



**Hewlett Packard
Enterprise**

HPE iLO 4 User Guide

Abstract

This guide provides information about configuring, updating, and operating HPE ProLiant Gen8 and Gen9 servers and HPE Synergy compute modules by using the HPE iLO 4 firmware. This document is intended for system administrators, Hewlett Packard Enterprise representatives, and Hewlett Packard Enterprise Authorized Channel Partners who are involved in configuring and using Hewlett Packard Enterprise servers that include iLO 4.

Part Number: 684918-404

Published: October 2016

Edition: 1

© Copyright 2012, 2016 Hewlett Packard Enterprise Development LP

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

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

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

Acknowledgements

© 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc.

© 2012 Google Inc. All rights reserved. Chrome is a trademark of Google Inc.

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

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

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

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

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

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

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

Revision History

Revision 2.50

October 2016

Updated for iLO 4 2.50

Contents

1	Introduction.....	19
	iLO overview.....	19
	iLO key features.....	19
	iLO web interface.....	19
	ROM-based configuration utilities.....	21
	iLO mobile app.....	21
	iLO scripting and command line.....	21
	iLO RESTful API.....	21
2	Setting up iLO.....	23
	Preparing to set up iLO.....	23
	iLO network connection options.....	23
	NIC teaming with Shared Network Port configurations.....	24
	iLO IP address acquisition.....	25
	iLO access security.....	25
	iLO configuration tools.....	26
	Initial setup steps: Process overview.....	27
	Connecting iLO to the network.....	27
	Setting up iLO by using the ROM-based setup utilities.....	27
	Accessing the ROM-based setup utilities.....	27
	Configuring a static IP address with the ROM-based setup utilities.....	27
	Configuring a static IP address (iLO RBSU).....	27
	Configuring a static IP address (iLO 4 Configuration Utility).....	28
	Managing local user accounts with the ROM-based setup utilities.....	29
	Adding user accounts (iLO RBSU).....	29
	Editing user accounts (iLO RBSU).....	29
	Removing user accounts (iLO RBSU).....	30
	Adding user accounts (iLO 4 Configuration Utility).....	30
	Editing or removing user accounts (iLO 4 Configuration Utility).....	31
	iLO setup with the web interface.....	31
	Logging in to iLO for the first time.....	31
	iLO default credentials.....	32
	iLO licensed features.....	32
	iLO drivers and utilities.....	32
	Microsoft driver support.....	32
	Linux driver and utility support.....	33
	VMware driver support.....	33
	Installing the iLO drivers and utilities.....	33
	Obtaining the iLO drivers and utilities.....	33
	Driver and utility installation with the SPP.....	34
	Loading hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux.....	34
	Removing hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux.....	34
	Installing hp-health for Ubuntu.....	34
	Removing hp-health for Ubuntu.....	34
3	Updating iLO firmware, language, and licensing.....	35
	Firmware updates.....	35
	Online firmware update methods.....	35
	Offline firmware update methods.....	36
	Supported firmware types.....	36
	Obtaining the iLO firmware image file.....	36
	Obtaining supported server firmware image files.....	37
	Server firmware file type details.....	37

Updating iLO or server firmware by using the iLO web interface.....	37
Requirements for firmware update to take effect.....	38
Language packs.....	38
Installing language packs.....	39
Selecting a language pack.....	40
Configuring the default language settings.....	41
Configuring the current browser session language.....	41
Uninstalling a language pack.....	41
How iLO determines the session language.....	41
iLO licensing.....	42
License key information.....	42
Installing a license key by using a browser.....	42
Viewing license information.....	43
License details.....	43
4 Managing user accounts and directory groups.....	44
iLO user accounts.....	44
Local user accounts.....	44
Viewing local user accounts.....	44
iLO user privileges.....	44
Adding local user accounts.....	45
Editing local user accounts.....	45
Deleting a user account.....	46
User account options.....	46
Password guidelines.....	46
IPMI/DCMI users.....	47
Directory groups.....	47
Viewing directory groups.....	47
Directory group privileges.....	48
Adding directory groups.....	48
Editing directory groups.....	49
Directory group settings.....	49
Deleting a directory group.....	50
5 Configuring iLO Federation.....	51
iLO Federation settings.....	51
Prerequisites for using the iLO Federation features.....	51
iLO Federation network requirements.....	51
Configuring the multicast options for one iLO system at a time.....	52
Multicast options.....	52
iLO Federation groups.....	53
iLO Federation group characteristics.....	53
iLO Federation group memberships for local iLO systems.....	53
iLO Federation group memberships for a set of iLO systems.....	54
iLO Federation group privileges.....	54
Managing iLO Federation group memberships (local iLO system).....	54
Viewing iLO Federation group memberships (local iLO system).....	54
Adding iLO Federation group memberships (local iLO system).....	55
Editing iLO Federation group memberships (local iLO system).....	56
Removing a local iLO system from an iLO Federation group.....	56
Adding iLO Federation group memberships (multiple iLO systems).....	56
Adding an iLO Federation group based on an existing group.....	56
Creating a group from a filtered set of servers.....	57
Servers affected by a group membership change.....	59
Configuring Enclosure iLO Federation Support.....	59
Verifying server blade support for iLO Federation.....	60

6 Configuring iLO access settings.....	61
iLO access settings.....	61
Configuring iLO service settings.....	61
Service settings.....	61
Configuring iLO access options.....	62
Access options.....	63
iLO login with an SSH client.....	67
7 Configuring the iLO security features.....	68
iLO security features.....	68
General security guidelines for iLO.....	68
iLO RBSU and iLO 4 Configuration Utility security.....	68
iLO security with the system maintenance switch.....	69
TPM and TM.....	69
Viewing the TPM or TM status.....	70
TPM or TM status values.....	70
User accounts and access.....	70
User privileges.....	70
Login security.....	70
Administering SSH keys.....	71
Authorizing a new SSH key by using the web interface.....	71
Authorizing a new SSH key by using the CLI.....	72
Deleting SSH keys.....	73
Authorizing SSH keys from an HPE SIM server	73
SSH keys.....	73
Administering SSL certificates.....	74
Viewing SSL certificate information.....	74
SSL certificate details.....	75
Obtaining and importing an SSL certificate.....	75
CSR input details.....	77
Directory authentication and authorization.....	78
Prerequisites for configuring authentication and directory server settings.....	78
Configuring Kerberos authentication settings in iLO.....	78
Kerberos settings.....	78
Configuring schema-free directory settings in iLO.....	79
Schema-free directory settings.....	79
Configuring HPE Extended Schema directory settings in iLO.....	79
HPE Extended Schema directory settings.....	80
Directory user contexts.....	80
Local user accounts with Kerberos authentication and directory integration.....	81
Running directory tests.....	81
Directory test input values.....	82
Directory test status values.....	82
Directory test results.....	82
iLO directory tests.....	83
iLO encryption settings.....	84
SSL.....	84
Ciphers supported by iLO.....	84
SSH.....	85
FIPS mode.....	85
AES/3DES encryption.....	86
Viewing encryption enforcement settings.....	86
Encryption settings.....	86
Modifying the AES/DES encryption setting.....	87
Connecting to iLO by using AES or 3DES encryption.....	87

Configuring a FIPS-validated environment with iLO.....	87
Enabling FIPS mode.....	87
Disabling FIPS mode.....	88
HPE SSO.....	89
Configuring iLO for HPE SSO.....	89
Single Sign-On Trust Mode options.....	90
SSO user privileges.....	90
Adding trusted certificates.....	90
Trusted certificate format.....	91
Extracting the HPE SIM server certificate.....	91
Importing a direct DNS name.....	91
Viewing trusted certificates and records.....	91
Trusted certificate and record details.....	92
Removing trusted certificates and records.....	92
Configuring the Login Security Banner.....	92
Configuring Remote Console Computer Lock settings.....	93
Remote Console Computer Lock options.....	94
Valid Remote Console Computer Lock keys.....	94
Configuring the Integrated Remote Console Trust setting (.NET IRC).....	94
Integrated Remote Console Trust setting options.....	95
8 Configuring the iLO network settings.....	96
iLO network settings.....	96
Viewing the network configuration summary.....	96
Network configuration summary details.....	96
IPv4 Summary details.....	97
IPv6 Summary details.....	97
Configuring the iLO Hostname Settings.....	98
iLO hostname and domain name limitations.....	98
Configuring the NIC settings.....	99
Enabling the iLO Dedicated Network Port through the iLO web interface.....	99
Link State values.....	99
Enabling the iLO Shared Network Port through the iLO web interface (nonblade servers only).....	100
iLO network port configuration options.....	101
iLO network connection considerations.....	101
Other available methods for configuring the NIC settings.....	102
Configuring IPv4 settings.....	102
DHCPv4 settings.....	102
General IPv4 settings.....	103
DNS server settings.....	103
WINS server settings.....	103
Ping Gateway on Startup setting.....	103
Configuring IPv6 settings.....	103
DHCPv6 settings.....	104
DNS server settings.....	105
General IPv6 settings.....	105
iLO features that support IPv6.....	105
Configuring iLO SNTP settings.....	106
SNTP options.....	107
iLO clock synchronization.....	108
DHCP NTP address selection.....	108
iLO NIC auto-selection.....	108
NIC auto-selection support.....	109
iLO startup behavior with NIC auto-selection enabled.....	109
Enabling iLO NIC auto-selection.....	110

Configuring NIC failover.....	110
Viewing iLO systems in the Windows Network folder.....	110
9 Configuring iLO management settings.....	112
iLO SNMP management.....	112
AMS and the Insight Management Agents.....	114
Installing AMS or the Insight Management Agents.....	114
Verifying the AMS installation.....	114
Verifying AMS status: iLO web interface.....	114
Verifying AMS status: Windows.....	115
Verifying AMS status: SUSE and Red Hat Enterprise Linux.....	115
Verifying AMS status: VMware.....	115
Verifying AMS status: Ubuntu.....	115
Restarting AMS.....	115
Nagios plug-in for Agentless Management.....	115
Configuring SNMP settings.....	116
SNMP options.....	117
SNMP options (Agentless Management configuration only).....	117
SNMPv3 authentication.....	118
Configuring SNMPv3 users.....	118
SNMPv3 user options.....	119
Configuring the SNMPv3 Engine ID.....	119
Configuring SNMP alerts.....	119
SNMP alert settings.....	120
Using the AMS Control Panel to configure SNMP and SNMP alerts (Windows only).....	121
SNMP traps.....	121
Configuring Insight Management integration.....	124
iLO AlertMail.....	125
Enabling AlertMail.....	125
AlertMail options.....	126
Disabling AlertMail.....	126
Remote Syslog.....	126
Enabling iLO Remote Syslog.....	126
Remote syslog options.....	127
Disabling iLO Remote Syslog.....	127
10 Managing remote support.....	128
HPE embedded remote support.....	128
Device support.....	129
Data collected by HPE remote support.....	129
HPE Proactive Care service.....	130
Prerequisites for remote support registration.....	130
Registering for remote support by using the iLO web interface.....	131
Registering for Insight Online direct connect.....	132
Other Insight Online direct connect registration methods.....	134
Editing the web proxy settings(Insight Online direct connect only).....	134
Registering for Insight Remote Support central connect.....	134
Other Insight Remote Support central connect registration methods.....	135
Unregistering from Insight Remote Support by using the iLO web interface.....	135
Unregistering from Insight Online direct connect.....	135
Unregistering from Insight Remote Support central connect.....	136
Remote support service events.....	136
Using maintenance mode.....	136
Sending a test service event.....	137
Viewing the Service Event Log.....	137
Service event log details.....	137

