR_CONFIG parameters

This module describes the GET_DIR_CONFIG command parameters.

None

# GET_DIR_CONFIG runtime errors

This module describes the GET_DIR_CONFIG command runtime errors.

None

# GET_DIR_CONFIG return messages

This module describes the GET_DIR_CONFIG command return messages.

Directory integration works with Lights-Out schema with or without extensions (schema-free). Depending on your directory configuration, the response to GET_DIR_CONFIG may contain 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_GENERIC_LDAP_ENABLED VALUE="N"/>
<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_GENERIC_LDAP_ENABLED VALUE="N">
<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 iLO directory settings. 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 Configure iLO Settings privilege is required to execute this command.

MOD_DIR_CONFIG is used in different ways, depending on the environment.

- See MOD_DIRECTORY.xml example for an example that shows directory integration and existing schemas.
- See Schemaless directory example (MOD_SCHEMALESS_DIR.XML) for an example that shows a schemaless directory configuration.

### Directory configuration notes

- To modify only the Kerberos authentication, start with the sample script `Mod_Kerberos_Config.xml`.
- Do not use the following tags when using directory integration with an extended schema:
  - 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

**MOD_DIRECTORY.xml 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 5 - All versions.
-->
            <!--            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 HPE 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"/>
            <DIR_GENERIC_LDAP_ENABLED VALUE="yes">
    <!-- Firmware support information for next 5 tags: -->
    <!-- iLO 5 - All versions.                          -->
    <!-- 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>
```

### Schemaless directory example (MOD_SCHEMALESS_DIR.XML)

```
<!--         RIBCL Sample Script for HPE Lights-Out Products          -->
<!--Copyright (c) 2003, 2019 Hewlett-Packard Enterprise Development LP-->

<!-- Description:  This is a sample XML script to modify the current -->
<!--               schemaless directory configuration on following   -->
<!--               device:                                           -->
<!--                 Integrated Lights-Out 5 (iLO 5)                 -->
<!--                 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.                                    -->
```

```
<!--        See "iLO Scripting and Command Line Guide" for more      -->
<!--        information on scripting and the syntax of the RIBCL     -->
<!--        XML.                                                     -->

<!--        Firmware support information for this script:            -->
<!--            iLO 5 - All versions.                                -->
<!--            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 5 - All versions.                             -->
            <!--       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 5 - All versions.                             -->
            <!--       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 5 - All versions.                             -->
            <!--       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 5 - All versions.                             -->
            <!--       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 5 - All versions.                             -->
            <!--       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 5 - All versions.                             -->
            <!--       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>
```

**Subtopics**

**MOD_DIR_CONFIG parameters**
This module describes the MOD_DIR_CONFIG command.
**MOD_DIR_CONFIG runtime errors**
This module describes the MOD_DIR_CONFIG command.

# MOD_DIR_CONFIG parameters

This module describes the MOD_DIR_CONFIG command.

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`.

DIR_GENERIC_LDAP_ENABLED enables or disables OpenLDAP support. This works only in schema-free mode. 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 Settings
  - **6**—Login Privilege (This value is only supported by iLO 3 and iLO 4.)

  **NOTE**

  Do not use the following tags when using directory integration with schema extension:

  - DIR_ENABLE_GRP_ACCT
  - DIR_GRPACCT1_NAME
  - DIR_GRPACCT1_PRIV
  - DIR_GENERIC_LDAP_ENABLED

  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 in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

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

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2, and DIR_USER_CONTEXT_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

This module describes the MOD_DIR_CONFIG command.

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.`

## IMPORT_LDAP_CA_CERTIFICATE

Use this command to import a directory server's CA certificate to iLO. On successful import of the certificate, the directory server certificate validation option is enabled. This feature ensures that iLO connects to the correct directory server during LDAP authentication. Use HPQLOCFG version 5.00 or later with this command. Replace USER_LOGIN and PASSWORD values with values that are appropriate for your environment.

For example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
      <DIR_INFO MODE="write">
         <IMPORT_LDAP_CA_CERTIFICATE>
-----BEGIN CERTIFICATE-----
<!--      Certificate Data          -->
-----END CERTIFICATE-----
         </IMPORT_LDAP_CA_CERTIFICATE>
      </DIR_INFO>
   </LOGIN>
</RIBCL>
```

### IMPORT_LDAP_CA_CERTIFICATE parameters

None

### IMPORT_LDAP_CA_CERTIFICATE runtime errors

The possible IMPORT_LDAP_CA_CERTIFICATE error messages include:

- `iLO information is open for read-only access. Write access is required for this operation.`
- `User does NOT have correct privilege for action. CONFIG_ILO_PRIV required.`
- `Failed to import the certificate.`

## GET_LDAP_CA_CERTIFICATE_STATUS

Use this command to check if an LDAP server's CA certificate is currently loaded or not. Use HPQLOCFG version 5.00 or later with this command. Replace USER_LOGIN and PASSWORD values with values that are appropriate for your environment. For example:

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

### GET_LDAP_CA_CERTIFICATE_STATUS parameters

None

### GET_LDAP_CA_CERTIFICATE_STATUS runtime errors

None

### GET_LDAP_CA_CERTIFICATE_STATUS return messages

A possible GET_LDAP_CA_CERTIFICATE_STATUS return message is:

```
<GET_LDAP_CA_CERTIFICATE_STATUS>
    <LDAP_CA_CERTIFICATE_STATUS VALUE="Not Loaded"/>
</GET_LDAP_CA_CERTIFICATE_STATUS>
```

Or

```
<GET_LDAP_CA_CERTIFICATE_STATUS>
    <LDAP_CA_CERTIFICATE_STATUS VALUE="Loaded"/>
</GET_LDAP_CA_CERTIFICATE_STATUS>
```

## 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
BpcyBvbmx5IGEgdGVz
dC4=
-----END KEYTAB-----
         </DIR_KERBEROS_KEYTAB>
      </MOD_DIR_CONFIG>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```

## START_DIR_TEST

The START_DIR_TEST command enables you to validate the configured directory settings. For this command to parse correctly, the START_DIR_TEST 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.

> **NOTE**
>
> The directory test results are reset when directory settings are saved, or when the directory tests are started.

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
      <DIR_INFO MODE="write">
         <START_DIR_TEST>
            <DIR_ADMIN_DISTINGUISHED_NAME VALUE="ad_admin_username"/>
            <DIR_ADMIN_PASSWORD VALUE="password"/>
            <TEST_USER_NAME VALUE="test_user_name"/>
            <TEST_USER_PASSWORD VALUE="password"/>
        </START_DIR_TEST>
      </DIR_INFO>
   </LOGIN>
</RIBCL>
```

**Subtopics**

**START_DIR_TEST parameters**
**START_DIR_TEST runtime errors**

## START_DIR_TEST parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting will be left empty.

- DIR_ADMIN_DISTINGUISHED_NAME searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.
- DIR_ADMIN_PASSWORD authenticates the directory administrator.
- TEST_USER_NAME tests login and access rights to iLO. This name does not need to be fully distinguished because user search contexts can be applied. This user must be associated with a role for this iLO.
- TEST_USER_PASSWORD authenticates the test user.

## START_DIR_TEST runtime errors

Possible START_DIR_TEST 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.`

## ABORT_DIR_TEST

The ABORT_DIR_TEST command stops a running directory test. For this command to parse correctly, the ABORT_DIR_TEST 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.

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

#### Subtopics

**ABORT_DIR_TEST runtime errors**

## ABORT_DIR_TEST runtime errors

Possible ABORT _DIR_TEST error messages include:

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

# GET_DIR_TEST_RESULTS

The GET_DIR_TEST_RESULTS command requests the results of directory tests. For this command to parse correctly, the GET_DIR_TEST_RESULTS command must appear within a DIR_INFO command block, and DIR_INFO MODE must be set to read. The user must have the Configure iLO Settings privilege to execute this command.

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

**Subtopics**

**GET_DIR_TEST_RESULTS runtime errors**

# GET_DIR_TEST_RESULTS runtime errors

Possible GET_DIR_TEST_RESULTS error messages include:

- `This iLO information is read only. Write is not allowed.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`
- `Directory test is in progress, please try after some time.`
- `Directory test is not running.`
- `Directory test aborted.`
- `Aborting Directory test.`

# 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>
```

**Subtopics**

**GET_RACK_SETTINGS**

# GET_RACK_SETTINGS

The GET_RACK_SETTINGS 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>
```

**Subtopics**

**GET_RACK_SETTINGS parameters**
**GET_RACK_SETTINGS runtime errors**
**GET_RACK_SETTINGS return messages**

## GET_RACK_SETTINGS parameters

None

## GET_RACK_SETTINGS runtime errors

A possible error message includes:

- `Server is NOT a rack server; Rack commands do not apply.`

## GET_RACK_SETTINGS return messages

A possible GET_RACK_SETTINGS return message is:

```
 <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>
```

**Subtopics**

**GET_OA_INFO**

# GET_OA_INFO

The GET_OA_INFO command requests the Onboard Administrator information from the enclosure where iLO 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>
```

**Subtopics**

**GET_OA_INFO parameters**
**GET_OA_INFO runtime errors**
**GET_OA_INFO return messages**

# GET_OA_INFO parameters

None

## GET_OA_INFO runtime errors

A possible error message includes:

- `Server is NOT a rack server; Rack commands do not apply.`

## GET_OA_INFO return messages

A possible GET_OA_INFO return message is:

```
<GET_OA_INFO>
<ipAddress>192.168.1.105</ipAddress/>
<ipv6Address>fe80::223:7dff:fea6:c80d</ipv6Address>
<macAddress>00:22:44:55:33:77</macAddress/>
<System_Health>2</System_Health>
<uidStatus>On</uidStatus>
<RACK>Rackname</RACK>
<ENCL>Enclosurename</ENCL>
<Location>7</Location>
</GET_OA_INFO>
```

Where the value returned for `System_Health` is a number, 1-4:

1. Unknown
2. Good
3. Degraded
4. Critical

In the example above, the system health is good.

## SERVER_INFO

This module describes the SERVER_INFO command.

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>
```

**Subtopics**

**GET_TPM_STATUS**
**GET_CURRENT_BOOT_MODE**
**GET_PENDING_BOOT_MODE**
**SET_PENDING_BOOT_MODE**

**GET_PERSISTENT_BOOT**
**SET_PERSISTENT_BOOT (Legacy)**
**SET_PERSISTENT_BOOT (UEFI)**
**GET_ONE_TIME_BOOT**
**SET_ONE_TIME_BOOT**
**GET_SDCARD_STATUS**
**GET_SUPPORTED_BOOT_MODE**
**GET_SERVER_NAME**
**SERVER_NAME**
**GET_SERVER_FQDN**
**SERVER_FQDN**
**GET_PRODUCT_NAME**
**GET_EMBEDDED_HEALTH**
This module describes the GET_EMBEDDED_HEALTH command.
**GET_POWER_READINGS**
This module describes the GET_POWER_READINGS command.
**GET_PWREG**
**SET_PWREG**
**GET_PS_DATA**
**GET_POWER_CAP**
This module describes the GET_POWER_CAP command.
**SET_POWER_CAP**
This module describes the SET_POWER_CAP command return messages.
**SET_CRITICAL_TEMP_REMAIN_OFF**
**GET_CRITICAL_TEMP_REMAIN_OFF**
**GET_HOST_POWER_SAVER_STATUS**
This section describes the GET_HOST_POWER_SAVER_STATUS command.
**SET_HOST_POWER_SAVER**
This module describes the SET_HOST_POWER_SAVER command.
**GET_HOST_POWER_STATUS**
This section describes the GET_HOST_POWER_STATUS command.
**SET_HOST_POWER**
**GET_HOST_PWR_MICRO_VER**
This module describes the GET_HOST_PWR_MICRO_VER command.
**RESET_SERVER**
This module describes the RESET_SERVER command.
**PRESS_PWR_BTN**
**HOLD_PWR_BTN**
**COLD_BOOT_SERVER**
**WARM_BOOT_SERVER**
**SERVER_AUTO_PWR**
**GET_SERVER_AUTO_PWR**
This module describes the GET_SERVER_AUTO_PWR command.
**GET_UID_STATUS**
**UID_CONTROL**

**SET_PERS_MOUSE_KEYBOARD_ENABLED**
**GET_PERS_MOUSE_KEYBOARD_ENABLED**
**GET_SERVER_POWER_ON_TIME**

# GET_TPM_STATUS

Use GET_TPM_STATUS to retrieve the status of the HPE 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. 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_TPM_STATUS/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**

**GET_TPM_STATUS parameters**
**GET_TPM_STATUS runtime errors**
**GET_TPM_STATUS return messages**

# 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"/>
    <TRUSTED_MODULE_TYPE VALUE="TPM 2.0"/>
    <TPM_CHIP_IDENTIFIER VALUE="STMicro"/>
    <TRUSTED_MODULE_VERSION VALUE="73"/>
</GET_TPM_STATUS>
</RIBCL>
```

## GET_CURRENT_BOOT_MODE

Use GET_CURRENT_BOOT_MODE to retrieve the current boot mode. The response will include either `legacy` boot mode or `UEFI` 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 can be set to either `read` or `write`. 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` or `UEFI`.

### Subtopics


**GET_CURRENT_BOOT_MODE parameters**
**GET_CURRENT_BOOT_MODE runtime errors**
**GET_CURRENT_BOOT_MODE return messages**

## 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 can be set to either `read` or `write`.

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`.

**Subtopics**


**GET_PENDING_BOOT_MODE parameters**
**GET_PENDING_BOOT_MODE runtime errors**
**GET_PENDING_BOOT_MODE return messages**


## 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>
```

**Subtopics**


**SET_PENDING_BOOT_MODE parameters**
**SET_PENDING_BOOT_MODE runtime errors**


## 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 can be set to either `read` or `write`.

For example:

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

**Subtopics**

**GET_PERSISTENT_BOOT return messages**

## 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="NETWORK1"/>
  <DEVICE value="NETWORK2"/>
  <DEVICE value="NETWORK3"/>
  <DEVICE value="NETWORK4"/>
  <DEVICE value="NETWORK5"/>
  <DEVICE value="NETWORK6"/>
  <DEVICE value="NETWORK7"/>
  <DEVICE value="NETWORK8"/>
  <DEVICE value="NETWORK9"/>
  <DEVICE value="NETWORK10"/>
  <DEVICE value="NETWORK11"/>
  <DEVICE value="NETWORK12"/>
</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 :
HPE
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 :
HPE
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 towards 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>
```

**Subtopics**


**SET_PERSISTENT_BOOT parameters**
**SET_PERSISTENT_BOOT runtime errors**


## 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, 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.

**Subtopics**


**SET_PERSISTENT_BOOT parameters**
**SET_PERSISTENT_BOOT runtime errors**

# 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 :
HPE
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 :
HPE
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 when using SET_PERSISTENT_BOOT 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>
```

**Subtopics**

**GET_ONE_TIME_BOOT return messages**

## 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`
- `<Boot*XXXX*>`

> **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.

> **NOTE**
>
> If the return message shows `BOOT_TYPE VALUE="INVALID"`, you may have selected a one time boot mode in the iLO web interface that is not supported by iLO 5 RIBCL or on the command line, such as HTTP Boot.

# 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>
```

**Subtopics**

**SET_ONE_TIME_BOOT parameters**
**SET_ONE_TIME_BOOT runtime errors**

# SET_ONE_TIME_BOOT parameters

The `value` sets a specified device as the source for a single boot. Valid values include the following:

- `NORMAL`
- `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 5 options:

- `EMB-MENU` —Displays the default boot menu
- `EMB-ACU` —Boots into ACU
- `EMB-HPSUM-AUTO` —Boots HPSUM in automatic update mode
- `RBSU` —Boots into the system RBSU.

**NOTE**

In the iLO 5 web interface, it is possible to set an HTTP boot. This boot mode is not supported on the command line or RIBCL scripts.

## 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_SDCARD_STATUS

Use GET_SDCARD_STATUS to determine whether an SD (secure digital) card is connected to the 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. You can set the SERVER_INFO MODE to `read` or `write`.

For example:

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

Possible values returned include:

- `PRESENT`
- `NOT PRESENT`
- `UNKNOWN`

**Subtopics**

**GET_SDCARD_STATUS return messages**

# GET_SDCARD_STATUS return messages

A possible GET_SDCARD_STATUS return message includes:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<RESPONSE
    STATUS="0x0000"
```

```
    MESSAGE='No error'
     />
<GET_SDCARD_STATUS>
  <SDCARD_STATUS VALUE="PRESENT"/>
</GET_SDCARD_STATUS>
</RIBCL>
```

# 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. You can set the SERVER_INFO MODE to `read` or `write` .

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`

### Subtopics

**GET_SUPPORTED_BOOT_MODE return messages**
**GET_SUPPORTED_BOOT_MODE runtime errors**

# 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.

### Subtopics

**GET_SERVER_NAME return message**
This module describes the GET_SERVER_NAME command return message

**GET_SERVER_NAME runtime errors**
This module describes the GET_SERVER_NAME command runtime errors.

## GET_SERVER_NAME return message

This module describes the GET_SERVER_NAME command 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

This module describes the GET_SERVER_NAME command 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>
```

**Subtopics**

**SERVER_NAME parameters**
This module describes the SERVER_NAME command parameters.
**SERVER_NAME return message**
This module describes the SERVER_NAME command return messages.
**SERVER_NAME runtime errors**
This module describes the SERVER_NAME command runtime errors.

## SERVER_NAME parameters

This module describes the SERVER_NAME command parameters.

VALUE is a quoted ASCII string less than 50 characters in total length.

## SERVER_NAME return message

This module describes the SERVER_NAME command return messages.

If this attribute is successfully set, no specific message returns.

## SERVER_NAME runtime errors

This module describes the SERVER_NAME command runtime errors.

- If the configure iLO settings privilege is absent, a runtime error is returned:

  ```
  User does NOT have correct privilege for action. CONFIG_ILO_PRIV required.
  ```

- If SERVER_INFO is not opened for write, a runtime error is returned.

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

# GET_SERVER_FQDN

The GET_SERVER_FQDN command is used to retrieve the fully qualified domain name of the server.

For example:

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

**Subtopics**

**GET_SERVER_FQDN**
**GET_SERVER_FQDN**

# GET_SERVER_FQDN

None

# GET_SERVER_FQDN

A typical response for this command 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>
```

# SERVER_FQDN

The command SERVER_FQDN sets the fully qualified domain name for the server. IP addresses are also accepted. 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` 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" />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**


**SERVER_FQDN parameters**
**SERVER_FQDN return messages**
**SERVER_FQDN runtime errors**


# SERVER_FQDN parameters

SERVER_FQDN—Value must be the FQDN or IP address of the host server.

# SERVER_FQDN return messages

If the attributes are successfully set, no specific messages return.

# SERVER_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. You can set the SERVER_INFO MODE to read or write.

For example:

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

**Subtopics**

**GET_PRODUCT_NAME runtime errors**
**GET_PRODUCT_NAME return messages**

# GET_PRODUCT_NAME runtime errors

None.

# GET_PRODUCT_NAME return messages

A possible GET_PRODUCT_NAME return message includes:

```
<RIBCL VERSION="2.0">
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
    />
  <GET_PRODUCT_NAME>
    <PRODUCT_NAME VALUE ="<HPE Gen10 server name>"/>
  </GET_PRODUCT_NAME>
</RIBCL>
```

# GET_EMBEDDED_HEALTH

This module describes the GET_EMBEDDED_HEALTH command.

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 or write.

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="2.23">
  <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/>
          <!--    Firmware support information for the below tag:    -->
          <!--            iLO 5 - All versions                       -->
          <!--            iLO 4 - 1.30 or later                      -->
        <GET_ALL_FIRMWARE_VERSIONS/>
      </GET_EMBEDDED_HEALTH>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**

**GET_EMBEDDED_HEALTH parameters**
This module describes the GET_EMBEDDED_HEALTH command parameters.
**GET_EMBEDDED_HEALTH return messages**
This module describes the GET_EMBEDDED_HEALTH command return messages.

# GET_EMBEDDED_HEALTH parameters

This module describes the GET_EMBEDDED_HEALTH command parameters.

None

# GET_EMBEDDED_HEALTH return messages

This module describes the GET_EMBEDDED_HEALTH command return messages.



**NOTE**

PART NUMBER (for MEMORY_DETAILS) is only returned for HPE Smart Memory.

For a sample return message, see Sample return for GET_EMBEDDED_HEALTH.

**NOTE**

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

This module describes the GET_POWER_READINGS command.

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>
```

**Subtopics**

**GET_POWER_READINGS parameters**
This module describes the GET_POWER_READINGS command parameters.
**GET_POWER_READINGS return messages**
This module describes the GET_POWER_READINGS command return messages.

# GET_POWER_READINGS parameters

This module describes the GET_POWER_READINGS command parameters.

None

# GET_POWER_READINGS return messages

This module describes the GET_POWER_READINGS command 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:

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

```
<RIBCL VERSION="2.0">
 <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 5 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 or write. 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>
```

### Subtopics


**GET_PWREG parameters**
**GET_PWREG return messages**
**GET_PWREG runtime errors**

## GET_PWREG parameters

None

## GET_PWREG return messages

A GET_PWREG return message includes:

```
<RESPONSE STATUS="0x0000" MSG="No Errors"/>
<GET_PWREG>
<PCAP MODE="OFF"></PCAP>
<EFFICIENCY_MODE>"3"</EFFICIENCY_MODE>
<PWRALERT TYPE="AVERAGE" THRESHOLD="600" DURATION="60"></PWRALERT>
<GET_HOST_POWER HOST_POWER="ON"/>
</GET_PWREG>
```

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 a supported license key.`

# SET_PWREG

The SET_PWREG command sets the power alert threshold for iLO 5 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>
```

**Subtopics**


**SET_PWREG parameters**
**SET_PWREG runtime errors**


# 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 a supported 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_PS_DATA

The GET_PS_DATA command is used to get the power supply redundancy settings that are configured in the server RBSU. For this command to parse correctly, the GET_PS_DATA command must appear within a SERVER_INFO command block.

For example:

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

**Subtopics**

**GET_PS_DATA parameters**
**GET_PS_DATA return messages**

## GET_PS_DATA parameters

None

## GET_PS_DATA return messages

The returns for this command include:

- DEV_PS_OPERATION—The minimum number of supplies recommended for server operation.
- DEV_PS_REDUNDANCY—The minimum number of supplies required for server redundancy.

> **NOTE**
> This command is not supported on blade servers and servers with enclosure-managed power supplies.

For example:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<GET_PS_DATA>
<DEV_PS_OPERATION>1</DEV_PS_OPERATION>
<DEV_PS_REDUNDANCY>2</DEV_PS_REDUNDANCY>
</GET_PS_DATA>
</RIBCL>
```

## GET_POWER_CAP

This module describes the GET_POWER_CAP command.