Supported service event types.....	138
Clearing the Service Event Log.....	138
Remote Support data collection.....	138
Sending data collection information.....	139
Viewing data collection status in iLO.....	139
Data Collection details.....	140
Sending Active Health System reporting information.....	140
Viewing Active Health System reporting status in iLO.....	140
Active Health System reporting details.....	140
11 Managing iLO with the ROM-based utilities.....	141
iLO ROM-based utilities.....	141
Configuring network settings with the ROM-based utilities.....	141
Configuring NIC and TCP/IP settings (iLO RBSU).....	141
Configuring DNS/DHCP settings (iLO RBSU).....	141
Configuring Advanced network settings (iLO RBSU).....	141
Configuring Network Options (iLO 4 Configuration Utility).....	142
Configuring Advanced Network Options (iLO 4 Configuration Utility).....	142
Network Options.....	143
Advanced Network Options.....	143
Configuring access settings with the ROM-based utilities.....	144
Configuring global settings (iLO RBSU).....	144
Configuring serial CLI options (iLO RBSU).....	144
Configuring access settings (iLO 4 Configuration Utility).....	144
Viewing information about iLO by using the iLO 4 Configuration Utility.....	145
About.....	145
12 Using the iLO web interface.....	146
iLO web interface.....	146
Browser support.....	146
Configuring the Internet Explorer JavaScript setting.....	146
Logging in to the iLO web interface.....	147
Cookie sharing between browser instances and iLO.....	147
Using the iLO controls.....	148
Starting a remote management tool from the login page.....	149
Language pack support.....	149
13 Viewing iLO overview and system information.....	150
Viewing iLO overview information.....	150
System information.....	150
System status details.....	151
HPE remote support status.....	152
Active sessions list.....	152
Viewing system information with iLO.....	152
Viewing health summary information.....	153
Redundancy status.....	153
Subsystem and device status.....	153
Subsystem and device status values.....	154
Viewing fan information.....	154
Fan details.....	155
Fans.....	155
Temperature information	155
Viewing the temperature graph.....	155
Temperature graph details.....	156
Viewing temperature sensor data.....	156
Temperature sensor details.....	157

Temperature monitoring.....	157
Viewing power information.....	158
Power Supply Summary details.....	158
Power Supplies list.....	160
HPE Power Discovery Services iPDU Summary.....	161
Power Readings.....	162
Power Microcontroller.....	162
Smart Storage Battery details.....	163
Power monitoring.....	163
High Efficiency Mode.....	163
Viewing processor information.....	163
Processor details.....	164
Viewing memory information.....	164
Advanced Memory Protection details.....	164
Memory Summary.....	166
Memory Details.....	167
Viewing network information.....	169
Physical Network Adapters.....	169
Logical Network Adapters.....	171
Viewing the device inventory.....	171
Device Inventory details.....	172
Device status values.....	172
Viewing PCI slot details.....	172
PCI slot tool tip details.....	173
Viewing storage information.....	173
Supported storage components.....	174
Smart Array details.....	174
Controllers.....	174
Drive Enclosures.....	175
Logical Drives.....	176
Physical Drives.....	176
Direct-attached storage details.....	177
Controllers.....	177
Physical Drives.....	177
Viewing firmware information.....	178
Firmware types.....	178
Firmware details.....	179
Viewing software information.....	179
HPE Software List details.....	180
Running Software details.....	180
Installed Software details.....	181
14 Using the iLO logs.....	182
iLO Event Log.....	182
Viewing the event log.....	182
Event log details.....	182
Event log icons.....	183
Customizing the event log view.....	183
Saving the event log to a CSV file.....	184
Clearing the event log.....	184
Integrated Management Log.....	184
Viewing the IML.....	185
IML details.....	185
IML icons.....	186
Customizing the IML view.....	186

Marking an IML entry as repaired.....	186
Adding a maintenance note to the IML.....	187
Saving the IML to a CSV file.....	187
Clearing the IML.....	188
IML troubleshooting links.....	188
15 Using the Active Health System.....	189
Active Health System.....	189
Active Health System data collection.....	189
Active Health System Log.....	189
Active Health System Log download methods.....	189
Downloading the Active Health System Log for a date range.....	190
Downloading the entire Active Health System Log.....	190
Extracting the Active Health System Log by using curl.....	191
curl command usage with iLO 4.....	191
Clearing the Active Health System Log.....	191
16 Using the iLO diagnostics, reboot, and reset features.....	193
iLO diagnostics.....	193
Viewing iLO self-test results.....	193
Resetting the iLO processor through the web interface	193
Generating an NMI.....	194
Configuring redundant ROM.....	194
Rebooting (Resetting) iLO.....	195
Resetting iLO (iLO 4 Configuration Utility).....	196
Rebooting iLO with the server UID button.....	196
Performing a graceful iLO reboot with the server UID button.....	196
Performing a hardware iLO reboot with the server UID button.....	197
Reset iLO to the factory default settings.....	197
Resetting iLO to the factory default settings (iLO RBSU).....	197
Resetting iLO to the factory default settings (iLO 4 Configuration Utility).....	197
17 Using iLO Federation.....	199
iLO Federation features.....	199
Selected Group list.....	199
Selected Group list filters.....	200
Selected Group list filter criteria.....	200
Exporting iLO Federation information to a CSV file.....	200
iLO Federation information export options.....	201
iLO Federation Multi-System view.....	201
Viewing server health and model information.....	201
Server health and model details.....	201
Viewing servers with critical and degraded status.....	201
Critical and degraded server status details.....	202
Viewing the iLO Federation Multi-System Map.....	202
iLO peer details.....	202
iLO Federation Group Virtual Media.....	203
Connecting scripted media for groups.....	203
Viewing scripted media status for groups.....	204
Scripted media details.....	204
Ejecting a scripted media device.....	204
Servers affected by a Group Virtual Media action.....	205
iLO Federation Group Power.....	205
Changing the power state for a group of servers.....	205
Virtual Power Button options.....	206
Servers affected by the Virtual Power Button.....	207

Configuring group power capping.....	207
Power capping considerations.....	208
Viewing group power capping information.....	209
Power capping details.....	209
iLO Federation Group Firmware Update.....	210
Obtaining the iLO firmware image file.....	210
Obtaining supported server firmware image files.....	210
Server firmware file type details.....	211
Updating the firmware for multiple servers.....	211
Viewing firmware information.....	212
Firmware details.....	212
Servers affected by a Group Firmware Update.....	212
Using iLO Federation group licensing.....	213
Viewing license information.....	213
iLO Federation group license details.....	213
Installing license keys (iLO Federation group).....	213
Servers affected by a license installation.....	214
Using the iLO Federation Group Configuration feature.....	214
18 Using the iLO Remote Consoles.....	215
Using the Integrated Remote Console.....	215
.NET IRC requirements.....	216
Microsoft .NET Framework.....	216
Microsoft ClickOnce.....	217
Starting the Integrated Remote Console.....	217
Acquiring the Remote Console.....	218
Using the Remote Console power switch.....	218
Using iLO Virtual Media from the Remote Console.....	219
Shared Remote Console (.NET IRC only).....	219
Joining a Shared Remote Console session.....	219
Console Capture (.NET IRC only).....	220
Viewing Server Startup and Server Prefailure sequences.....	221
Saving Server Startup and Server Prefailure video files.....	221
Capturing video files.....	221
Viewing saved video files.....	222
Remote Console hot keys.....	222
Creating hot keys.....	222
Keys for configuring Remote Console hot keys.....	223
Resetting hot keys.....	223
Viewing configured remote console hot keys (Java IRC only).....	223
Using a text-based Remote Console.....	224
Using the iLO Virtual Serial Port.....	224
Configuring the iLO Virtual Serial Port in the host system RBSU.....	224
Configuring the iLO Virtual Serial Port in the UEFI System Utilities.....	225
Configuring the iLO Virtual Serial Port for Linux.....	226
Windows EMS Console with iLO Virtual Serial Port.....	227
Configuring Windows for use with the iLO Virtual Serial Port.....	227
Starting an iLO Virtual Serial Port session.....	228
Viewing the iLO Virtual Serial Port log.....	228
Text-based Remote Console (Textcons).....	228
Customizing the Text-based Remote Console.....	229
Using the Text-based Remote Console.....	230
Using Linux with the Text-based Remote Console.....	230
19 Using iLO Virtual Media.....	231
iLO Virtual Media.....	231

Virtual Media operating system information.....	232
Operating system USB requirement.....	232
Configuring Windows 7 for use with iLO Virtual Media with Windows 7.....	232
Operating system considerations: Virtual Floppy/USB key.....	233
Changing diskettes.....	233
Operating system considerations: Virtual CD/DVD-ROM.....	233
Mounting a USB Virtual Media CD/DVD-ROM on Linux systems.....	234
Operating system considerations: Virtual Folder	234
Using Virtual Media from the iLO web interface.....	234
Viewing and modifying the Virtual Media port.....	234
Viewing local media.....	235
Local media details.....	235
Ejecting a local media device.....	235
Connecting scripted media.....	235
Viewing connected scripted media.....	236
Scripted media details.....	236
Ejecting scripted media.....	236
Remote Console Virtual Media.....	236
Virtual Drives.....	236
Using a physical drive on a client PC.....	236
Using an image file.....	237
Using an image file through a URL (IIS/Apache).....	237
Using the Create Media Image feature (Java IRC only).....	237
Creating a disk image file.....	237
Copying data from an image file to a physical disk.....	238
Using a Virtual Folder (.NET IRC only).....	238
Virtual folders.....	238
Setting up IIS for scripted Virtual Media.....	239
Configuring IIS.....	239
Configuring IIS for read/write access.....	239
Inserting Virtual Media with a helper application.....	240
Sample Virtual Media helper application.....	240
Virtual Media Boot Order.....	241
Configuring the server boot mode.....	242
Configuring the server boot order.....	242
Changing the one-time boot status.....	243
Changing the one-time boot status in Legacy BIOS mode.....	243
Changing the one-time boot status in UEFI mode.....	244
Using the additional options.....	244
20 Using the power management features.....	245
Server power-on with iLO 4.....	245
Brownout recovery.....	245
Graceful shutdown.....	245
Power efficiency.....	246
Power-on protection.....	246
Power allocation (blade servers).....	246
Managing the server power.....	247
Virtual Power Button options.....	247
Configuring the System Power Restore Settings.....	248
Auto Power-On settings.....	248
Power-On Delay settings.....	249
Viewing server power usage.....	249
Power meter graph details.....	249
Power meter graph display options.....	250