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. You can set the SERVER_INFO MODE to read or write. 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>
```

**Subtopics**

**GET_POWER_CAP parameters**
This module describes the GET_POWER_CAP command parameters.
**GET_POWER_CAP return messages**
This module describes the GET_POWER_CAP command return messages.

## GET_POWER_CAP parameters

This module describes the GET_POWER_CAP command parameters.

None

## GET_POWER_CAP return messages

This module describes the GET_POWER_CAP command return messages.

A cap value of zero indicates a power cap is not currently set on the server.

## SET_POWER_CAP

This module describes the SET_POWER_CAP command return messages.

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>
```

**Subtopics**

**SET_POWER_CAP parameters**
This module describes the SET_POWER_CAP command parameters.
**SET_POWER_CAP runtime errors**
This module describes the SET_POWER_CAP command runtime errors.

# SET_POWER_CAP parameters

This module describes the SET_POWER_CAP command 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

This module describes the SET_POWER_CAP command 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.`

## SET_CRITICAL_TEMP_REMAIN_OFF

The SET_CRITICAL_TEMP_REMAIN_OFF command controls the behavior of a server after shutting down due to critical temperature. 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. 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">
    <SERVER_INFO MODE="write">
      <SET_CRITICAL_TEMP_REMAIN_OFF VALUE="No"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

**Subtopics**

**SET_CRITICAL_TEMP_REMAIN_OFF parameters**
**SET_CRITICAL_TEMP_REMAIN_OFF runtime errors**

## SET_CRITICAL_TEMP_REMAIN_OFF parameters

SET_CRITICAL_TEMP_REMAIN_OFF controls the reaction of the server after a critical temperature shutdown. A value of **`No`** (the default) sets the server to automatically power on after a critical temperature shutdown. A value of **`Yes`** sets the server to remain powered off after a critical temperature shutdown.

## SET_CRITICAL_TEMP_REMAIN_OFF runtime errors

The possible SET_CRITICAL_TEMP_REMAIN_OFF 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. CONFIG_ILO_PRIV required.`

# GET_CRITICAL_TEMP_REMAIN_OFF

The GET_CRITICAL_TEMP_REMAIN_OFF command retrieves the critical temperature shutdown behavior of the server. For this command to parse correctly, the command must appear within a SERVER_INFO command block.

For example:

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

**Subtopics**

**GET_CRITICAL_TEMP_REMAIN_OFF return messages**

# GET_CRITICAL_TEMP_REMAIN_OFF return messages

Information is returned within one of the following responses:

- `<CRITICAL_TEMP_REMAIN_OFF VALUE="Yes"/>`
- `<CRITICAL_TEMP_REMAIN_OFF VALUE="No"/>`

# GET_HOST_POWER_SAVER_STATUS

This section describes the GET_HOST_POWER_SAVER_STATUS command.

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>
```

**Subtopics**


**GET_HOST_POWER_SAVER_STATUS parameters**
This module describes the GET_HOST_POWER_SAVER_STATUS parameters.
**GET_HOST_POWER_SAVER_STATUS runtime errors**
This module describes the GET_HOST_POWER_SAVER_STATUS runtime errors.
**GET_HOST_POWER_SAVER_STATUS return messages**
This module describes the GET_HOST_POWER_SAVER_STATUS return messages


## GET_HOST_POWER_SAVER_STATUS parameters

This module describes the GET_HOST_POWER_SAVER_STATUS parameters.

None

## GET_HOST_POWER_SAVER_STATUS runtime errors

This module describes the 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

This module describes the GET_HOST_POWER_SAVER_STATUS return messages

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

This module describes the SET_HOST_POWER_SAVER command.

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.

**NOTE**

If you set the HOST_POWER_SAVER parameter to **1** , you must reboot the server to enable the change.

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>
```

**Subtopics**

**SET_HOST_POWER_SAVER parameters**

**SET_HOST_POWER_SAVER runtime errors**

This module describes the GET_HOST_POWER_SAVER runtime errors

## SET_HOST_POWER_SAVER parameters

The HOST_POWER_SAVER command controls the Dynamic Power Saver feature of the server processor if this feature is supported.

The possible values are:

- **1**—Operating system control mode (Intel and AMD systems)
- **2**—HPE Static Low Power mode (Intel systems only)
- **3**—HPE Dynamic Power Savings mode (Intel systems only)
- **4**—HPE Static High Performance mode (Intel and AMD systems)

AMD support is available in iLO 5 2.40 and later.

When you use this feature, note the following:

- On AMD systems:
  - Mode changes cannot be applied when the system is in POST.
  - A reboot is required to complete any mode change.
- On Intel systems a reboot is required to complete the mode change when you:
  - Change to OS Control mode.
  - Change from OS Control mode to any other mode.

## SET_HOST_POWER_SAVER runtime errors

This module describes the GET_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. CONFIG_ILO_PRIV required.`

# GET_HOST_POWER_STATUS

This section describes the GET_HOST_POWER_STATUS command.

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>
```

**Subtopics**

**GET_HOST_POWER_STATUS parameters**
This module describes the GET_HOST_POWER_STATUS parameters.
**GET_HOST_POWER_STATUS runtime errors**
This module describes the GET_HOST_POWER_STATUS runtime errors.
**GET_HOST_POWER_STATUS Return Messages**
This module describes the GET_HOST_POWER_STATUS runtime errors.

# GET_HOST_POWER_STATUS parameters

This module describes the GET_HOST_POWER_STATUS parameters.

None

# GET_HOST_POWER_STATUS runtime errors

This module describes the 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

This module describes the GET_HOST_POWER_STATUS runtime errors.

The following information is returned within the response:

```
<GET_HOST_POWER
HOST POWER="ON"/>
```

## 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>
```

**Subtopics**

**SET_HOST_POWER Parameters**
This module describes the SET_HOST_POWER parameters.
**SET_HOST_POWER Runtime Errors**
This module describes the SET_HOST_POWER runtime errors..

# SET_HOST_POWER Parameters

This module describes the 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

This module describes the 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

This module describes the GET_HOST_PWR_MICRO_VER command.

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. You can set the 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_PWR_MICRO_VER/>
  </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**


**GET_HOST_PWR_MICRO_VER parameters**
This module describes the GET_HOST_PWR_MICRO_VER parameters.
**GET_HOST_PWR_MICRO_VER runtime errors**
This module describes the GET_HOST_PWR_MICRO_VER runtime errors.
**GET_HOST_PWR_MICRO_VER return messages**
This module describes the GET_HOST_PWR_MICRO_VER return messages.


## GET_HOST_PWR_MICRO_VER parameters

This module describes the GET_HOST_PWR_MICRO_VER parameters.

None

## GET_HOST_PWR_MICRO_VER runtime errors

This module describes the 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. The power micro is still displayed.
- `N/A`—If the server does not support a power micro.

## GET_HOST_PWR_MICRO_VER return messages

This module describes the 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

This module describes the RESET_SERVER command.

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>
```

**Subtopics**

**RESET_SERVER error messages**
This module describes the RESET_SERVER command errors.

**RESET_SERVER parameters**
This module describes the RESET_SERVER command parameters.

## RESET_SERVER error messages

This module describes the RESET_SERVER command errors.

The possible RESET_SERVER 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.`

## RESET_SERVER parameters

This module describes the RESET_SERVER command 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>
```

**Subtopics**

**PRESS_PWR_BTN parameters**
This module describes the PRESS_PWR_BTN parameters.
**PRESS_PWR_BTN runtime errors**
This module describes the PRESS_PWR_BTN runtime errors.

## PRESS_PWR_BTN parameters

This module describes the PRESS_PWR_BTN parameters.

None

## PRESS_PWR_BTN runtime errors

This module describes the 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>
```

**Subtopics**

**HOLD_PWR_BTN parameters**
This module describes the HOLD_PWR_BTN parameters.
**HOLD_PWR_BTN runtime errors**
This module describes the HOLD_PWR_BTN runtime errors.

# HOLD_PWR_BTN parameters

This module describes the 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

This module describes the 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 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>
```

**Subtopics**

**COLD_BOOT_SERVER parameters**
This module describes the COLD_BOOT_SERVER parameters.
**COLD_BOOT_SERVER runtime errors**
This module describes the COLD_BOOT_SERVER runtime errors.

# COLD_BOOT_SERVER parameters

This module describes the COLD_BOOT_SERVER parameters.

None

# COLD_BOOT_SERVER runtime errors

This module describes the 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 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>
```

**Subtopics**

**WARM_BOOT_SERVER parameters**
This module describes the WARM_BOOT_SERVER parameters.
**WARM_BOOT_SERVER runtime errors**
This module describes the WARM_BOOT_SERVER runtime errors.

# WARM_BOOT_SERVER parameters

This module describes the WARM_BOOT_SERVER parameters.

None

# WARM_BOOT_SERVER runtime errors

This module describes the 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 initiated 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.

**Subtopics**

**SERVER_AUTO_PWR parameters**

**SERVER_AUTO_PWR runtime errors**

This module describes the SERVER_AUTO_PWR runtime errors.

## 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.

  The 15, 30, 45, and 60 second delay values are not available on c-Class blade servers or Synergy compute modules. These server types are managed by external products such as OA, HPE OneView, or the Frame Link Module. iLO will attempt to power on the servers based on the configured power-on delay setting, but external factors might affect the actual startup time.
- `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

This module describes the 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

This module describes the GET_SERVER_AUTO_PWR command.

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 5 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>
```

**Subtopics**

**GET_SERVER_AUTO_PWR parameters**
This module describes the GET_SERVER_AUTO_PWR parameters.
**GET_SERVER_AUTO_PWR return message**
This module describes the GET_SERVER_AUTO_PWR return message.

## GET_SERVER_AUTO_PWR parameters

This module describes the GET_SERVER_AUTO_PWR parameters.

None

## GET_SERVER_AUTO_PWR return message

This module describes the GET_SERVER_AUTO_PWR return message.

A possible GET_SERVER_AUTO_PWR return is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.23">
<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>
```

**Subtopics**

**GET_UID_STATUS parameters**
This module describes the GET_UID_STATUS parameters.
**GET_UID_STATUS response**
This module describes the GET_UID_STATUS parameters.

# GET_UID_STATUS parameters

This module describes the GET_UID_STATUS parameters.

None

## GET_UID_STATUS response

This module describes the GET_UID_STATUS parameters.

The response will include one of the following:

```
<GET_UID_STATUS UID="OFF"/>
<GET_UID_STATUS UID="Flashing"/>
<GET_UID_STATUS UID =”ON”/>
```

## 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>
```

### Subtopics

**UID_CONTROL parameters**
This module describes the UID_CONTROL parameters.
**UID_CONTROL errors**
This module describes the UID_CONTROL errors.

## UID_CONTROL parameters

This module describes the 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

This module describes the UID_CONTROL errors.

The possible UID_CONTROL error messages include:

- `Server UID is already ON.`
- `Server UID is already OFF.`
- `Server UID status cannot be changed while UID is blinking.`

## 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>
```

**Subtopics**


**SET_PERS_MOUSE_KEYBOARD_ENABLED parameters**
**SET_PERS_MOUSE_KEYBOARD_ENABLED runtime errors**

## 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.`
- `Invalid Boolean` (Appears when a parameter value other than `Y` or `N` is used.)

## 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>
```

### Subtopics


**GET_PERS_MOUSE_KEYBOARD_ENABLED parameters**
**GET_PERS_MOUSE_KEYBOARD_ENABLED return messages**

## 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="2.23">
<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 or write.