Viewing the current power state.....	250
Current power state details.....	251
Viewing the server power history.....	251
Power history details.....	251
Power settings.....	252
Power Regulator settings.....	252
Power Regulator modes.....	252
Configuring power caps.....	253
Power capping considerations.....	253
Configuring battery backup unit settings.....	254
Battery backup unit options.....	254
Configuring SNMP alert settings.....	254
Configuring the persistent mouse and keyboard.....	255
21 Working with enclosures, frames, and chassis.....	256
Using the Active Onboard Administrator.....	256
Viewing OA information.....	256
OA details.....	256
Starting the OA GUI.....	256
Toggling the enclosure UID LED.....	257
Enclosure bay IP addressing.....	257
Dynamic Power Capping for server blades.....	257
iLO virtual fan.....	257
iLO option.....	257
Viewing frame information.....	258
Frame details.....	258
Toggling the frame UID LED.....	258
Server details.....	259
Toggling the server UID LED.....	259
Viewing chassis information.....	259
Power Supplies list.....	259
Intelligent Power Distribution Unit details.....	261
Smart Storage Battery details.....	261
22 Using the Embedded User Partition.....	262
iLO Embedded User Partition.....	262
Configuring the Embedded User Partition.....	263
Configuring the Embedded User Partition (UEFI System Utilities).....	263
Configuring the Embedded User Partition (UEFI Shell).....	263
Configuring the Embedded User Partition (RESTful Interface Tool).....	263
Configuring the Embedded User Partition boot settings.....	264
Configuring the Embedded User Partition boot order setting (iLO web interface).....	264
Configuring the Embedded User Partition for one-time boot (iLO web interface).....	264
Configuring the Embedded User Partition boot order setting (UEFI System Utilities).....	265
Configuring the Embedded User Partition for one-time boot (UEFI System Utilities).....	265
Configuring the Embedded User Partition boot order setting (UEFI Shell).....	266
Configuring the Embedded User Partition for one-time boot (UEFI Shell).....	266
Configuring the Embedded User Partition boot order setting (RESTful Interface Tool).....	266
Configuring the Embedded User Partition for one-time boot (RESTful Interface Tool).....	266
23 Using iLO with other software products and tools.....	267
Viewing Location Discovery Services information.....	267
Location Discovery Services details.....	267
Location Discovery Services.....	268
Using the HPE Insight Management Agents.....	268
IPMI server management.....	269

Advanced IPMI tool usage on Linux.....	270
Using iLO with HPE Insight Control server provisioning	270
Using Enterprise Secure Key Manager with iLO.....	270
Configuring key manager servers.....	271
Adding key manager configuration details.....	272
Testing the ESKM configuration.....	273
Viewing ESKM events.....	273
Clearing the ESKM log.....	273
iLO and remote management tools.....	273
Starting a remote management tool from iLO.....	273
Deleting a remote manager configuration.....	274
Using iLO with HPE OneView.....	274
Server signatures (Synergy compute modules only).....	275
Using iLO with HPE SIM.....	275
HPE SIM features.....	275
Establishing SSO with HPE SIM.....	275
iLO identification and association.....	276
Viewing iLO status in HPE SIM.....	276
iLO links in HPE SIM.....	276
Viewing iLO in HPE SIM System lists.....	276
Receiving SNMP alerts in HPE SIM.....	276
HPE SIM port matching.....	277
Reviewing iLO license information in HPE SIM.....	277
24 Kerberos authentication and Directory services.....	278
Kerberos authentication with iLO.....	278
Configuring Kerberos authentication.....	278
Configuring the iLO hostname and domain name for Kerberos authentication.....	278
iLO hostname and domain name requirements for Kerberos authentication.....	278
Preparing the domain controller for Kerberos support.....	279
Generating a keytab file for iLO in a Windows environment.....	279
Ktpass.....	279
Setspn.....	280
Verifying that your environment meets the Kerberos authentication time requirement.....	281
Configuring Kerberos support in iLO.....	281
Using the iLO web interface to configure iLO for Kerberos login.....	281
Using XML configuration and control scripts to configure iLO for Kerberos login.....	281
Using the CLI, CLP, or SSH interface to configure iLO for Kerberos login.....	281
Configuring supported browsers for single sign-on.....	282
Enabling single-sign-on in Internet Explorer.....	282
Enabling single-sign on in Firefox.....	283
Chrome.....	283
Verifying the single sign-on (Zero Sign In) configuration.....	283
Verifying that login by name works.....	283
Directory integration.....	283
Choosing a directory configuration to use with iLO.....	284
Schema-free directory authentication.....	284
Prerequisites for using schema-free directory integration.....	285
Using the iLO web interface to configure iLO for schema-free directory integration.....	286
Using XML configuration and control scripts to configure iLO for schema-free directory integration.....	286
Required values for the schema-free integration with Active Directory:.....	286
Using the CLI, CLP, or SSH interface to configure iLO for schema-free directory integration.....	286
Setting up a schema-free configuration (Directories Support for ProLiant Management Processors).....	287

Schema-free nested groups (Active Directory only).....	287
HPE Extended Schema directory authentication.....	287
Process overview: Configuring the HPE Extended Schema with Active Directory.....	287
Prerequisites for configuring Active Directory with the HPE Extended Schema configuration.....	288
Directory services support.....	288
Installing the iLO directory support software.....	288
Directories Support for ProLiant Management Processors install options.....	289
Running the Schema Extender.....	290
Schema Extender required information.....	291
Directory services objects.....	291
Managing roles and objects with the Active Directory snap-ins.....	291
Setting a client IP address or DNS name restriction.....	294
Sample configuration: Active Directory and HPE Extended Schema.....	294
Configuration process overview.....	295
Snap-in installation and initialization for Active Directory.....	295
Creating and configuring directory objects for use with iLO in Active Directory.....	295
Directory-enabled remote management (HPE Extended Schema configuration).....	297
Roles based on organizational structure.....	297
How role access restrictions are enforced.....	298
User access restrictions.....	299
User address restrictions.....	299
IP address range restrictions.....	299
IP address and subnet mask restrictions.....	299
DNS-based restrictions.....	299
User time restrictions.....	300
Role access restrictions.....	300
Role-based time restrictions.....	300
Role-based address restrictions.....	301
Multiple restrictions and roles.....	301
Tools for configuring multiple iLO systems at a time.....	302
User login using directory services.....	302
Directories Support for ProLiant Management Processors utility (HPLOMIG.exe).....	303
Directories Support for ProLiant Management Processors Compatibility.....	304
Configuring directory authentication with HPLOMIG.....	304
Discovering management processors.....	304
HPLOMIG management processor search criteria.....	305
HPLOMIG management processor import list requirements.....	306
Optional: Upgrading firmware on management processors (HPLOMIG).....	306
Selecting directory configuration options.....	307
Management processor selection methods.....	309
Directory access methods and settings.....	309
Naming management processors (HPE Extended Schema only).....	309
Configuring directories when HPE Extended Schema is selected.....	310
Configuring management processors (Schema-free configuration only).....	315
Management processor settings.....	316
Setting up management processors for directories.....	316
25 Troubleshooting.....	319
Using the iLO Virtual Serial Port with Windbg.....	319
Using the ProLiant Preboot Health Summary.....	320
Preboot Health Summary details.....	321
Event log entries.....	322
Incorrect time stamp on iLO Event Log entries.....	322
Login and iLO access issues.....	322
iLO firmware login name and password not accepted.....	322

iLO management port not accessible by name.....	323
iLO RBSU unavailable after iLO and server reset.....	323
Unable to access the iLO login page.....	324
Unable to return to iLO login page after iLO reset.....	324
Unable to connect to iLO after changing network settings.....	324
An iLO connection error occurs after an iLO firmware update.....	325
Unable to connect to iLO processor through NIC.....	325
Unable to log in to iLO after installing iLO certificate.....	325
Unable to connect to iLO IP address.....	326
iLO communications fail.....	326
Secure Connection Failed error when using Firefox to connect to iLO.....	326
Certificate error when navigating to iLO web interface.....	327
iLO login page displays a Website Certified by an Unknown Authority message.....	328
iLO inaccessible on a server managed by HPE OneView.....	328
Unable connect to an iLO system with the iOS mobile app.....	329
iLO responds to pings intermittently or does not respond.....	329
Running an XML script with iLO fails.....	330
Directory issues.....	330
Logging in to iLO with Kerberos authentication fails.....	330
iLO Credential prompt appears during Kerberos login attempt.....	331
iLO Credential prompt appears during Kerberos login by name attempt.....	332
A directory connection to iLO ends prematurely.....	332
Configured Directory user contexts do not work with iLO login.....	332
iLO directory user account does not log out after directory timeout expires.....	333
Failure generating Kerberos Keytab file for iLO Zero Sign In configuration.....	333
Error when running Setspn for iLO Kerberos configuration.....	333
iLO Zero Sign In fails after domain controller OS reinstall.....	334
Failed iLO login with Active Directory credentials.....	334
Directory Server DNS Name test reports a failure.....	334
Ping Directory Server test reports a failure.....	335
Connect to Directory Server test reports a failure.....	335
Connect using SSL test reports a failure.....	335
Bind to Directory Server test reports a failure.....	336
Directory Administrator Login test reports a failure.....	336
User Authentication test reports a failure.....	336
User Authorization test reports a failure.....	336
Directory User Contexts test reports a failure.....	337
LOM Object Exists test reports a failure.....	337
Remote Console issues.....	337
iLO Java IRC displays red X when Firefox is used to run Java IRC on Linux client.....	337
iLO Java IRC does not start.....	338
Cursor cannot reach iLO Remote Console window corners.....	338
iLO Remote Console text window not updated correctly.....	338
Mouse or keyboard not working in iLO remote console.....	338
iLO .NET IRC sends characters continuously after switching windows	339
iLO Java IRC displays incorrect floppy and USB-key device information.....	339
Caps Lock out of sync between iLO and Java IRC.....	340
Num Lock out of sync between iLO and Shared Remote Console.....	340
Keystrokes repeat unintentionally during iLO Remote Console session.....	340
Session leader does not receive connection request when iLO .NET IRC is in replay mode.....	341
iLO Remote Console Keyboard LED does not work correctly.....	341
iLO .NET IRC becomes inactive or disconnects.....	341
iLO .NET IRC failed to connect to server.....	342
File not present after copy from server to iLO Virtual Media USB key.....	343
iLO .NET IRC takes a long time to verify application requirements.....	343

iLO .NET IRC will not start.....	343
iLO .NET IRC cannot be shared.....	344
iLO .NET IRC will not start in Firefox.....	344
iLO .NET IRC will not start in Google Chrome.....	345
Unable to boot to DOS using a USB key mounted with the iLO Remote Console.....	345
Text-based Remote Console issues.....	346
Unable to view Linux installer in text-based Remote Console.....	346
Unable to pass data through SSH terminal.....	346
VSP-driven selection during the serial timeout window sends output to BIOS redirect instead of VSP.....	346
Scrolling and text appear irregular during BIOS redirection.....	347
SSH issues.....	347
Initial PuTTY input slow with iLO.....	347
PuTTY client unresponsive with iLO Shared Network Port.....	347
Text is displayed incorrectly when using an SSH connection to iLO.....	348
An SSH session fails to start or terminates unexpectedly.....	348
Remote Support issues.....	348
SSL Bio Error during Insight RS registration.....	348
Server not identified by server name in Insight Online or Insight RS.....	349
Server OS name and version not listed in Insight RS or Insight Online.....	349
Connection error during Insight Online direct connect registration.....	350
iLO session ends unexpectedly during iLO Insight Online direct connect registration.....	350
Server health status is red in Insight RS or Insight Online.....	351
iLO Federation issues.....	351
Query errors occur on iLO Federation pages.....	351
A timeout error is displayed on the iLO Multi-System Map page.....	352
iLO Multi-System Map page displays a 502 error.....	352
iLO Multi-System Map page displays a 403 error.....	353
iLO peers are not displayed on iLO Federation pages.....	353
iLO peers are displayed with IPv6 addresses on IPv4 networks.....	353
Firmware update issues.....	354
Unsuccessful iLO firmware update.....	354
iLO firmware update error.....	354
iLO firmware update does not finish.....	354
iLO network Failed Flash Recovery.....	355
License key installation errors.....	356
Unable to access Virtual Media or graphical Remote Console.....	356
Unable to get SNMP information in HPE SIM.....	357
Unable to receive HPE SIM alarms (SNMP traps) from iLO.....	357
Server name still present after System Erase Utility is executed.....	357
AMS is installed but unavailable in iLO.....	358
26 Support and other resources.....	359
Accessing Hewlett Packard Enterprise Support.....	359
Accessing updates.....	359
Lost license key recovery.....	360
Websites.....	360
Customer self repair.....	360
Remote support.....	360
Documentation feedback.....	361
A iLO license options.....	362
HPE iLO standard and licensed features.....	362
B Directory services schema.....	365
HPE Management Core LDAP OID classes and attributes.....	365

Core class definitions.....	365
Core attribute definitions.....	366
Lights-Out Management specific LDAP OID classes and attributes.....	368
Lights-Out Management attributes.....	368
Lights-Out Management class definitions.....	368
Lights-Out Management attribute definitions.....	369
Glossary.....	371
Index.....	375

1 Introduction

iLO overview

iLO is a remote server management processor embedded on the system boards of HPE ProLiant servers and Synergy compute modules. iLO enables the monitoring and controlling of servers from remote locations. HPE iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely. iLO (Standard) comes preconfigured on HPE servers **without an additional cost or license**.

Features that enhance server administrator productivity are licensed. For more information, see the iLO licensing guide at the following website: <http://www.hpe.com/support/iLOLicenseGuide-en>.

iLO key features

- **Server health monitoring**—iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. iLO also monitors installed firmware and software versions and the status of fans, memory, the network, processors, power supplies, storage, and devices installed on the system board.
- **Agentless management**—When you use the Agentless Management configuration, the management software (SNMP) operates within the iLO firmware instead of the host OS. This configuration frees memory and processor resources on the host OS for use by server applications. iLO monitors all key internal subsystems, and can send SNMP alerts directly to a central management server, even with no host OS installed.
- **Integrated Management Log**—View server events and configure notifications via SNMP alerts, remote syslogs, and email alerts.
- **Active Health System Log**—Download the Active Health System log. You can send the log file to Hewlett Packard Enterprise when you have an open support case.
- **iLO Federation management**—Use the iLO Federation features to discover and manage multiple servers at a time.
- **Integrated Remote Console**—If you have a network connection to the server, you can access a secure high-performance console to manage the server from any location.
- **Virtual Media**—Remotely mount high-performance Virtual Media devices to the server.
- **Power management**—Securely and remotely control the power state of the managed server.
- **Deployment and provisioning**—Use Virtual Power and Virtual Media for tasks such as the automation of deployment and provisioning.
- **Power consumption and power settings**—Monitor the server power consumption, configure server power settings, and configure power capping on supported servers.
- **Embedded remote support**—Register a ProLiant Gen8 or Gen9 server for HPE remote support.
- **User accounts**—Use local or directory-based user accounts to log in to iLO.
- **Kerberos support**—Configure Kerberos authentication, which adds the **Zero Sign In** button to the login screen.

iLO web interface

The iLO web interface groups similar tasks for easy navigation and workflow. The interface is organized in a navigational tree view on the left side of the page. The top-level branches are **Information**, **iLO Federation**, **Remote Console**, **Virtual Media**, **Power Management**, **Network**, **Remote Support**, and **Administration**.

The following additional branches are available if your server type or configuration supports them:

- If you have a ProLiant server blade, the **BL c-Class** branch is included.
- If you have a Synergy compute module, the **Synergy Frame** branch is included.
- If you have a ProLiant XL or SL server, the **Chassis** branch is included.
- When a remote management tool is used with iLO, the **<Remote Management Tool Name>** branch is included.

The screenshot shows the iLO 4 web interface. The top header includes the iLO 4 logo, the server model 'ProLiant MicroServer Gen8', the local user 'admin', and navigation links for 'HOME' and 'SIGN OUT'. The main content area is titled 'iLO Overview'. On the left, a sidebar menu is open, showing the 'Information' branch expanded, with 'Overview' selected. Other branches listed include 'System Information', 'iLO Event Log', 'Integrated Management Log', 'Active Health System Log', 'Diagnostics', 'Location Discovery Services', 'Insight Agent', 'iLO Federation', 'Remote Console', 'Virtual Media', 'Power Management', 'Network', 'Remote Support', and 'Administration'. The main content area displays two tables: 'Information' and 'Status'. The 'Information' table includes fields like Server Name (ProLiant MicroServer Gen8), Product Name (ProLiant MicroServer Gen8), UUID, Server Serial Number (815P601007G), Product ID (J06 06/06/2014), System ROM (J06 06/06/2014), System ROM Date (06/06/2014), Backup System ROM (J06 06/06/2014), Integrated Remote Console (.NET, Java Web Start, Java Applet, iLO Advanced), License Type, iLO Firmware Version (2.50 Jul 19 2016), IP Address, Link-Local IPv6 Address, and iLO Hostname. The 'Status' table includes fields like System Health (OK), Server Power (ON), UID Indicator (UID OFF), TPM Status (Not Present), SD-Card Status (Not Present), and iLO Date/Time (Wed Jul 27 09:36:52 2016). Below these tables is a section titled 'Connection to HPE' with a checked checkbox for 'Registered to Remote Support'. At the bottom, there is an 'Active Sessions' table with one entry for 'User: Local User: admin', 'IP Address' (redacted), and 'Source: HTTPS'. The bottom navigation bar includes icons for 'POWER: ON', 'UID: OFF', 'EN(LANGUAGE)', and a checked checkbox.

When you use the iLO web interface, note the following:

- Each high level iLO branch has a submenu that you can display by clicking the icon to the left of that branch. To view an iLO web interface page, click a submenu item.
- Assistance for all iLO pages is available from the iLO help pages. To access page-specific help, click the question mark icon (?).
- Troubleshooting information is available for selected IML events. Supported events are displayed as links in the **Description** column on the **Integrated Management Log** page.
- Typical administrator tasks are available from the **iLO Federation**, **Network**, **Remote Support**, **Administration**, and **<Remote Management Tool Name>** branches of the iLO web interface.
- Typical user tasks are available from the **Information**, **Remote Console**, **Virtual Media**, **Power Management**, **iLO Federation**, **BL c-Class**, **Chassis**, and **Synergy Frame** branches of the iLO web interface.

ROM-based configuration utilities

Depending on your server model, you can use iLO RBSU or the iLO 4 Configuration Utility to configure network parameters, global settings, and user accounts. On servers that support UEFI, such as the ProLiant DL580 Gen8 server, ProLiant Gen9 servers, and Synergy compute modules, use the iLO 4 Configuration Utility in the UEFI System Utilities. On servers that do not support UEFI, use the iLO RBSU.

iLO RBSU and the iLO 4 Configuration Utility are designed for the initial iLO setup, and are not intended for continued iLO administration. You can start these utilities when the server is booted, and you can run them remotely with the Remote Console.

To determine whether your server supports iLO RBSU or the iLO 4 Configuration Utility, see the server QuickSpecs at <http://www.hpe.com/info/qs/>.

You can configure iLO to require users to log in when they access the ROM-based configuration utilities, or you can disable the utilities for all users. These settings can be configured in the iLO access options. Disabling iLO RBSU or the iLO 4 Configuration Utility prevents reconfiguration from the host unless the system maintenance switch is set to disable iLO security.

More information

[iLO access settings](#)

[iLO ROM-based utilities](#)

iLO mobile app

The iLO mobile app provides access to your servers from a mobile device. The mobile app interacts directly with the iLO processor, providing total control of the server at all times as long as the server is plugged in. For example, you can access the server when it is in a healthy state or when it is powered off with a blank hard drive. As an IT administrator, you can troubleshoot problems and perform software deployments from almost anywhere.

For more information about the iLO mobile app, see <http://www.hpe.com/info/ilo/mobileapp>.

iLO scripting and command line

You can use the iLO scripting tools to configure multiple servers, to incorporate a standard configuration into the deployment process, and to control servers and subsystems.

The iLO scripting and CLI guide describes the syntax and tools available for using iLO through a command line or scripted interface.

iLO RESTful API

iLO 4.2.00 and later includes the iLO RESTful API. The iLO RESTful API is a management interface that server management tools can use to perform server configuration, inventory, and monitoring via iLO. A REST client, such as the RESTful Interface Tool, sends HTTPS operations to the iLO web server to `GET` and `PATCH` JSON-formatted data, and to configure supported iLO and server settings.

iLO 4.2.30 and later is Redfish 1.0-conformant while remaining backward compatible with the existing iLO RESTful API.

Some examples of the supported HTTPS operations include `GET`, `PUT`, `POST`, `PATCH`, and `DELETE`.

You can use the RESTful Interface Tool to access all of the iLO features that are enabled with the iLO Standard or iLO Standard for BladeSystem license. To access features enabled by the iLO Scale-Out, iLO Essentials, iLO Advanced, or iLO Advanced for BladeSystem license, you must install a license.

iLO 4 supports the iLO RESTful API with ProLiant Gen8 and Gen9 servers and Synergy compute modules. The RESTful Interface Tool is not supported with ProLiant Gen8 servers.

For more information about the iLO RESTful API and the RESTful Interface Tool, see the following website: <http://www.hpe.com/info/restfulapi>.

2 Setting up iLO

Preparing to set up iLO

Before setting up an iLO management processor, you must decide how to handle networking and security. The following questions can help you configure iLO:

1. [How should iLO connect to the network?](#)
2. [Will NIC Teaming be used with the Shared Network Port configuration?](#)
3. [How will iLO acquire an IP address?](#)
4. [What access security is required, and what user accounts and privileges are needed?](#)
5. [What tools will you use to configure iLO?](#)

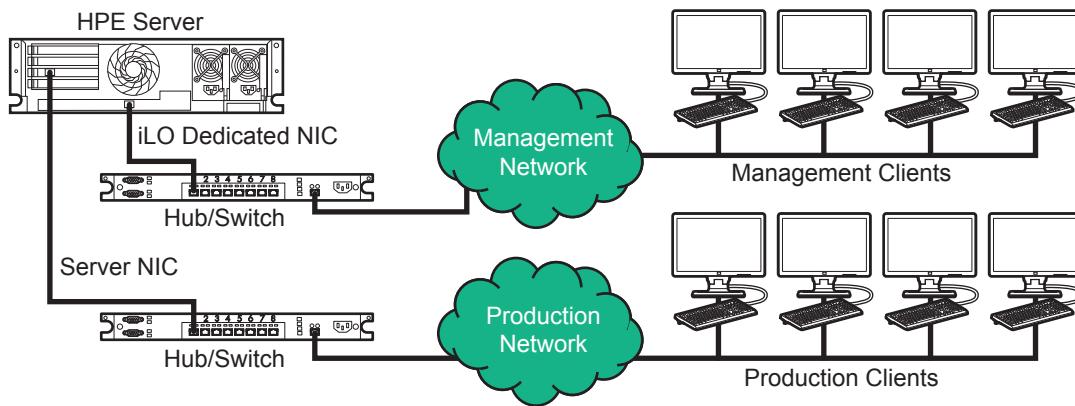
iLO network connection options

Typically, iLO is connected to the network through a dedicated management network or a shared connection on the production network.