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>
```

**Subtopics**


**GET_SERVER_POWER_ON_TIME parameters**
**GET_SERVER_POWER_ON_TIME return message**

## 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" />
```

## 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 an SSO 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>
```

### Subtopics

**GET_SSO_SETTINGS**
This module describes the GET_SSO_SETTINGS command.

**MOD_SSO_SETTINGS**
This module describes the MOD_SSO_SETTINGS command.
**SSO_SERVER**
This module describes the SSO_SERVER command.
**DELETE_SERVER**
This module describes the DELETE_SERVER command.

# GET_SSO_SETTINGS

This module describes the GET_SSO_SETTINGS command.

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>
```



**NOTE**

The information returned by GET_SSO_SETTINGS has not been enhanced to support the extended privileges available from the iLO 5 web interface. For more information about user and group privileges in iLO 5, see the HPE iLO 5 User Guide in the HPE Information Library at **http://www.hpe.com/support/ilo-docs**.

### Subtopics

**GET_SSO_SETTINGS parameters**
This module describes the GET_SSO_SETTINGS parameters.
**GET_SSO_SETTINGS return messages**

## GET_SSO_SETTINGS parameters

This module describes the 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.hpe.com"
      ISSUED_BY="viv.hpe.com"
      VALID_FROM="061108192059Z"
      VALID_UNTIL="161108192059Z">
-----BEGIN CERTIFICATE-----
.
.
.
```

```
-----END CERTIFICATE-----
</SSO_SERVER>
<SSO_SERVER INDEX="1">
ant.hpe.com
</SSO_SERVER>
</GET_SSO_SETTINGS>
```

# MOD_SSO_SETTINGS

This module describes the MOD_SSO_SETTINGS command.

The MOD_SSO_SETTINGS command is used to modify the SSO settings for iLO 5. 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.



**NOTE**

MOD_SSO_SETTINGS has not been enhanced to support the extended privileges available from the iLO 5 web interface. For more information about user and group privileges in iLO 5, see the HPE iLO 5 User Guide in the HPE Information Library at **http://www.hpe.com/support/ilo-docs**.

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" />
   </MOD_SSO_SETTINGS>
  </SSO_INFO>
 </LOGIN>
</RIBCL>
```

**Subtopics**


**MOD_SSO_SETTINGS parameters**
This module describes the MOD_SSO_SETTINGS parameters.
**MOD_SSO_SETTINGS runtime errors**
This module describes the MOD_SSO_SETTINGS runtime errors..


## MOD_SSO_SETTINGS parameters

This module describes the 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 SSO on this processor.
- `Certificate`—Accepts only SSO requests authenticated using a certificate.
- `Name`—Trusts SSO requests from the named 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 iLO User Guide on the Hewlett Packard Enterprise website at **http://www.hpe.com/support/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

This module describes the MOD_SSO_SETTINGS runtime errors..

Possible MOD_SSO_SETTINGS error messages include:

- `Incorrect firmware version. SSO is only supported on iLO 5 v1.15 firmware or later.`
- `User does not have correct privilege for action. CONFIG_ILO_PRIV required.`
- `SSO_INFO must be in write mode.`

## SSO_SERVER

This module describes the SSO_SERVER command.

The SSO_SERVER command is used to create 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 a 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 5 (the LOM processor requests the certificate from the specified SIM server using anonymous HTTP request). The iLO 5 processor must be able to contact the 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 5. However, you must obtain the x.509 certificate in advance. This method enables you to configure the iLO 5 in advance of placing it on the network with the SIM server. The method also enables you to verify the contents of the SIM server certificate. For additional methods of obtaining the certificate from the SIM server, see the iLO User Guide on the Hewlett Packard Enterprise information library at **http://www.hpe.com/support/ilo-docs** or the SIM User Guide at: **http://www.hpe.com/info/hpsim/docs**.

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>
```

**Subtopics**

**SSO_SERVER parameters**
This module describes the SSO_SERVER parameters.
**SSO_SERVER runtime errors**
This module describes the SSO_SERVER runtime errors.

# SSO_SERVER parameters

This module describes the 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 SIM Trusted Server. The name is not validated by iLO until an SSO login is attempted. For example, the syntax to add a SIM Trusted Server name:

```
<SSO_SERVER NAME="hpsim1.hp.net" />
```

IMPORT_FROM indicates that iLO must request the SIM Trusted Server certificate from 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 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 a SIM Trusted Server certificate resembles the following:

```
<SSO_SERVER>
 -----BEGIN CERTIFICATE-----
```

```
 MIIC3TCCAkYCBESzwFUwDQYJKoZIhvcNAQEFBQAwgbUxCzAJBgNVBAYTAlVTMRMwE...
 kXzhuVzPfWzQ+a2E9tGAE/YgNGTfS9vKkVLUf6QoP/RQpYpkl5BxrsN3gM/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

This module describes the SSO_SERVER runtime errors.

A runtime error is generated if the:

- Certificate is a duplicate.
- Certificate is corrupt.
- SIM server cannot be contacted using IMPORT_FROM.
- 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

This module describes the DELETE_SERVER command.

The DELETE_SERVER command is used to remove a 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. 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>
```

**Subtopics**

**DELETE_SERVER parameters**
This module describes the DELETE_SERVER parameters.
**DELETE_SERVER runtime errors**
This module describes the DELETE_SERVER runtime errors.

## DELETE_SERVER parameters

This module describes the 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

This module describes the DELETE_SERVER runtime errors.

A runtime error is generated if the index is invalid.

## Secure Shell

**Subtopics**

**SSH overview**
**Supported SSH features**
This module describes the iLO-supported SSH features.

**Using Secure Shell**
**SSH key authorization**
This module describes SSH key authorization with iLO.
**Importing SSH keys from PuTTY**
**Importing SSH keys generated using ssh-keygen**

## SSH overview

SSH is a 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 supports:

- SSH protocol version 2.
- PuTTY, a free version of the SSHprotocol, available for download on the Internet. Hewlett Packard Enterprise 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

This module describes the iLO-supported SSH features.

The library supports only version 2 (SSH-2) of the protocol. Supported SSH Features shows the SSH features supported by iLO.

**Table 1. 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 |

| Feature | Supported Algorithm |
|---|---|
| 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, enter the **`ssh -l`** command followed by the login name, and then the IP address or DNS name:

```
ssh -l loginname ipaddress/dnsname
```

### 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 sessionname
    ```

# SSH key authorization

This module describes SSH key authorization with iLO.

SSH key-based authentication enables 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. SIM can perform these tasks on multiple LOM devices nearly simultaneously, at scheduled times. SIM provides a menu-driven interface to manage and configure multiple targets. Enhancements to SIM are provided by tool definition files.

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

A 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.

**Subtopics**

**Tool definition files**
**Mxagentconfig utility**
This module describes the Mxagentconfig utility

# Tool definition files

TDEF files extend the menu system of HPE Systems Insight Manager (SIM) to provide the command line commands that SIM transmits to iLO through an SSH connection.

# `Mxagentconfig` utility

This module describes the Mxagentconfig utility

`Mxagentconfig` is a utility used to export and install 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

### About this task

The public key file format generated by PuTTY is not compatible with iLO. The following example illustrates, a PuTTY generated public key file:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1yc2EAAAABJQAAAIB0x0wVO9itQB11o+tHnY3VvmsGgwghCyLOVzJl
3A9F5yzKj+RXJVPxOGusAhmJwF8PBQ9wV5E0Rumm6gNOaPyvAMJCG/l0PW7Fhac1
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.

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.

### Procedure

1. Double-click the PuTTY Key Generator icon to launch the utility.
2. Select the type of key to generate, either SSH-2 RSA or 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.
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 Adminstration 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 IP address.
12. Select **Connection > SSH > Auth**.
13. Click **Browse**, and then locate the private key file.
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

### Prerequisites

- SSH key created using `ssh-keygen`
- `Key.pub` file created

### Procedure

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.

### Results

The key file is ready to import and authorize.

## PERL scripting

**Subtopics**

**Using PERL with the XML scripting interface**
**XML enhancements**
**Opening an SSL connection**
This module describes opening an SSL connection to use with iLO scripting.
**Sending the XML header and script body**
This module describes the required XML header and script body.

# 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.

Packages containing various and comprehensive sample scripts for Windows and Linux are available for download on the Hewlett Packard Enterprise website: **https://www.hpe.com/support/ilo5**.

# XML enhancements

If you are using a utility other than HPQLOCFG (such as PERL), the following steps help ensure that the iLO 5 firmware returns properly formatted XML. You must incorporate the following tag into the script sent to iLO 5:

```
<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 Hewlett Packard Enterprise, 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>
```

## Opening an SSL connection

This module describes opening an SSL connection to use with iLO scripting.

### About this task

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

This module describes the required XML header and script body.

### About this task

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:

**Procedure**

1. PERL scripts must send the XML header before sending the body of the script.
2. PERL scripts must provide script data fast enough to prevent the device from timing out.
3. Only one XML document is allowed per connection, which means one pair of RIBCL tags.
4. The device does not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

# iLO ports

**Subtopics**

**Enabling the Shared Network Port feature through XML scripting**
This module describes how to enable the shared network port.
**Re-enabling the dedicated NIC management port**
This module describes how to re-enable the NIC management port.

# Enabling the Shared Network Port feature through XML scripting

This module describes how to enable the shared network port.

### About this task

For information on how to use the `SHARED_NETWORK_PORT` command to enable the iLO 5 Shared Network Port through XML scripting, see RIBCL XML Scripting Language.

The following sample script configures the iLO 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

This module describes how to re-enable the NIC management port.

### About this task

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

To re-enable the dedicated management port using RBSU:

### Procedure

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 **F9** key to enter System Utilities.
4. Navigate to **System Utilities > System Configuration > iLO 5 Configuration Utility > Network options**.
5. Change the **Network Interface Adapter** to `On`.

   There are two other available choices, depending on the whether you have the add-on adapter installed. Use LOM for an embedded NIC, and use Flex LOM for the add-on adapter. The shared network port is not supported on HPE Blade or Synergy Gen10 servers.
6. Press the **F10** key to save the configuration.
7. Press one of the following keys to complete the procedure:
   - **F7** — Load Defaults
   - **F10** — Save
   - **F12** — Save and Exit

**Results**

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>
```

# Sample script and command reference

The HPE Lights-Out XML Scripting Sample bundles contain sample scripts that you can modify as needed for use in your environment. The following table lists the available sample scripts and the related command for each.

iLO sample scripts are available at Hewlett Packard Enterprise **website**.