Dedicated management network

In this configuration, the iLO port is on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the production network. In this configuration, iLO cannot be accessed directly from the production network. The Dedicated management network is the preferred iLO network configuration.

Figure 1 Dedicated management network



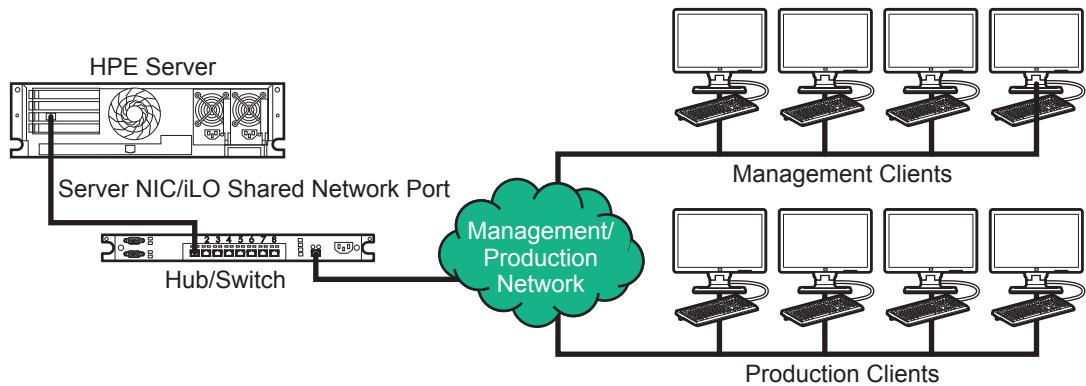
Production network

In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iLO.

There are some drawbacks to using this configuration.

- With a shared network connection, traffic can hinder iLO performance.
- During the server boot process and when the OS NIC drivers are loading and unloading, there are brief periods of time (2–8 seconds) when iLO cannot be reached from the network. After these short periods, iLO communication is restored and iLO will respond to network traffic.

Figure 2 Shared network connection



NIC teaming with Shared Network Port configurations

NIC teaming is a feature you can use to improve server NIC performance and reliability. If iLO is configured to use the Shared Network Port, make sure you observe the following constraints:

NIC teaming constraints

Note the following when you select a teaming mode to use when iLO is configured to use the Shared Network Port:

- iLO network communications will be blocked in the following conditions:
 - The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
 - The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.
- Because iLO and the server transmit and receive on the same switch port, the selected NIC teaming mode must allow the switch to tolerate traffic with two different MAC addresses on the same switch port. Some implementations of LACP (802.3ad) will not tolerate multiple MAC addresses on the same link.

Hewlett Packard Enterprise NIC teaming modes

If your server is configured to use Hewlett Packard Enterprise NIC teaming, observe the following guidelines.

For additional information, see the [ProLiant Network Adapter Teaming support document](#).

If your server uses another implementation of NIC teaming, see “[NIC teaming constraints](#)” and the vendor documentation for information about selecting a NIC teaming mode.

- **Network Fault Tolerance (NFT)**—The server transmits and receives on only one NIC (the primary adapter). The other NICs (secondary adapters) that are part of the team do not

transmit server traffic and they ignore received traffic. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the **Preferred Primary Adapter**.

- **Transmit Load Balancing (TLB)**—The server transmits on multiple adapters but receives only on the primary adapter. This mode allows the iLO Shared Network Port to function correctly.

Select the NIC/port iLO uses as the **Preferred Primary Adapter**.

- **Switch Assisted Load Balancing (SLB)**—This mode type refers to the following:
 - HPE ProCurve Port Trunking
 - Cisco Fast EtherChannel/Gigabit EtherChannel (Static Mode Only, no PAgP)
 - IEEE 802.3ad Link Aggregation (Static Mode only, no LACP)
 - Bay Network Multi-Link Trunking
 - Extreme Network Load Sharing

In this mode, there is no concept of primary and secondary adapters. All adapters are considered equal for the purposes of sending and receiving data. This mode is the most problematic for iLO Shared Network Port configurations because traffic destined for iLO can be received on only one of the server NIC/ports. To determine the constraints that your switch vendor places on their implementation of SLB, see the switch vendor documentation.

iLO IP address acquisition

To enable iLO access after it is connected to the network, the iLO management processor must acquire an IP address and subnet mask. You can use a dynamic address or a static address.

- A **dynamic IP address** is set by default. iLO obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.

If you use DHCP:

- The iLO management port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, it will reissue the request at 90-second intervals.
- The DHCP server must be configured to provide DNS and WINS name resolution.

- If DNS or DHCP servers are not available on the network, a **static IP address** is used. A static IP address can be configured by using iLO RBSU or the iLO 4 Configuration Utility. If you plan to use a static IP address, you must have the IP address before starting the iLO setup process.

iLO access security

You can use the following methods to manage access to iLO:

- **Local accounts**—Up to 12 user accounts can be stored in iLO. This configuration is ideal for small environments such as labs and small-sized or medium-sized businesses.
- **Directory services**—Use the corporate directory to manage iLO user access. This configuration is ideal for environments with many users. If you plan to use directory services, consider enabling at least one local administrator account for alternate access.

More information

[iLO security features](#)

[iLO user accounts](#)

[Directory authentication and authorization](#)

iLO configuration tools

iLO supports various interfaces for configuration and operation. This guide discusses the following interfaces:

- Use **iLO RBSU** or the **iLO 4 Configuration Utility** when the system environment does not use DHCP, DNS, or WINS.
- Use the **iLO web interface** when you can connect to iLO on the network by using a web browser. You can also use this method to reconfigure an iLO management processor.

Other configuration options not discussed in this guide follow:

- **Intelligent Provisioning**—Press **F10** during POST to start Intelligent Provisioning. For information about the iLO settings you can configure, see the Intelligent Provisioning documentation at the following website: <http://www.hpe.com/info/intelligentprovisioning/docs>.
- **HPE Scripting Toolkit**—This toolkit is a server deployment product for IT experts that provides unattended automated installation for high-volume server deployments. For more information, see the Scripting Toolkit user guide for Windows or Linux.
- **Scripting**—You can use scripting for advanced setup of multiple iLO management processors. Scripts are XML files written for a scripting language called RIBCL. You can use RIBCL scripts to configure iLO on the network during initial deployment or from a deployed host.

The following methods are available:

- **HPQLOCFG**—This utility replaces the previously used CPQLOCFG utility. It is a Windows command-line utility that sends XML configuration and control scripts over the network to iLO.
- **HPONCFG**—A local online scripted setup utility that runs on the host and passes RIBCL scripts to the local iLO. HPONCFG requires the ProLiant iLO 3/4 Channel Interface Driver.
- **Custom scripting environments (LOCFG.PL)**—The iLO scripting samples include a Perl sample that can be used to send RIBCL scripts to iLO over the network.
- **SMASH CLP**—A command-line protocol that can be used when a command line is accessible through SSH or the physical serial port.

For more information about these methods, see the iLO scripting and CLI guide.

iLO sample scripts are available at the following website: <http://www.hpe.com/support/ilo4>.

- **iLO RESTful API**—A management interface that server management tools can use to perform configuration, inventory, and monitoring of a supported server via iLO.

For more information, see <http://www.hpe.com/info/restfulinterface/docs>.

HPE OneView—A management tool that interacts with the iLO management processor to configure, monitor, and manage ProLiant servers or Synergy compute modules. For more information, see “[Using iLO with HPE OneView](#)” (page 274).

Initial setup steps: Process overview

The iLO default settings enable you to use most features without additional configuration. However, the configuration flexibility of iLO enables customization for multiple enterprise environments. This chapter discusses the initial iLO setup steps.

1. [Connect iLO to the network](#).
2. If you are not using dynamic IP addressing, use the ROM-based setup utilities to [configure a static IP address](#).
3. If you will use the local accounts feature, use the ROM-based setup utilities to [configure user accounts](#).
4. Optional: [Install an iLO license](#).
5. [If necessary, install the iLO drivers](#).

Connecting iLO to the network

Connect iLO to the network through a production network or a dedicated management network.

iLO uses standard Ethernet cabling, which includes CAT 5 UTP with RJ-45 connectors.

Straight-through cabling is necessary for a hardware link to a standard Ethernet hub or switch.

For more information about setting up your hardware, see the server user guide at the following website: <http://www.hpe.com/info/docs>.

More information

[iLO network connection options](#)

Setting up iLO by using the ROM-based setup utilities

Hewlett Packard Enterprise recommends using iLO RBSU or the iLO 4 Configuration Utility to set up iLO for the first time and to configure iLO network parameters for environments that do not use DHCP, DNS, or WINS.

To determine whether your server supports iLO RBSU or the iLO 4 Configuration Utility, see the server QuickSpecs at <http://www.hpe.com/info/qs/>.

On servers that use the system RBSU and not the UEFI System Utilities, the iLO option ROM lists the installed license and the firmware version. This information is not listed in the option ROM on UEFI systems.

Accessing the ROM-based setup utilities

- To access the iLO RBSU, press **F8** during POST.
Use the arrow keys and the **Enter** key to navigate through the iLO RBSU menus. To make configuration changes, follow the on-screen instructions.
- To access the UEFI System Utilities, press **F9** during POST, and then select **System Configuration**→**iLO 4 Configuration Utility**.
For more information, see the UEFI System Utilities user guide.

Configuring a static IP address with the ROM-based setup utilities

This step is required only if you want to use a static IP address. When you use dynamic IP addressing, the DHCP server automatically assigns an IP address for iLO.

To simplify installation, Hewlett Packard Enterprise recommends using DNS or DHCP with iLO.

Configuring a static IP address (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.

2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Disable DHCP:
 - a. From the iLO RBSU screen, select **Network**→**DNS/DHCP**, and then press **Enter**.
 - b. Select **DHCP Enable**.
 - c. To set **DHCP Enable** to **OFF**, press the spacebar, and then press **F10** to save the changes.
5. Enter the network settings:
 - a. From the iLO RBSU screen, select **Network**→**NIC and TCP/IP**, and then press **Enter**.
 - b. Enter the appropriate information in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields.
 - c. To save the changes, press **F10**.
6. Select **File**→**Exit**.

The changes take effect when you exit iLO RBSU.

Configuring a static IP address (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Configuration** screen, use the up or down arrow keys and the **Enter** key to navigate to the **System Configuration**→**iLO 4 Configuration Utility**→**Network Options** screen.
5. Disable DHCP:
 - a. Select **DHCP Enable**, and then press **Enter**.
 - b. Select **OFF**, and then press **Enter**.
6. Enter an IP address, subnet mask, and gateway IP address:
 - a. Select **IP Address**, and then press **Enter**.
 - b. Type the IP address, and then press **Enter**.
 - c. Select **Subnet Mask**, and then press **Enter**.
 - d. Type the subnet mask address, and then press **Enter**.
 - e. Select **Gateway IP Address**, and then press **Enter**.
 - f. Type the gateway IP address, and then press **Enter**.
7. To save the changes, press **F10**.
The iLO 4 Configuration Utility prompts you to confirm that you want to save all pending configuration changes.
8. To save and exit, press **Y**.
The iLO 4 Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.
9. Press **Enter**.
iLO resets, and the iLO session is automatically ended. You can reconnect in approximately 30 seconds.