**Table 1. Sample scripts and related commands**

| Sample script | Related Command |
|---|---|
| Abort_Directory_test.xml | ABORT_DIR_TEST |
| 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 |
| 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_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 |

| Sample script | Related Command |
|---|---|
| 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_User_Info.xml | GET_ALL_USER_INFO |
| Get_All_Users.xml | GET_ALL_USERS |
| 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_Directory_Test_Results | GET_DIR_TEST_RESULTS |
| 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_CTRO.xml | GET_CRITICAL_TEMP_REMAIN_OFF |
| Get_Host_Data.xml | GET_HOST_DATA |

| Sample script | Related Command |
|---|---|
| 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_LDAP_CA_Cert_Status.xml | GET_LDAP_CA_CERTIFICATE_STATUS |
| 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_Power_On_Time.xml | GET_SERVER_POWER_ON_TIME |
| Get_Power_Readings.xml | GET_POWER_READINGS |
| Get_PowerCap.xml | GET_POWER_CAP |
| Get_Product_Name.xml | GET_PRODUCT_NAME |
| Get_PS_Data.xml | GET_PS_DATA |
| Get_Pwreg_Alert_Threshold.xml | GET_PWREG |
| Get_Rack_Settings.xml | GET_RACK_SETTINGS |
| Get_SDCard_Status.xml | GET_SDCARD_STATUS |
| Get_Security_Msg.xml | GET_SECURITY_MSG |
| Get_Server_FQDN.xml | GET_SERVER_FQDN and GET_SMH_FQDN |
| Get_Server_Name.xml | GET_SERVER_NAME |

| Sample script | Related Command |
|---|---|
| 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_LDAP_CA_Cert.xml | IMPORT_LDAP_CA_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 |

| Sample script | Related Command |
|---|---|
| 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 |
| Send_Snmp_Test_Trap.xml | SEND_SNMP_TEST_TRAP |
| Set_AHS_Status.xml | SET_AHS_STATUS |
| Set_Asset_tag.xml | SET_ASSET_TAG |
| Set_Boot_Mode.xml | SET_PENDING_BOOT_MODE |
| Set_Brownout.xml | MOD_GLOBAL_SETTINGS |
| Set_Host_CTRO.xml | SET_CRITICAL_TEMP_REMAIN_OFF |
| 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 |

| Sample script | Related Command |
|---|---|
| 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<br>SMH_FQDN |
| Set_Server_Name.xml | SERVER_NAME |
| Set_Virtual_Power_BTN.xml | PRESS_PWR_BTN<br>COLD_BOOT_SERVER<br>WARM_BOOT_SERVER<br>HOLD_PWR_BTN |
| Set_VM_Status.xml | SET_VM_STATUS |
| Shared_Network_Port.xml | MOD_NETWORK_SETTINGS |
| Start_Directory_test.xml | START_DIR_TEST |
| UID_Control.xml | UID_CONTROL |
| Update_Firmware.xml | UPDATE_RIB_FIRMWARE |
| Update_Language.xml | UPDATE_LANG_PACK |