10. Resume the normal boot process:
 - a. Start the iLO remote console.
The iLO 4 Configuration Utility is still open from the previous session.
 - b. Press **ESC** several times to navigate to the **System Configuration** page.
 - c. To exit the System Utilities and resume the normal boot process, press **ESC**.

Managing local user accounts with the ROM-based setup utilities

Adding user accounts (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. From the iLO RBSU screen, select **User→Add**, and then press **Enter**.
5. Enter the following details:
 - **User Name**
 - **Login Name**
 - **Password** and **Verify password**
6. Select from the following privileges. To enable a privilege, set it to **Yes**. To disable a privilege, set it to **No**.
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**
7. To save the new user account, press **F10**.
8. Repeat [Step 4](#) through [Step 7](#) until you are done creating user accounts.
9. Select **File→Exit**.

More information

[iLO user privileges](#)

[User account options](#)

[Password guidelines](#)

Editing user accounts (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. From the iLO RBSU screen, select **User→Edit**, and then press **Enter**.
5. Select the user name that you want to edit, and then press **Enter**.
6. Update the user name, login name, password, or user privileges, and then press **F10** to save the changes.
7. Select **File→Exit**.

More information

[iLO user privileges](#)

[User account options](#)

[Password guidelines](#)

Removing user accounts (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. From the iLO RBSU screen, select **User→Remove**, and then press **Enter**.
5. Select the user that you want to remove, and then press **Enter**.
The iLO RBSU prompts you to confirm the request.
6. To confirm the request, press **Enter**.
7. Select **File→Exit**.

Adding user accounts (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→User Management→Add User**, and press **Enter**.
5. Select any of the following privileges, and then press **Enter**:
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**
6. For each option, select one of the following settings and press **Enter** again.
 - **YES** (default)—Enables the privilege for this user.
 - **NO**—Disables the privilege for this user.
7. Select from the following options, and then press **Enter**.
 - **New User Name**
 - **Login Name**
 - **Password and Password Confirm**
8. Complete each option for the new user, and press **Enter**.
9. Create as many user accounts as needed, and then press **F10**.
10. Press **Esc** until the main menu is displayed.
11. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
12. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

More information

[iLO user privileges](#)

[User account options](#)

[Password guidelines](#)

Editing or removing user accounts (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**User Management**→**Edit/Remove User**, and press **Enter**.
5. Select the **Action** menu for the user name you want to edit or delete, and press **Enter**.
6. Select one of the following, and press **Enter**.
 - **No Change**—Returns you to the main menu.
 - **Delete**—Deletes this user.
 - **Edit**—Edits the user.
7. Depending on your selection in **Step 6**, do one of the following:
 - If you selected **No Change**, no further action is needed.
 - If you selected **Delete**, the user name is marked to be deleted when you save the changes on this page.
 - If you selected **Edit**, update the login name, password, or user permissions.
8. Update as many user accounts as needed, and then press **F10**.
9. Press **Esc** until the main menu is displayed.
10. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
11. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

More information

[iLO user privileges](#)

[User account options](#)

[Password guidelines](#)

iLO setup with the web interface

If you can connect to iLO on the network by using a web browser, you can use the iLO web interface to configure iLO. You can also use this method to reconfigure an iLO management processor.

Access iLO from a remote network client by using a supported browser and providing the default DNS name, user name, and password.

Logging in to iLO for the first time

1. Enter `https://<iLO hostname or IP address>`.
HTTPS (HTTP exchanged over an SSL encrypted session) is required for accessing the iLO web interface.
2. Enter the default user credentials, and then click **Log In**.

More information

[Login security](#)

[iLO default credentials](#)

iLO default credentials

The iLO firmware is configured with a default user name, password, and DNS name. Default user information is on the serial label pull tab attached to the server that contains the iLO management processor. Use these values to access iLO remotely from a network client by using a web browser.

- **User name**—Administrator
- **Password**—A random eight-character alphanumeric string
- **DNS name**—ILOXXXXXXXXXXXX, where the Xs represent the server serial number.

① **IMPORTANT:** Hewlett Packard Enterprise recommends changing the default password after you log in to iLO for the first time.

If you reset iLO to the factory default settings, use the default iLO account information to log in after the reset.

iLO licensed features

iLO (Standard) is preconfigured on HPE servers without an additional cost or license. Features that enhance productivity are licensed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

To activate iLO licensed features, install an iLO license.

More information

[Installing a license key by using a browser](#)

iLO drivers and utilities

iLO is an independent microprocessor running an embedded operating system. The architecture ensures that most iLO functionality is available, regardless of the host operating system. The iLO drivers and System Health Application and Command Line Utilities enable software such as HPONCFG and the Agentless Management Service to communicate with iLO. The installed OS and system configuration determine the installation requirements.

Microsoft driver support

When you use Windows with iLO, the following drivers are available:

- **ProLiant iLO 3/4 Channel Interface Driver for Windows**—This driver is required for the operating system to communicate with iLO. Install this driver in all configurations.
- **ProLiant iLO 3/4 Management Controller Driver Package for Windows**—This package includes the following components:
 - `hpqilo3core` provides iLO Management Controller Driver support.
 - `hpqilo3service` provides the ProLiant Health Monitor Service and ProLiant System Shutdown Service.
 - `hpqilo3whea` is a helper service for Windows Hardware Error Architecture. If a hardware fault occurs, this service passes information between iLO and the operating system.

The Management Controller Driver Package is required to support Automatic Server Recovery and the Insight Management Agents or Insight Management WBEM Providers (if installed).

Linux driver and utility support

When you use Linux with iLO, the following drivers and utilities are available:

- **System Health Application and Command Line Utilities** (`hp-health`)—A collection of applications and tools that enables monitoring of fans, power supplies, temperature sensors, and other management events. This RPM contains the `hpasmd`, `hpasmlited`, `hpasmpld`, and `hpasmxld` daemons.

- `hpilo`—This driver manages agent and tool application access to iLO.

This driver is part of the Linux kernel for SUSE Linux Enterprise Server 10 SP3 and later and Red Hat Enterprise Linux 5.3 and later. The `hpilo` driver is loaded automatically at startup.

For servers that support earlier versions of SUSE Linux Enterprise Server and Red Hat Enterprise Linux, install the `hp-ilo` RPM package from the SPP.

On Ubuntu systems, this driver is loaded automatically at startup after the Linux Management Component Pack package is loaded.

VMware driver support

When you use VMware with iLO, the following driver is available:

ProLiant Channel Interface Driver (`hpilo`)—This driver manages agent, WBEM provider, and tool application access to iLO. It is included in the customized Hewlett Packard Enterprise VMware images. For raw VMware images, the driver must be installed manually.

Installing the iLO drivers and utilities

Obtaining the iLO drivers and utilities

Obtain the iLO drivers and System Health Application and Command Line Utilities by downloading the Service Pack for ProLiant, or by downloading them from the Hewlett Packard Enterprise website.

- **For Windows, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server**—Use the SPP to install the iLO drivers or System Health Application and Command Line Utilities.
- **For Windows, Red Hat Enterprise Linux and SUSE Linux Enterprise Server**—Download the iLO drivers or System Health Application and Command Line Utilities from the Hewlett Packard Enterprise Support Center at <http://www.hpe.com/support/hpesc>.
- **For VMware**—Download the iLO driver from the `vibsdepot` section of the Software Delivery Repository website: <http://www.hpe.com/support/SDR-Linux>.
Follow the installation instructions provided with the software.
- **For Ubuntu**—Subscribe to the Linux Management Component Pack at <http://www.hpe.com/support/SDR-Linux> to obtain the System Health Application and Command Line Utilities.

More information

[Driver and utility installation with the SPP](#)

[Loading hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux](#)

[Installing hp-health for Ubuntu](#)

Driver and utility installation with the SPP

See the following websites for information about using the SPP:

- SPP documentation: <http://www.hpe.com/info/spp/documentation>
- SPP Custom Download hosted service: <http://www.hpe.com/servers/spp/custom>

Loading hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux

Use the following command to load hp-health:

```
rpm -ivh hp-health-<d.vv.v-pp.Linux_version.arch>.rpm
```

Where <d> is the Linux distribution and version, <vv.v-pp> are version numbers, and <arch> is the architecture (i386 or x86_64).

Removing hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux

Use the following command to remove hp-health:

```
rpm -e hp-health
```

Installing hp-health for Ubuntu

1. Subscribe to the Linux Management Component Pack.

Hewlett Packard Enterprise recommends subscribing to the Linux Management Component Pack repository to ensure that your Ubuntu systems have the latest Hewlett Packard Enterprise software.

For instructions, see the following website: www.hpe.com/support/hpesc.

2. To update the repository cache, enter the following command `apt-get update`.
3. To install hp-health, enter the following command:

```
apt-get install hp-health.
```

Removing hp-health for Ubuntu

Use the following command to remove hp-health:

```
apt-get remove hp-health
```

3 Updating iLO firmware, language, and licensing

Firmware updates

Firmware updates enhance server and iLO functionality with new features, improvements, and security updates.

You can update firmware by using an online or offline firmware update method.

Online firmware update

When you use an online method to update firmware, you can perform the update without shutting down the server operating system. Online firmware updates can be performed in-band or out-of-band.

- **In-band**—Firmware is sent to iLO from the server host operating system. The ProLiant Channel Interface Driver is required for in-band firmware updates. During a host-based firmware update, iLO does not verify user credentials or privileges because the host-based utilities require a root (Linux and VMware) or Administrator (Windows) login.
The iLO Online ROM Flash Component and HPONCFG are examples of online in-band firmware update methods.
- **Out-of-band**—Firmware is sent to iLO over a network connection. Users with the Configure iLO Settings privilege can update firmware by using an out-of-band method. If the system maintenance switch is set to disable iLO security, any user can update firmware with an out-of-band method.
The iLO web interface, HPQLOCFG, HPLOMIG, the iLO RESTful API, LOCFG.PL, and SMASH CLP are examples of online out-of-band firmware update methods.

Offline firmware update

Offline firmware update—When you use an offline method to update the firmware, you must reboot the server by using an offline utility.

The SPP, the Scripting Toolkit for Windows, and the Scripting Toolkit for Linux are examples of offline firmware update methods.

Online firmware update methods

In-band firmware updates

You can use the following in-band firmware update methods:

- **Online ROM Flash Component**—Use an executable file to update firmware while the server is running. The executable file contains the installer and the firmware package. You can download online ROM flash components for iLO and server firmware at the following website: <http://www.hpe.com/support/ilo4>.
- **HPONCFG**—Use this utility to update firmware by using XML scripts. Download the iLO or server firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.
Sample scripts are available at <http://www.hpe.com/support/ilo4>. For more information about scripting, see the iLO scripting and CLI guide.

Out-of-band firmware updates

You can use the following out-of-band firmware update methods:

- **iLO web interface**—Download a supported firmware file and install it by using the iLO web interface. You can update firmware for a single server or an iLO Federation group.
- **HPQLOCFG**—Use this utility to update firmware by using XML scripts. Download the iLO or server firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.
Sample scripts are available at <http://www.hpe.com/support/ilo4>. For more information about scripting, see the iLO scripting and CLI guide.
- **HPLOMIG** (also called Directories Support for ProLiant Management Processors)—You do not need to use directory integration to take advantage of the firmware update capabilities in HPLOMIG. This utility can be used to discover multiple iLO processors and update their firmware in one step.
- **SMASH CLP**—Access SMASH CLP through the SSH port, and use standard commands to view firmware information and update firmware.
For more information about SMASH CLP, see the iLO scripting and CLI guide.
- **iLO RESTful API**—Use the iLO RESTful API and a REST client to update firmware. For more information, see <http://www.hpe.com/info/restfulinterface/docs>.

Offline firmware update methods

You can use the following offline firmware update methods:

- **SPP**—Use the SPP to install firmware. For more information, see the following website: <http://www.hpe.com/info/spp/documentation>.
- **Scripting Toolkit**—Use the Scripting Toolkit to configure several settings within the server and update firmware. This method is useful for deploying to multiple servers. For instructions, see the Scripting Toolkit user guide for Windows or Linux.

Supported firmware types

The following firmware types can be updated from the **Firmware Update** page:

- iLO firmware
- System ROM (BIOS)
- Chassis firmware (SL and XL servers)
- Power Management Controller
- System Programmable Logic Device (CPLD)
- NVMe Backplane Firmware
- EdgeLine Chassis Controller Firmware

Obtaining the iLO firmware image file

The BIN file from the iLO Online ROM Flash Component is required for some of the methods you can use to update the iLO firmware.

1. Navigate to the Hewlett Packard Enterprise Support Center at <http://www.hpe.com/support/hpesc>.
2. To locate and download the iLO Online ROM Flash Component file, follow the onscreen instructions.

To extract the BIN file, download a Windows or Linux component.

3. Extract the BIN file.

- For Windows components: Double-click the downloaded file, and then click the **Extract** button. Select a location for the extracted files, and then click **OK**.
- For Linux components: Depending on the file format, enter one of the following commands:
 - `#sh ./CP00XXXX.scexe -unpack=/tmp/`
 - `#rpm2cpio hp-firmware-ilo4-2.xx-1x1.i386.rpm | cpio -id`

The name of the iLO firmware image file is similar to `ilo4_<yyy>.bin`, where `<yyy>` represents the firmware version.

Obtaining supported server firmware image files

1. Navigate to the Hewlett Packard Enterprise Support Center at <http://www.hpe.com/support/hpesc>.
2. To locate and download an Online ROM Flash Component file, follow the onscreen instructions.
3. Double-click the downloaded file, and then click the **Extract** button.
4. Select a location for the extracted files, and then click **OK**.

Server firmware file type details

- The system ROM firmware image file name uses a format similar to the following: `CPQJ0123.B18`.
- The Power Management Controller, chassis firmware, and NVMe backplane files use the file extension `.hex`. For example, the file name might be similar to `ABCD5S95.hex`.
- The System Programmable Logic Device (CPLD) firmware file uses the file extension `.vme`.

Updating iLO or server firmware by using the iLO web interface

You can update firmware from any network client by using the iLO web interface.

Prerequisites

Configure iLO Settings privilege

Installing a firmware update

1. Obtain the firmware image file.
2. Navigate to the **Administration**→**Firmware** page.
3. Click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome), and then specify the location of the firmware image file in the **File** box.

Local File: *Update the firmware by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the update from starting.*

File:

No file chosen

4. To start the update process, click **Upload**.

iLO notifies you that:

- When you update the iLO firmware, iLO will reboot automatically.
- Some types of server firmware might require a server reboot, but the server will not reboot automatically.

5. Click **OK**.

The iLO firmware receives, validates, and then flashes the firmware image.

If you navigate away from the **Firmware Update** page before the file upload is complete, the firmware update will not start.

① **IMPORTANT:** Do not interrupt a firmware update. If a firmware update is interrupted or fails, attempt it again immediately.

When you update the iLO firmware, iLO reboots and closes your browser connection. It might take several minutes before you can re-establish a connection.

6. For iLO firmware updates only: To start working with the new firmware, clear your browser cache, and then log in to iLO.
7. For server firmware updates only: If the firmware type requires a system reset or server reboot for the new firmware to take effect, take the appropriate action. For more information, see ["Requirements for firmware update to take effect" \(page 38\)](#).
8. Optional: To confirm that the new firmware is active, check the version on the **System Information**→**Firmware** page.

More information

[Unsuccessful iLO firmware update](#)

[iLO network Failed Flash Recovery](#)

[Obtaining the iLO firmware image file](#)

[Obtaining supported server firmware image files](#)

Requirements for firmware update to take effect

- System ROM (BIOS)—Requires a server reboot.
- Chassis firmware (Power Management)—Requires a chassis reset, which is triggered automatically.
- System Programmable Logic Device (CPLD)—Requires a server reboot.
- Power Management Controller and NVMe Backplane Firmware—Do not require a server reboot or a system reset.

The NVMe firmware version will be displayed in the iLO web interface after the next server reboot.

Language packs

Language packs enable you to change the iLO web interface from English to a supported language of your choice. Language packs provide translations for the iLO web interface, .NET IRC, and Java IRC.

Consider the following when using language packs:

- The following language packs are available: Japanese and Simplified Chinese.
- The English language cannot be uninstalled.

- For iLO 4 2.10 and earlier—You can install one language pack.
Installing a new language pack replaces the currently installed language pack, regardless of the language pack version.
- For iLO 4 2.20 and later—You can install multiple language packs.
When version 2.20 or later of a language pack is installed, installing a new language pack (same language, v2.20 or later) replaces the installed language pack.
- iLO 4 2.20 or later requires version 2.20 or later of the iLO language pack.
- For iLO 4 2.20 and later—Language packs are not supported on servers (such as the ProLiant ML10 Gen9 and ML10v2 Gen9 servers) that do not have a NAND. On these servers, the message **This server does not support installing additional language packs** is displayed on the **Access Settings**→**Language** page.
To continue using language packs on servers without a NAND, use iLO 4 2.10 or earlier.
- When you upgrade from an earlier version of iLO 4 to version 2.20 or later, previously installed language packs are deleted.
- The Java IRC and .NET IRC use the language of the current iLO session.
- For localization support with the Java IRC on Windows systems, you must select the correct language in the **Regional and Language Options** Control Panel.
- For localization support with the Java IRC on Linux systems, make sure that the fonts for the specified language are installed and available to the JRE.
- If an installed language pack does not include the translation for a text string, the text is displayed in English.
- When you update the iLO firmware, Hewlett Packard Enterprise recommends downloading the latest language pack to ensure that the language pack contents match the iLO web interface.

Installing language packs

Prerequisites

Configure iLO Settings privilege

Installing a language pack

1. Navigate to the following website: <http://www.hpe.com/support/ilo4>.
2. To locate and download a language pack, follow the onscreen instructions.
3. To extract the contents, double-click the downloaded file.
The language pack file name is similar to the following:
lang_<language>_<version>.lpk.
4. Navigate to the **Administration**→**Access Settings**→**Language** page.
5. Click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome).

Install Language Pack

Obtain the latest language pack for use in the Web GUI, .NET IRC, and Java IRC from <http://www.hpe.com/support/ilo4>.

Note: iLO 4 versions 2.20 and higher require language packs versioned 2.20 or higher.

Local File: *Install a language pack by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the installation from starting.*

File: No file chosen

6. Select the language pack, and then click **Open**.

iLO prompts you to confirm the installation.

For iLO 4 2.10 and earlier: If you have a previously installed language pack, this language pack will replace it if you proceed with the installation.

7. Click **OK**.

8. Click **Install**.

iLO installs the language pack, reboots, and closes your browser connection.

It might take several minutes before you can re-establish a connection.

Selecting a language pack

Use one of the following methods to select an installed language pack:

- Navigate to the login page, and then select a language in the **Language** menu.

Directory or local user name:

Password:

Language



- Click the **Language** menu in the toolbar on the bottom right side of the browser window, and then select a language.



- Select a language on the **Administration**→**Access Settings**→**Language** page. For instructions, see “[Configuring the current browser session language](#)” (page 41).

Configuring the default language settings

Prerequisites

Configure iLO Settings privilege

Setting the default language

Use this procedure to configure the default language for the users of this instance of the iLO firmware.

1. Navigate to the **Administration**→**Access Settings**→**Language** page.
2. Select a value in the **Default Language** menu.

The available languages are English and any other language for which a language pack is installed.

3. Click **Apply**.

iLO notifies you that the default language was changed.

In subsequent iLO web interface sessions, if there is no browser cookie from a previous session, and the browser or OS language is not supported, the iLO web interface uses the configured default language.

Configuring the current browser session language

1. Navigate to the **Administration**→**Access Settings**→**Language** page.
2. Select a value in the **Current Language** menu.

The available languages are English and any other language for which a language pack is installed.

3. Click **Apply**.

The iLO web interface for the current browser session changes to the selected language.

Uninstalling a language pack

Prerequisites

Configure iLO Settings privilege

Removing a language pack

1. Navigate to the **Administration**→**Access Settings**→**Language** page.
2. For iLO 4.2.20 or later: Select the check box next to the language you want to uninstall.
3. Click **Uninstall**.
4. When prompted to confirm the request, click **OK**.

iLO removes the selected language pack, reboots, and closes your browser connection.

It might take several minutes before you can re-establish a connection.

How iLO determines the session language

iLO uses the following process to determine the language of a web interface session:

1. If you previously logged in to the iLO web interface on the same computer using the same browser, and you have not cleared the cookies, the language setting of the last session with that iLO processor is used.
2. If there is no cookie, the current browser language is used if iLO supports it and the required language pack is installed.

3. **Internet Explorer only:** If the browser language is not supported, then the OS language is used if iLO supports it and the required language pack is installed.
4. If there is no cookie, and the browser or OS language is not supported, iLO uses the configured default language. For more information, see “[Configuring the default language settings](#)” (page 41).

iLO licensing

iLO standard features are included with every server to simplify server setup, perform health monitoring, monitor power and thermal control, and facilitate remote administration.

iLO licenses activate functionality such as graphical Remote Console with multiuser collaboration, video record/playback, and many more features.

License key information

- For information about purchasing, registering, and redeeming a license key, see the iLO licensing guide at the following website: <http://www.hpe.com/info/ilo/docs>.
- One iLO license is required for each server on which the product is installed and used. Licenses are not transferable.
- You cannot license a server with a license key that is meant for a different server type.
- Use the **Licensing** page to view and install licenses for ProLiant servers.
- An iLO Advanced license is automatically included with Synergy compute modules. Use the **Licensing** page to view the license. You cannot add or remove a license on Synergy compute modules.
- If you lose a license key, follow the lost license key instructions. For more information, see “[Lost license key recovery](#)” (page 360).
- A free iLO evaluation license key is available for download from the following website: <http://www.hpe.com/info/tryilo>. For more information, see the iLO licensing guide.

Installing a license key by using a browser

Prerequisites

- Configure iLO Settings privilege
- The server you want to license is a ProLiant server. For Synergy compute modules, an iLO Advanced license is automatically included, and the **Enter License Activation Key** section is not displayed on the iLO **Licensing** page.

Installing a license key

1. Navigate to the **Administration**→**Licensing** page.
2. Enter a license key in the **Activation Key** box.

Enter License Activation Key

Note: When a new license activation key is installed, the current key is replaced by the new key.

Activation Key	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------------	----------------------	----------------------	----------------------	----------------------

To move between segments, press the **Tab** key or click inside a segment of the **Activation Key** box. The cursor advances automatically when you enter data into the segments of the **Activation Key** box.