## Sample return for GET_EMBEDDED_HEALTH

A possible GET_EMBEDDED_HEALTH return message is:

```
<GET_EMBEDDED_HEALTH_DATA>
     <FANS>
          <FAN>
               <ZONE VALUE = "System"/>
               <LABEL VALUE = "Fan 1"/>
               <STATUS VALUE = "OK"/>
               <SPEED VALUE = "9" UNIT="Percentage"/>
```

```
        </FAN>
        <FAN>
             <ZONE VALUE = "System"/>
             <LABEL VALUE = "Fan 2"/>
             <STATUS VALUE = "OK"/>
             <SPEED VALUE = "12" UNIT="Percentage"/>
        </FAN>
        <FAN>
             <ZONE VALUE = "System"/>
             <LABEL VALUE = "Fan 3"/>
             <STATUS VALUE = "OK"/>
             <SPEED VALUE = "11" UNIT="Percentage"/>
        </FAN>
        <FAN>
             <ZONE VALUE = "System"/>
             <LABEL VALUE = "Fan 4"/>
             <STATUS VALUE = "OK"/>
             <SPEED VALUE = "11" UNIT="Percentage"/>
        </FAN>
        <FAN>
             <ZONE VALUE = "System"/>
             <LABEL VALUE = "Fan 5"/>
             <STATUS VALUE = "OK"/>
             <SPEED VALUE = "11" UNIT="Percentage"/>
        </FAN>
        <FAN>
             <ZONE VALUE = "System"/>
             <LABEL VALUE = "Fan 6"/>
             <STATUS VALUE = "OK"/>
             <SPEED VALUE = "9" UNIT="Percentage"/>
        </FAN>
   </FANS>
   <TEMPERATURE>
        <TEMP>
             <LABEL VALUE = "01-Inlet Ambient"/>
             <LOCATION VALUE = "Ambient"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "21" UNIT="Celsius"/>
             <CAUTION VALUE = "42" UNIT="Celsius"/>
             <CRITICAL VALUE = "50" 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>
        <TEMP>
            <LABEL VALUE = "04-P1 DIMM 1-6"/>
            <LOCATION VALUE = "Memory"/>
            <STATUS VALUE = "Not Installed"/>
            <CURRENTREADING VALUE = "N/A"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "05-P1 DIMM 7-12"/>
            <LOCATION VALUE = "Memory"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "30" UNIT="Celsius"/>
            <CAUTION VALUE = "89" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "06-P2 DIMM 1-6"/>
            <LOCATION VALUE = "Memory"/>
            <STATUS VALUE = "Not Installed"/>
            <CURRENTREADING VALUE = "N/A"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "07-P2 DIMM 7-12"/>
            <LOCATION VALUE = "Memory"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "28" UNIT="Celsius"/>
```

```
            <CAUTION VALUE = "89" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "08-HD Max"/>
            <LOCATION VALUE = "System"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "35" UNIT="Celsius"/>
            <CAUTION VALUE = "60" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "09-Exp Bay Drive"/>
            <LOCATION VALUE = "System"/>
            <STATUS VALUE = "Not Installed"/>
            <CURRENTREADING VALUE = "N/A"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "10-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 = "11-PS 1 Inlet"/>
            <LOCATION VALUE = "Power Supply"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "31" UNIT="Celsius"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "12-PS 2 Inlet"/>
            <LOCATION VALUE = "Power Supply"/>
            <STATUS VALUE = "Not Installed"/>
            <CURRENTREADING VALUE = "N/A"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
```

```
        <TEMP>
             <LABEL VALUE = "13-VR P1"/>
             <LOCATION VALUE = "System"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "38" UNIT="Celsius"/>
             <CAUTION VALUE = "115" UNIT="Celsius"/>
             <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
             <LABEL VALUE = "14-VR P2"/>
             <LOCATION VALUE = "System"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "35" UNIT="Celsius"/>
             <CAUTION VALUE = "115" UNIT="Celsius"/>
             <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
             <LABEL VALUE = "15-VR P1 Mem"/>
             <LOCATION VALUE = "System"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "33" UNIT="Celsius"/>
             <CAUTION VALUE = "115" UNIT="Celsius"/>
             <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
             <LABEL VALUE = "16-VR P1 Mem"/>
             <LOCATION VALUE = "System"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "33" UNIT="Celsius"/>
             <CAUTION VALUE = "115" UNIT="Celsius"/>
             <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
             <LABEL VALUE = "17-VR P2 Mem"/>
             <LOCATION VALUE = "System"/>
             <STATUS VALUE = "OK"/>
             <CURRENTREADING VALUE = "33" UNIT="Celsius"/>
             <CAUTION VALUE = "115" UNIT="Celsius"/>
             <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
             <LABEL VALUE = "18-VR P2 Mem"/>
             <LOCATION VALUE = "System"/>
```

```
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "32" UNIT="Celsius"/>
            <CAUTION VALUE = "115" UNIT="Celsius"/>
            <CRITICAL VALUE = "120" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "19-PS 1 Internal"/>
            <LOCATION VALUE = "Power Supply"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "20-PS 2 Internal"/>
            <LOCATION VALUE = "Power Supply"/>
            <STATUS VALUE = "Not Installed"/>
            <CURRENTREADING VALUE = "N/A"/>
            <CAUTION VALUE = "N/A"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "21-PCI 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 = "22-PCI 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-PCI 3"/>
            <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-PCI 4"/>
            <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-PCI 5"/>
            <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-PCI 6"/>
            <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 = "27-HD Controller"/>
            <LOCATION VALUE = "I/O Board"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "65" UNIT="Celsius"/>
            <CAUTION VALUE = "100" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "28-LOM Card"/>
            <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 = "29-LOM"/>
            <LOCATION VALUE = "System"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "40" UNIT="Celsius"/>
            <CAUTION VALUE = "100" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "30-Front Ambient"/>
            <LOCATION VALUE = "Ambient"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "29" UNIT="Celsius"/>
            <CAUTION VALUE = "65" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "31-PCI 1 Zone."/>
            <LOCATION VALUE = "I/O Board"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "30" UNIT="Celsius"/>
            <CAUTION VALUE = "70" UNIT="Celsius"/>
            <CRITICAL VALUE = "75" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "32-PCI 2 Zone."/>
            <LOCATION VALUE = "I/O Board"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "31" UNIT="Celsius"/>
            <CAUTION VALUE = "70" UNIT="Celsius"/>
            <CRITICAL VALUE = "75" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "33-PCI 3 Zone."/>
            <LOCATION VALUE = "I/O Board"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "32" UNIT="Celsius"/>
            <CAUTION VALUE = "70" UNIT="Celsius"/>
            <CRITICAL VALUE = "75" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "34-PCI 4 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 = "35-PCI 5 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 = "36-PCI 6 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 = "37-HD Cntlr Zone"/>
            <LOCATION VALUE = "I/O Board"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "47" UNIT="Celsius"/>
            <CAUTION VALUE = "75" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "38-I/O Zone"/>
            <LOCATION VALUE = "System"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "36" UNIT="Celsius"/>
            <CAUTION VALUE = "75" UNIT="Celsius"/>
            <CRITICAL VALUE = "80" UNIT="Celsius"/>
        </TEMP>
        <TEMP>
            <LABEL VALUE = "39-P/S 2 Zone"/>
            <LOCATION VALUE = "System"/>
            <STATUS VALUE = "OK"/>
            <CURRENTREADING VALUE = "33" UNIT="Celsius"/>
            <CAUTION VALUE = "70" UNIT="Celsius"/>
            <CRITICAL VALUE = "N/A"/>
```

```
          </TEMP>
          <TEMP>
               <LABEL VALUE = "40-Battery Zone"/>
               <LOCATION VALUE = "System"/>
               <STATUS VALUE = "OK"/>
               <CURRENTREADING VALUE = "34" UNIT="Celsius"/>
               <CAUTION VALUE = "75" UNIT="Celsius"/>
               <CRITICAL VALUE = "80" UNIT="Celsius"/>
          </TEMP>
          <TEMP>
               <LABEL VALUE = "41-iLO Zone"/>
               <LOCATION VALUE = "System"/>
               <STATUS VALUE = "OK"/>
               <CURRENTREADING VALUE = "37" UNIT="Celsius"/>
               <CAUTION VALUE = "90" UNIT="Celsius"/>
               <CRITICAL VALUE = "95" UNIT="Celsius"/>
          </TEMP>
          <TEMP>
               <LABEL VALUE = "42-Rear 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 = "43-Storage Batt"/>
               <LOCATION VALUE = "System"/>
               <STATUS VALUE = "OK"/>
               <CURRENTREADING VALUE = "25" UNIT="Celsius"/>
               <CAUTION VALUE = "60" UNIT="Celsius"/>
               <CRITICAL VALUE = "N/A"/>
          </TEMP>
          <TEMP>
               <LABEL VALUE = "44-Fuse"/>
               <LOCATION VALUE = "Power Supply"/>
               <STATUS VALUE = "OK"/>
               <CURRENTREADING VALUE = "31" UNIT="Celsius"/>
               <CAUTION VALUE = "100" UNIT="Celsius"/>
               <CRITICAL VALUE = "N/A"/>
          </TEMP>
     </TEMPERATURE>
     <POWER_SUPPLIES>
```

```
          <POWER_SUPPLY_SUMMARY>
               <PRESENT_POWER_READING VALUE = "83 Watts"/>
               <POWER_MANAGEMENT_CONTROLLER_FIRMWARE_VERSION VALUE =
"1.0.9"/>
               <POWER_SYSTEM_REDUNDANCY VALUE = "Not Redundant"/>
               <HP_POWER_DISCOVERY_SERVICES_REDUNDANCY_STATUS VALUE =
"N/A"/>
               <HIGH_EFFICIENCY_MODE VALUE = "Balanced"/>
          </POWER_SUPPLY_SUMMARY>
          <SUPPLY>
               <LABEL VALUE = "Power Supply 1"/>
               <PRESENT VALUE = "Yes"/>
               <STATUS VALUE = "Good, In Use"/>
               <PDS VALUE = "No"/>
               <HOTPLUG_CAPABLE VALUE = "Yes"/>
               <MODEL VALUE = "720478-B21"/>
               <SPARE VALUE = "754377-001"/>
               <SERIAL_NUMBER VALUE = "5DMVV0A4D7Z048"/>
               <CAPACITY VALUE = "500 Watts"/>
               <FIRMWARE_VERSION VALUE = "1.00"/>
          </SUPPLY>
          <SUPPLY>
               <LABEL VALUE = "Power Supply 2"/>
               <PRESENT VALUE = "No"/>
               <STATUS VALUE = "Unknown"/>
               <PDS VALUE = "Other"/>
               <HOTPLUG_CAPABLE VALUE = "Yes"/>
               <MODEL VALUE = "N/A"/>
               <SPARE VALUE = "N/A"/>
               <SERIAL_NUMBER VALUE = "N/A"/>
               <CAPACITY VALUE = "N/A"/>
               <FIRMWARE_VERSION VALUE = "N/A"/>
          </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_DISCOVERY_SERVICES_IPDU_SUMMARY>
```

```
          <SMART_STORAGE_BATTERY>
               <LABEL VALUE = "Battery 1"/>
               <PRESENT VALUE = "Yes"/>
               <STATUS VALUE = "OK"/>
               <MODEL VALUE = "727258-B21"/>
               <SPARE VALUE = "750450-001"/>
               <SERIAL_NUMBER VALUE = "6EMYC0AWY7X77Q"/>
               <CAPACITY VALUE = "96 Watts"/>
               <FIRMWARE_VERSION VALUE = "1.1"/>
          </SMART_STORAGE_BATTERY>
     </POWER_SUPPLIES>
     <VRM>
     </VRM>
     <PROCESSORS>
          <PROCESSOR>
               <LABEL VALUE = "Proc 1"/>
               <NAME VALUE = "Intel(R) Xeon(R) CPU E5-2623 v3 @ 3.00GHz"/>
               <STATUS VALUE = "OK"/>
               <SPEED VALUE = "3000 MHz"/>
               <EXECUTION_TECHNOLOGY VALUE = "4/4 cores; 8 threads"/>
               <MEMORY_TECHNOLOGY VALUE = "64-bit Capable"/>
               <INTERNAL_L1_CACHE VALUE = "256 KB"/>
               <INTERNAL_L2_CACHE VALUE = "1024 KB"/>
               <INTERNAL_L3_CACHE VALUE = "10240 KB"/>
          </PROCESSOR>
          <PROCESSOR>
               <LABEL VALUE = "Proc 2"/>
               <NAME VALUE = "Intel(R) Xeon(R) CPU E5-2623 v3 @ 3.00GHz"/>
               <STATUS VALUE = "OK"/>
               <SPEED VALUE = "3000 MHz"/>
               <EXECUTION_TECHNOLOGY VALUE = "4/4 cores; 8 threads"/>
               <MEMORY_TECHNOLOGY VALUE = "64-bit Capable"/>
               <INTERNAL_L1_CACHE VALUE = "256 KB"/>
               <INTERNAL_L2_CACHE VALUE = "1024 KB"/>
               <INTERNAL_L3_CACHE VALUE = "10240 KB"/>
          </PROCESSOR>
     </PROCESSORS>
     <MEMORY>
          <ADVANCED_MEMORY_PROTECTION>
               <AMP_MODE_STATUS VALUE = "Advanced ECC"/>
               <CONFIGURED_AMP_MODE VALUE = "Advanced ECC"/>
               <AVAILABLE_AMP_MODES VALUE = "Advanced ECC, Online Spare
(Rank Sparing), Intrasocket Mirroring"/>
```

```
          </ADVANCED_MEMORY_PROTECTION>
          <MEMORY_DETAILS_SUMMARY>
               <CPU_1>
                    <NUMBER_OF_SOCKETS VALUE = "12"/>
                    <TOTAL_MEMORY_SIZE VALUE = "16 GB"/>
                    <OPERATING_FREQUENCY VALUE = "1866 MHz"/>
                    <OPERATING_VOLTAGE VALUE = "1.20 v"/>
               </CPU_1>
               <CPU_2>
                    <NUMBER_OF_SOCKETS VALUE = "12"/>
                    <TOTAL_MEMORY_SIZE VALUE = "16 GB"/>
                    <OPERATING_FREQUENCY VALUE = "1866 MHz"/>
                    <OPERATING_VOLTAGE VALUE = "1.20 v"/>
               </CPU_2>
          </MEMORY_DETAILS_SUMMARY>
          <MEMORY_DETAILS>
               <CPU_1>
                    <SOCKET VALUE = "1"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "2"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "3"/>
                    <STATUS VALUE = "Not Present"/>
```

```
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "4"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "5"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "6"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
```

```
                <TECHNOLOGY VALUE = "N/A"/>
            </CPU_1>
            <CPU_1>
                <SOCKET VALUE = "7"/>
                <STATUS VALUE = "Not Present"/>
                <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                <PART NUMBER = "N/A"/>
                <TYPE VALUE = "N/A"/>
                <SIZE VALUE = "N/A"/>
                <FREQUENCY VALUE = "N/A"/>
                <MINIMUM_VOLTAGE VALUE = "N/A"/>
                <RANKS VALUE = "N/A"/>
                <TECHNOLOGY VALUE = "N/A"/>
            </CPU_1>
            <CPU_1>
                <SOCKET VALUE = "8"/>
                <STATUS VALUE = "Not Present"/>
                <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                <PART NUMBER = "N/A"/>
                <TYPE VALUE = "N/A"/>
                <SIZE VALUE = "N/A"/>
                <FREQUENCY VALUE = "N/A"/>
                <MINIMUM_VOLTAGE VALUE = "N/A"/>
                <RANKS VALUE = "N/A"/>
                <TECHNOLOGY VALUE = "N/A"/>
            </CPU_1>
            <CPU_1>
                <SOCKET VALUE = "9"/>
                <STATUS VALUE = "Good, In Use"/>
                <HP_SMART_MEMORY VALUE = "Yes" Type = "Smart"/>
                <PART NUMBER = "762200-081"/>
                <TYPE VALUE = "DIMM DDR4"/>
                <SIZE VALUE = "8192 MB"/>
                <FREQUENCY VALUE = "2133 MHz"/>
                <MINIMUM_VOLTAGE VALUE = "1.20 v"/>
                <RANKS VALUE = "2"/>
                <TECHNOLOGY VALUE = "RDIMM"/>
            </CPU_1>
            <CPU_1>
                <SOCKET VALUE = "10"/>
                <STATUS VALUE = "Not Present"/>
                <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                <PART NUMBER = "N/A"/>
```

```
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "11"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_1>
               <CPU_1>
                    <SOCKET VALUE = "12"/>
                    <STATUS VALUE = "Good, In Use"/>
                    <HP_SMART_MEMORY VALUE = "Yes" Type = "Smart"/>
                    <PART NUMBER = "762200-081"/>
                    <TYPE VALUE = "DIMM DDR4"/>
                    <SIZE VALUE = "8192 MB"/>
                    <FREQUENCY VALUE = "2133 MHz"/>
                    <MINIMUM_VOLTAGE VALUE = "1.20 v"/>
                    <RANKS VALUE = "2"/>
                    <TECHNOLOGY VALUE = "RDIMM"/>
               </CPU_1>
               <CPU_2>
                    <SOCKET VALUE = "1"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_2>
```

```
            <CPU_2>
                 <SOCKET VALUE = "2"/>
                 <STATUS VALUE = "Not Present"/>
                 <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                 <PART NUMBER = "N/A"/>
                 <TYPE VALUE = "N/A"/>
                 <SIZE VALUE = "N/A"/>
                 <FREQUENCY VALUE = "N/A"/>
                 <MINIMUM_VOLTAGE VALUE = "N/A"/>
                 <RANKS VALUE = "N/A"/>
                 <TECHNOLOGY VALUE = "N/A"/>
            </CPU_2>
            <CPU_2>
                 <SOCKET VALUE = "3"/>
                 <STATUS VALUE = "Not Present"/>
                 <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                 <PART NUMBER = "N/A"/>
                 <TYPE VALUE = "N/A"/>
                 <SIZE VALUE = "N/A"/>
                 <FREQUENCY VALUE = "N/A"/>
                 <MINIMUM_VOLTAGE VALUE = "N/A"/>
                 <RANKS VALUE = "N/A"/>
                 <TECHNOLOGY VALUE = "N/A"/>
            </CPU_2>
            <CPU_2>
                 <SOCKET VALUE = "4"/>
                 <STATUS VALUE = "Not Present"/>
                 <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                 <PART NUMBER = "N/A"/>
                 <TYPE VALUE = "N/A"/>
                 <SIZE VALUE = "N/A"/>
                 <FREQUENCY VALUE = "N/A"/>
                 <MINIMUM_VOLTAGE VALUE = "N/A"/>
                 <RANKS VALUE = "N/A"/>
                 <TECHNOLOGY VALUE = "N/A"/>
            </CPU_2>
            <CPU_2>
                 <SOCKET VALUE = "5"/>
                 <STATUS VALUE = "Not Present"/>
                 <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                 <PART NUMBER = "N/A"/>
                 <TYPE VALUE = "N/A"/>
                 <SIZE VALUE = "N/A"/>
```

```
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_2>
               <CPU_2>
                    <SOCKET VALUE = "6"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_2>
               <CPU_2>
                    <SOCKET VALUE = "7"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_2>
               <CPU_2>
                    <SOCKET VALUE = "8"/>
                    <STATUS VALUE = "Not Present"/>
                    <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                    <PART NUMBER = "N/A"/>
                    <TYPE VALUE = "N/A"/>
                    <SIZE VALUE = "N/A"/>
                    <FREQUENCY VALUE = "N/A"/>
                    <MINIMUM_VOLTAGE VALUE = "N/A"/>
                    <RANKS VALUE = "N/A"/>
                    <TECHNOLOGY VALUE = "N/A"/>
               </CPU_2>
               <CPU_2>
                    <SOCKET VALUE = "9"/>
```

```
                <STATUS VALUE = "Good, In Use"/>
                <HP_SMART_MEMORY VALUE = "Yes" Type = "Smart"/>
                <PART NUMBER = "762200-081"/>
                <TYPE VALUE = "DIMM DDR4"/>
                <SIZE VALUE = "8192 MB"/>
                <FREQUENCY VALUE = "2133 MHz"/>
                <MINIMUM_VOLTAGE VALUE = "1.20 v"/>
                <RANKS VALUE = "2"/>
                <TECHNOLOGY VALUE = "RDIMM"/>
            </CPU_2>
            <CPU_2>
                <SOCKET VALUE = "10"/>
                <STATUS VALUE = "Not Present"/>
                <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                <PART NUMBER = "N/A"/>
                <TYPE VALUE = "N/A"/>
                <SIZE VALUE = "N/A"/>
                <FREQUENCY VALUE = "N/A"/>
                <MINIMUM_VOLTAGE VALUE = "N/A"/>
                <RANKS VALUE = "N/A"/>
                <TECHNOLOGY VALUE = "N/A"/>
            </CPU_2>
            <CPU_2>
                <SOCKET VALUE = "11"/>
                <STATUS VALUE = "Not Present"/>
                <HP_SMART_MEMORY VALUE = "N/A" Type = "Unknown"/>
                <PART NUMBER = "N/A"/>
                <TYPE VALUE = "N/A"/>
                <SIZE VALUE = "N/A"/>
                <FREQUENCY VALUE = "N/A"/>
                <MINIMUM_VOLTAGE VALUE = "N/A"/>
                <RANKS VALUE = "N/A"/>
                <TECHNOLOGY VALUE = "N/A"/>
            </CPU_2>
            <CPU_2>
                <SOCKET VALUE = "12"/>
                <STATUS VALUE = "Good, In Use"/>
                <HP_SMART_MEMORY VALUE = "Yes" Type = "Smart"/>
                <PART NUMBER = "762200-081"/>
                <TYPE VALUE = "DIMM DDR4"/>
                <SIZE VALUE = "8192 MB"/>
                <FREQUENCY VALUE = "2133 MHz"/>
                <MINIMUM_VOLTAGE VALUE = "1.20 v"/>
```

```
                    <RANKS VALUE = "2"/>
                    <TECHNOLOGY VALUE = "RDIMM"/>
               </CPU_2>
          </MEMORY_DETAILS>
     </MEMORY>
     <NIC_INFORMATION>
          <iLO>
               <NETWORK_PORT VALUE = "iLO Dedicated Network Port"/>
               <PORT_DESCRIPTION VALUE = "iLO Dedicated Network Port"/>
               <LOCATION VALUE = "Embedded"/>
               <MAC_ADDRESS VALUE = "38:63:bb:3a:27:10"/>
               <IP_ADDRESS VALUE = "15.154.127.140"/>
               <STATUS VALUE = "OK"/>
          </iLO>
          <NIC>
               <NETWORK_PORT VALUE = "Port 1"/>
               <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 331i
Adapter"/>
               <LOCATION VALUE = "Embedded"/>
               <MAC_ADDRESS VALUE = "38:63:bb:40:56:48"/>
               <IP_ADDRESS VALUE = "N/A"/>
               <STATUS VALUE = "Unknown"/>
          </NIC>
          <NIC>
               <NETWORK_PORT VALUE = "Port 2"/>
               <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 331i
Adapter"/>
               <LOCATION VALUE = "Embedded"/>
               <MAC_ADDRESS VALUE = "38:63:bb:40:56:49"/>
               <IP_ADDRESS VALUE = "N/A"/>
               <STATUS VALUE = "Unknown"/>
          </NIC>
          <NIC>
               <NETWORK_PORT VALUE = "Port 3"/>
               <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 331i
Adapter"/>
               <LOCATION VALUE = "Embedded"/>
               <MAC_ADDRESS VALUE = "38:63:bb:40:56:4a"/>
               <IP_ADDRESS VALUE = "N/A"/>
               <STATUS VALUE = "Unknown"/>
          </NIC>
          <NIC>
               <NETWORK_PORT VALUE = "Port 4"/>
```

```
                <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 331i
Adapter"/>
                <LOCATION VALUE = "Embedded"/>
                <MAC_ADDRESS VALUE = "38:63:bb:40:56:4b"/>
                <IP_ADDRESS VALUE = "N/A"/>
                <STATUS VALUE = "Unknown"/>
           </NIC>
           <NIC>
                <NETWORK_PORT VALUE = "Port 1"/>
                <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 366FLR
Adapter #3"/>
                <LOCATION VALUE = "Embedded"/>
                <MAC_ADDRESS VALUE = "8c:dc:d4:af:1c:ec"/>
                <IP_ADDRESS VALUE = "15.154.127.139"/>
                <STATUS VALUE = "OK"/>
           </NIC>
           <NIC>
                <NETWORK_PORT VALUE = "Port 2"/>
                <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 366FLR
Adapter #3"/>
                <LOCATION VALUE = "Embedded"/>
                <MAC_ADDRESS VALUE = "8c:dc:d4:af:1c:ed"/>
                <IP_ADDRESS VALUE = "N/A"/>
                <STATUS VALUE = "Unknown"/>
           </NIC>
           <NIC>
                <NETWORK_PORT VALUE = "Port 3"/>
                <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 366FLR
Adapter #3"/>
                <LOCATION VALUE = "Embedded"/>
                <MAC_ADDRESS VALUE = "8c:dc:d4:af:1c:ee"/>
                <IP_ADDRESS VALUE = "N/A"/>
                <STATUS VALUE = "Unknown"/>
           </NIC>
           <NIC>
                <NETWORK_PORT VALUE = "Port 4"/>
                <PORT_DESCRIPTION VALUE = "HP Ethernet 1Gb 4-port 366FLR
Adapter #3"/>
                <LOCATION VALUE = "Embedded"/>
                <MAC_ADDRESS VALUE = "8c:dc:d4:af:1c:ef"/>
                <IP_ADDRESS VALUE = "N/A"/>
                <STATUS VALUE = "Unknown"/>
           </NIC>
```

```
    </NIC_INFORMATION>
    <STORAGE>
        <CONTROLLER>
            <LABEL VALUE = "Controller on System Board"/>
            <STATUS VALUE = "OK"/>
            <CONTROLLER_STATUS VALUE = "OK"/>
            <SERIAL_NUMBER VALUE = "PDNLH0BRH8A25C"/>
            <MODEL VALUE = "Smart Array P440ar Controller"/>
            <FW_VERSION VALUE = "3.52"/>
            <CACHE_MODULE_STATUS VALUE = "OK"/>
            <CACHE_MODULE_SERIAL_NUM VALUE = "PDNLH0BRH8A25C"/>
            <CACHE_MODULE_MEMORY VALUE = "2097152 KB"/>
            <ENCRYPTION_STATUS VALUE = "Not Enabled"/>
            <ENCRYPTION_SELF_TEST_STATUS VALUE = "OK"/>
            <ENCRYPTION_CSP_STATUS VALUE = "OK"/>
            <DRIVE_ENCLOSURE>
                <LABEL VALUE = "Port 1I Box 3"/>
                <STATUS VALUE = "OK"/>
                <DRIVE_BAY VALUE = "04"/>
            </DRIVE_ENCLOSURE>
            <DRIVE_ENCLOSURE>
                <LABEL VALUE = "Port 2I Box 0"/>
                <STATUS VALUE = "OK"/>
                <DRIVE_BAY VALUE = "04"/>
            </DRIVE_ENCLOSURE>
            <LOGICAL_DRIVE>
                <LABEL VALUE = "01"/>
                <STATUS VALUE = "OK"/>
                <CAPACITY VALUE = "231 GiB"/>
                <FAULT_TOLERANCE VALUE = "RAID 0"/>
                <LOGICAL_DRIVE_TYPE VALUE = "Data LUN"/>
                <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 2"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EGT20000C5236EYR"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB”/>
                    <LOCATION VALUE = "Port 1I Box 3 Bay 2"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
```

```
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
               <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 1"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EJE30000C523FA8T"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB"/>
                    <LOCATION VALUE = "Port 1I Box 3 Bay 1"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
          </LOGICAL_DRIVE>
          <LOGICAL_DRIVE>
               <LABEL VALUE = "02"/>
               <STATUS VALUE = "OK"/>
               <CAPACITY VALUE = "231 GiB"/>
               <FAULT_TOLERANCE VALUE = "RAID 0"/>
               <LOGICAL_DRIVE_TYPE VALUE = "Data LUN"/>
               <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
               <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 2"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EGT20000C5236EYR"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB"/>
                    <LOCATION VALUE = "Port 1I Box 3 Bay 2"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
               <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 1"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EJE30000C523FA8T"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB"/>
```

```
                    <LOCATION VALUE = "Port 1I Box 3 Bay 1"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
          </LOGICAL_DRIVE>
          <LOGICAL_DRIVE>
               <LABEL VALUE = "03"/>
               <STATUS VALUE = "OK"/>
               <CAPACITY VALUE = "231 GiB"/>
               <FAULT_TOLERANCE VALUE = "RAID 0"/>
               <LOGICAL_DRIVE_TYPE VALUE = "Data LUN"/>
               <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
               <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 2"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EGT20000C5236EYR"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB"/>
                    <LOCATION VALUE = "Port 1I Box 3 Bay 2"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
               <PHYSICAL_DRIVE>
                    <LABEL VALUE = "Port 1I Box 3 Bay 1"/>
                    <STATUS VALUE = "OK"/>
                    <SERIAL_NUMBER VALUE = "9XF3EJE30000C523FA8T"/>
                    <MODEL VALUE = "MM0500FBFVQ"/>
                    <CAPACITY VALUE = "465 GiB"/>
                    <MARKETING_CAPACITY VALUE = "341 GB"/>
                    <LOCATION VALUE = "Port 1I Box 3 Bay 1"/>
                    <FW_VERSION VALUE = "HPD8"/>
                    <DRIVE_CONFIGURATION VALUE = "Configured"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <MEDIA_TYPE VALUE = "HDD"/>
               </PHYSICAL_DRIVE>
          </LOGICAL_DRIVE>
          <LOGICAL_DRIVE>
               <LABEL VALUE = "04"/>
```

```
                    <STATUS VALUE = "OK"/>
                    <CAPACITY VALUE = "231 GiB"/>
                    <FAULT_TOLERANCE VALUE = "RAID 0"/>
                    <LOGICAL_DRIVE_TYPE VALUE = "Data LUN"/>
                    <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                    <PHYSICAL_DRIVE>
                         <LABEL VALUE = "Port 1I Box 3 Bay 2"/>
                         <STATUS VALUE = "OK"/>
                         <SERIAL_NUMBER VALUE = "9XF3EGT20000C5236EYR"/>
                         <MODEL VALUE = "MM0500FBFVQ"/>
                         <CAPACITY VALUE = "465 GiB"/>
                         <MARKETING_CAPACITY VALUE = "341 GB"/>
                         <LOCATION VALUE = "Port 1I Box 3 Bay 2"/>
                         <FW_VERSION VALUE = "HPD8"/>
                         <DRIVE_CONFIGURATION VALUE = "Configured"/>
                         <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                         <MEDIA_TYPE VALUE = "HDD"/>
                    </PHYSICAL_DRIVE>
                    <PHYSICAL_DRIVE>
                         <LABEL VALUE = "Port 1I Box 3 Bay 1"/>
                         <STATUS VALUE = "OK"/>
                         <SERIAL_NUMBER VALUE = "9XF3EJE30000C523FA8T"/>
                         <MODEL VALUE = "MM0500FBFVQ"/>
                         <CAPACITY VALUE = "465 GiB"/>
                         <MARKETING_CAPACITY VALUE = "341 GB"/>
                         <LOCATION VALUE = "Port 1I Box 3 Bay 1"/>
                         <FW_VERSION VALUE = "HPD8"/>
                         <DRIVE_CONFIGURATION VALUE = "Configured"/>
                         <ENCRYPTION_STATUS VALUE = "Not Encrypted"/>
                         <MEDIA_TYPE VALUE = "HDD"/>
                    </PHYSICAL_DRIVE>
               </LOGICAL_DRIVE>
          </CONTROLLER>
          <DISCOVERY_STATUS>
               <STATUS VALUE = "Discovery Complete"/>
          </DISCOVERY_STATUS>
     </STORAGE>
     <FIRMWARE_INFORMATION>
          <INDEX_1>
               <FIRMWARE_NAME VALUE = "iLO"/>
               <FIRMWARE_VERSION VALUE = "2.40 pass 30 Dec 02 2015"/>
          </INDEX_1>
          <INDEX_2>
```

```
                <FIRMWARE_NAME VALUE = "System ROM"/>
                <FIRMWARE_VERSION VALUE = "P89 v2.00 (10/10/2015)"/>
           </INDEX_2>
           <INDEX_3>
                <FIRMWARE_NAME VALUE = "Redundant System ROM"/>
                <FIRMWARE_VERSION VALUE = "P89 v2.00 (07/09/2015)"/>
           </INDEX_3>
           <INDEX_4>
                <FIRMWARE_NAME VALUE = "Intelligent Provisioning"/>
                <FIRMWARE_VERSION VALUE = "2.01.29"/>
           </INDEX_4>
           <INDEX_5>
                <FIRMWARE_NAME VALUE = "Intelligent Platform Abstraction
Data"/>
                <FIRMWARE_VERSION VALUE = "20.1"/>
           </INDEX_5>
           <INDEX_6>
                <FIRMWARE_NAME VALUE = "Power Management Controller
Firmware"/>
                <FIRMWARE_VERSION VALUE = "1.0.9"/>
                <FIRMWARE_FAMILY VALUE = "14h"/>
           </INDEX_6>
           <INDEX_7>
                <FIRMWARE_NAME VALUE = "Power Management Controller FW
Bootloader"/>
                <FIRMWARE_VERSION VALUE = "1.0"/>
           </INDEX_7>
           <INDEX_8>
                <FIRMWARE_NAME VALUE = "System Programmable Logic Device"/>
                <FIRMWARE_VERSION VALUE = "Version 0x33"/>
           </INDEX_8>
           <INDEX_9>
                <FIRMWARE_NAME VALUE = "SAS Programmable Logic Device"/>
                <FIRMWARE_VERSION VALUE = "Version 0x01"/>
           </INDEX_9>
           <INDEX_10>
                <FIRMWARE_NAME VALUE = "Server Platform Services (SPS)
Firmware"/>
                <FIRMWARE_VERSION VALUE = "3.0.6.267.1"/>
           </INDEX_10>
           <INDEX_11>
                <FIRMWARE_NAME VALUE = "HPE Smart Storage Battery 1
Firmware"/>
```

```
                <FIRMWARE_VERSION VALUE = "1.1"/>
          </INDEX_11>
          <INDEX_12>
                <FIRMWARE_NAME VALUE = "TPM Firmware"/>
                <FIRMWARE_VERSION VALUE = "3.17"/>
          </INDEX_12>
          <INDEX_13>
                <FIRMWARE_NAME VALUE = "Smart Array P440ar Controller"/>
                <FIRMWARE_VERSION VALUE = "3.52"/>
          </INDEX_13>
          <INDEX_14>
                <FIRMWARE_NAME VALUE = "HP Ethernet 1Gb 4-port 331i
Adapter"/>
                <FIRMWARE_VERSION VALUE = "1.38.0"/>
          </INDEX_14>
          <INDEX_15>
                <FIRMWARE_NAME VALUE = "HP Ethernet 1Gb 4-port 366FLR
Adapter #3"/>
                <FIRMWARE_VERSION VALUE = "1.1200.0"/>
          </INDEX_15>
     </FIRMWARE_INFORMATION>
     <HEALTH_AT_A_GLANCE>
          <BIOS_HARDWARE STATUS= "OK"/>
          <FANS STATUS= "OK"/>
          <FANS REDUNDANCY= "Redundant"/>
          <TEMPERATURE STATUS= "OK"/>
          <POWER_SUPPLIES STATUS= "OK"/>
          <POWER_SUPPLIES REDUNDANCY= "Not Redundant"/>
          <BATTERY STATUS= "OK"/>
          <PROCESSOR STATUS= "OK"/>
          <MEMORY STATUS= "OK"/>
          <NETWORK STATUS= "OK"/>
          <STORAGE STATUS= "OK"/>
     </HEALTH_AT_A_GLANCE>
</GET_EMBEDDED_HEALTH_DATA>
```

## Websites

**iLO**

**https://www.hpe.com/info/ilo**

**iLO 5 documentation**

**https://www.hpe.com/support/ilo-docs**

**iLO helpful links and resources**

**https://www.hpe.com/support/ilo-resource-ref-en**

**HPE iLO Free Online Training**

**https://www.hpe.com/ww/iloBundle**

**HPE ProLiant Gen10 servers**

**https://www.hpe.com/info/proliantgen10-docs**

**HPE ProLiant Gen10 Plus servers**

**https://www.hpe.com/info/proliantgen10plus-docs**

**HPE ProLiant training**

**https://www.hpe.com/ww/learnproliant**

**UEFI System Utilities**

**https://www.hpe.com/info/ProLiantUEFI/docs**

**SUM**

**https://www.hpe.com/info/sum-docs**

**SPP**

**https://www.hpe.com/info/spp/documentation**

**Intelligent Provisioning**

**https://www.hpe.com/info/intelligentprovisioning/docs**

**iLO RESTful API and RESTful Interface Tool**

**https://www.hpe.com/support/restfulinterface/docs**

**Remote Support**

**https://www.hpe.com/info/insightremotesupport/docs**

**HPE InfoSight for Servers**

**https://www.hpe.com/servers/infosight**

**iLO Amplifier Pack**

**https://www.hpe.com/servers/iloamplifierpack**

**HPE OneView**

**https://www.hpe.com/info/oneview/docs**

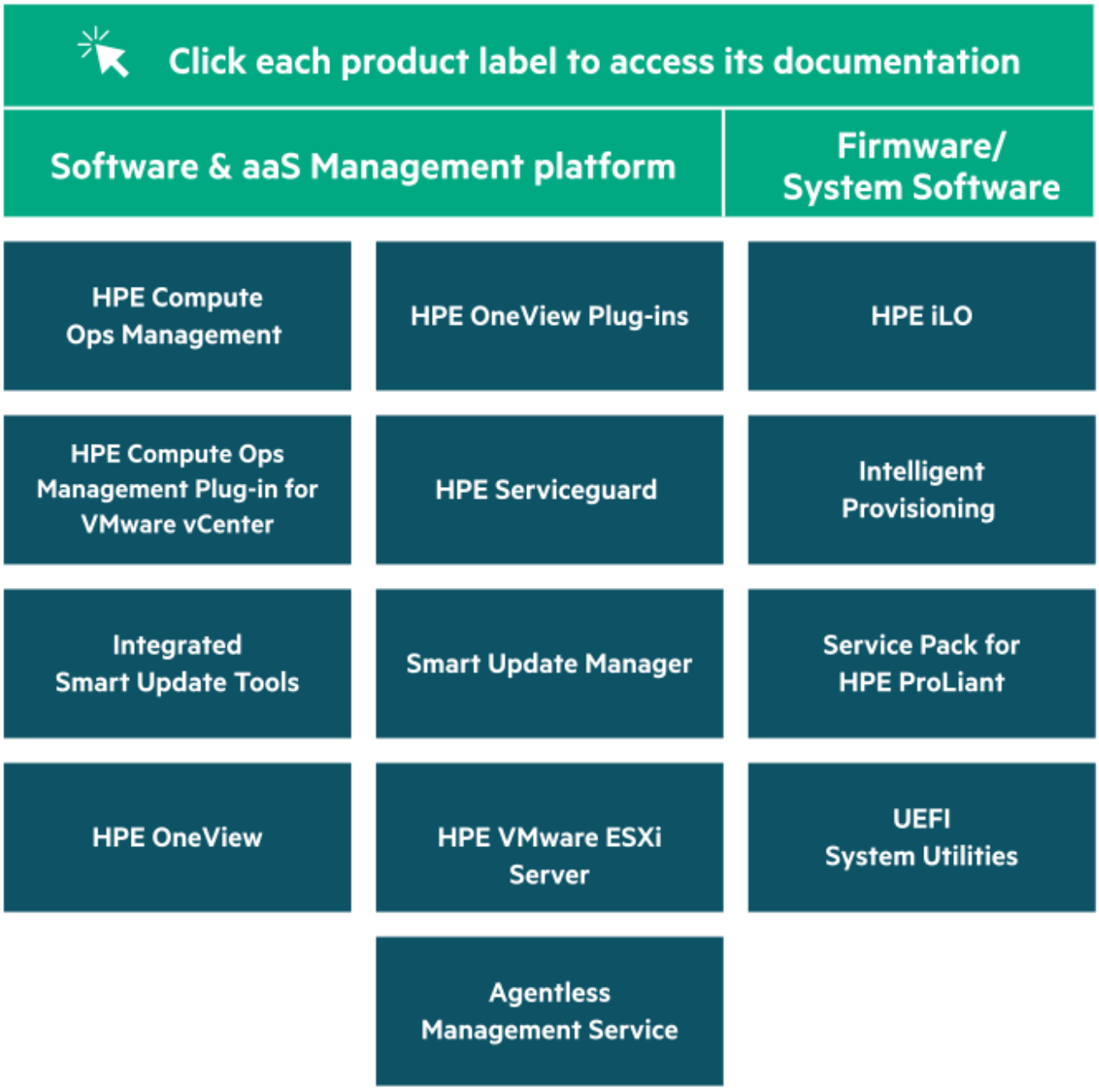
**HPE SIM**

**https://www.hpe.com/info/insightmanagement/sim/docs**

## HPE Compute Software and Firmware Product Documentation Quick Links

This infographic provides quick links for documentation for the listed HPE products. It offers easy access to documentation that helps you to understand, implement, and troubleshoot your products.

Each product-specific section lists the current version, the earlier two major versions, and their revisions.




**Navigating the Hewlett Packard Enterprise Support Center**

- **Navigation and workspace**
- **Search and product knowledge**

**Subtopics**

**HPE iLO Documentation Quick Links**

## HPE iLO Documentation Quick Links

For a comprehensive list of all the documents for HPE iLO, see **https://www.hpe.com/support/hpeilodocs-quicklinks**.

## Support and other resources

**Subtopics**

**Accessing Hewlett Packard Enterprise Support**
**HPE product registration**
**Accessing updates**
**Remote support**
**Warranty information**
**Regulatory information**
**Documentation feedback**

## Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  **https://www.hpe.com/info/assistance**

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  **https://www.hpe.com/support/hpesc**

**Information to collect**

- Technical support registration number (if applicable)
- Product name, model or version, and serial number

- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

## HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see **https://www.hpe.com/info/add-products-contracts**.

## Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  **Hewlett Packard Enterprise Support Center**

  **https://www.hpe.com/support/hpesc**

  **My HPE Software Center**

  **https://www.hpe.com/software/hpesoftwarecenter**

- To subscribe to eNewsletters and alerts:

  **https://www.hpe.com/support/e-updates**

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  **https://www.hpe.com/support/AccessToSupportMaterials**

> **IMPORTANT**
>
> Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Account set up with relevant entitlements.

## Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

**HPE Get Connected**

**https://www.hpe.com/services/getconnected**

**HPE Tech Care Service**

**https://www.hpe.com/services/techcare**

**HPE Complete Care Service**

**https://www.hpe.com/services/completecare**

## Warranty information

To view the warranty information for your product, see the **warranty check tool**.

# Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

**https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts**

### Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

**https://www.hpe.com/info/reach**

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

**https://www.hpe.com/info/ecodata**

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

**https://www.hpe.com/info/environment**

# Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the **Feedback** button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.