3. Click **Install**.

The EULA confirmation opens. The EULA details are available in the License Pack option kit.

4. Click **OK**.

The license key is now enabled.

For tips on troubleshooting license installation, see “[License key installation errors](#)” (page 356).

Viewing license information

Navigate to the **Administration**→**Licensing** page.

License details

Current License Status		
License	Status	Activation Key
iLO Advanced	OK	xxxxx-xxxxx-xxxxx-xxxx-RR53R

- **License**—The license name
- **Status**—The license status
- **Activation Key**—The installed key

4 Managing user accounts and directory groups

iLO user accounts

iLO enables you to manage user accounts stored locally in secure memory and directory group accounts. Use MMC or ConsoleOne to manage directory-based user accounts.

You can create up to 12 local user accounts with custom login names and advanced password encryption. Privileges control individual user settings, and can be customized to meet user access requirements.

To support more than 12 users, you must have an iLO license, which enables integration with an unlimited number of directory-based user accounts. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

The following privileges are required for user and directory group administration:

- **Administer User Accounts**—Required for adding, modifying, and deleting users. If you do not have this privilege, you can view your own settings and change your password.
- **Configure iLO Settings**—Required for adding, modifying, and deleting directory groups. If you do not have this privilege, you can view directory groups.

You can also manage users with the iLO RBSU or the iLO 4 Configuration Utility.

Local user accounts

Viewing local user accounts

Navigate to the **Administration**→**User Administration** page.

The **Local Users** table shows the login names, user names, and assigned privileges of each configured user. Move the cursor over an icon to see the privilege name.

Local Users						
Login Name	User Name	RA	VM	VPR	CG	CS
admin	admin					
Administrator	Administrator	✓	✓	✓	✓	✓
susan	susan	✓	✓	✓	✓	✓

New **Edit** **Delete**

iLO user privileges

The following privileges apply to user accounts:

- **RA Remote Console Access**—Enables a user to access the host system Remote Console, including video, keyboard, and mouse control.
- **VM Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
- **VPR Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **CG Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to update the iLO firmware. This privilege does not enable local user account administration.

After iLO is configured, revoking this privilege from all users prevents reconfiguration with the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the UEFI

System Utilities, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.

Adding local user accounts

Prerequisites

Administer User Accounts privilege

Adding a user account

1. Navigate to the **Administration**→**User Administration** page.
2. To open the **Add/Edit Local User** page, click **New** in the **Local Users** section.
3. Enter the following details:
 - **User Name**
 - **Login Name**
 - **Password and Password Confirm**
4. Select from the following privileges:
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**To select all of the available user privileges, click the **select all** check box.
5. To save the new user, click **Add User**.

More information

[iLO user privileges](#)

[User account options](#)

[Password guidelines](#)

Editing local user accounts

Prerequisites

Administer User Accounts privilege

Editing a user account

1. Navigate to the **Administration**→**User Administration** page.
2. Select a user in the **Local Users** section, and then click **Edit**.
3. Update the following values on the **Add/Edit Local User** page, as needed:
 - **User Name**
 - **Login Name**
4. To change the password, click the **Change password** check box, and then update the **Password** and **Password Confirm** values.

5. Select from the following privileges:

- **Administer User Accounts**
- **Remote Console Access**
- **Virtual Power and Reset**
- **Virtual Media**
- **Configure iLO Settings**

To select all of the available user privileges, click the **select all** check box.

6. To save the user account changes, click **Update User**.

More information

[iLO user privileges](#)

[Password guidelines](#)

[User account options](#)

Deleting a user account

Prerequisites

Administer User Accounts privilege

Deleting a user account

1. Navigate to the **Administration**→**User Administration** page.
2. Select the check box next to the user account that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

User account options

The following options are available when you add and edit user accounts.

- **User Name** appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The **User Name** must use printable characters. Assigning descriptive user names can help you to identify the owner of each login name.
- **Login Name** is the name you use when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.
- **Password** and **Password Confirm** set and confirm the password that is used for logging in to iLO.

Password guidelines

Hewlett Packard Enterprise recommends that you follow these password guidelines when you create and edit 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, such as the company name, product name, user name, or login name.
- Use passwords with at least three of the following characteristics:
 - One numeric character
 - One special character
 - One lowercase character
 - One uppercase character
- The minimum length for an iLO 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. The default **Minimum Password Length** is eight characters.

① **IMPORTANT:** Hewlett Packard Enterprise does not recommend setting 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. For information about setting the **Minimum Password Length**, see [“iLO access settings” \(page 61\)](#).

IPMI/DCMI users

The iLO firmware follows the IPMI 2.0 specification. When you add IPMI/DCMI users, the login name must be a maximum of 16 characters, and the password must be a maximum of 20 characters.

When you select iLO user privileges, the equivalent IPMI/DCMI user privilege is displayed in the **IPMI/DCMI Privilege based on above settings** box.

- **User**—A user has read-only access. A user cannot configure or write to iLO, or perform system actions.
For IPMI User privileges: Disable all privileges. Any combination of privileges that does not meet the Operator level is an IPMI User.
- **Operator**—An operator can perform system actions, but cannot configure iLO or manage user accounts.
For IPMI Operator privileges: Enable Remote Console Access, Virtual Power and Reset, and Virtual Media. Any combination of privileges greater than Operator that does not meet the Administrator level is an IPMI Operator.
- **Administrator**—An administrator has read and write access to all features.
For IPMI Administrator privileges: Enable all privileges.

Directory groups

Viewing directory groups

Navigate to the **Administration**→**User Administration** page.

The **Directory Groups** table shows the group DN, group SID, and the assigned privileges for the configured groups. Move the cursor over an icon to see the privilege name.

Directory Groups		SID						
Group	Administrators	S-1-5-11						
Authenticated Users								
New				Edit		Delete		

Directory group privileges

The following privileges apply to directory groups:

- **Login Privilege**—Enables members of a group to log in to iLO.
- **Remote Console Access**—Enables users to access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Media**—Enables users to use the Virtual Media feature on the host system.
- **Virtual Power and Reset**—Enables users to power-cycle or reset the host system. These activities interrupt the system availability. Users with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **Configure iLO Settings**—Enables users to configure most iLO settings, including security settings, and to update iLO firmware.

After iLO is configured, revoking this privilege from all users prevents reconfiguration with the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the UEFI System Utilities, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- **Administer User Accounts**—Enables users to add, edit, and delete local iLO user accounts.

Adding directory groups

Prerequisites

Configure iLO Settings privilege

Adding a directory group

1. Navigate to the **Administration**→**User Administration** page.
2. Click **New** in the **Directory Groups** section.
3. Provide the following details in the **Group Information** section:
 - **Group DN**
 - **Group SID** (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**
 - **Login Privilege**
5. To save the new directory group, click **Add Group**.

More information

[Directory group privileges](#)

[Directory group settings](#)

Editing directory groups

Prerequisites

Configure iLO Settings privilege

Editing a directory group

1. Navigate to the **Administration**→**User Administration** page.
2. Select a group in the **Directory Groups** section, and then click **Edit**.
3. Provide the following details in the **Group Information** section:
 - **Group DN**
 - **Group SID** (Kerberos authentication and Active Directory integration only)
4. Select from the following privileges:
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**
 - **Login Privilege**
5. To save the directory group changes, click **Update Group**.

More information

[Directory group privileges](#)

[Directory group settings](#)

Directory group settings

Each directory group includes a DN, SID, and account privileges. For Kerberos login, the SIDs of groups are compared to the SIDs for directory groups configured for iLO. If a user is a member of multiple groups, the user account is granted the privileges of all of the groups.

You can use global and universal groups to set privileges. Domain local groups are not supported.

When you add a directory group to iLO, configure the following values:

- **Group DN** (Security Group DN)—Members of this group are granted the privileges set for the group. The specified group must exist in the directory, and users who need access to iLO must be members of this group. Enter a DN from the directory (for example, CN=Group1, OU=Managed Groups, DC=domain, DC=extension).
Shortened DNs are also supported (for example, Group1). The shortened DN is not a unique match. Hewlett Packard Enterprise recommends using the fully qualified DN.
- **Group SID** (Security ID)—Microsoft Security ID is used for Kerberos and directory group authorization. This value is required for Kerberos authentication. The required format is S-1-5-2039349.

Deleting a directory group

Prerequisites

Configure iLO Settings privilege

Deleting a directory group

1. Navigate to the **Administration**→**User Administration** page.
2. Select the check box next to the directory group that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

5 Configuring iLO Federation

iLO Federation settings

iLO uses multicast discovery, peer-to-peer communication, and iLO Federation groups to communicate with other iLO systems.

When an iLO Federation page loads, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all of the data for the selected group is retrieved.

Configure the iLO Federation group and multicast settings on the **Administration→iLO Federation** page.

Prerequisites for using the iLO Federation features

- The network configuration meets the iLO Federation requirements.
- The multicast options are configured for each iLO system that will be added to an iLO Federation group.
If you use the default multicast option values, configuration is not required.
- iLO Federation group memberships are configured.
All iLO systems are automatically added to the **DEFAULT** group.
- Enclosure support for iLO Federation is configured in the Onboard Administrator software (ProLiant server blades only).
This setting is enabled by default.

iLO Federation network requirements

- Servers that will be used with iLO Federation must use the iLO Dedicated Network Port configuration. The iLO Federation features cannot be used with the iLO Shared Network Port configuration.
- Optional: iLO Federation supports both IPv4 and IPv6. If both options have valid configurations, you can configure iLO to use IPv4 instead of IPv6. To configure this setting, clear the **iLO Client Applications use IPv6 first** check box on the **Network→iLO Dedicated Network Port→IPv6** page.
- Configure the network to forward multicast traffic if you want to manage iLO systems in multiple locations.
- Ensure that multicast traffic is enabled if the switches in your network include the option to enable or disable it. This configuration is required for iLO Federation and other Hewlett Packard Enterprise products to discover the iLO systems on the network.
- For iLO systems that are separated by Layer 3 switches, configure the switches to forward SSDP multicast traffic between networks.
- Configure the network to allow multicast traffic (UDP port 1900) and direct HTTP (TCP default port 80) communication between iLO systems.
- For networks with multiple VLANs, configure the switches to allow multicast traffic between the VLANs.
- For networks with Layer 3 switches:
 - For IPv4 networks: Enable PIM on the switch and configure it for PIM Dense Mode.
 - For IPv6 networks: Configure the switch for MLD snooping.

Configuring the multicast options for one iLO system at a time

Use the following procedure to configure the multicast options for each iLO system that will be added to an iLO Federation group. If you use the default values, configuration is not required.

You can use RIBCL scripts to view and configure multicast options for multiple iLO systems. For more information, see the iLO Federation user guide.

Prerequisites

Configure iLO Settings privilege

Configuring the multicast options

1. Navigate to the **Administration**→**iLO Federation** page.
2. For **iLO Federation Management**, select **Enabled** or **Disabled**.
3. For **Multicast Discovery**, select **Enabled** or **Disabled**.
4. Enter a value for **Multicast Announcement Interval (seconds/minutes)**.
5. Select a value for **IPv6 Multicast Scope**.

To ensure that multicast discovery works correctly, make sure that all iLO systems in the same group use the same value for **IPv6 Multicast Scope**.

6. Enter a value for **Multicast Time To Live (TTL)**.

To ensure that multicast discovery works correctly, make sure that all iLO systems in the same group use the same value for **Multicast Time to Live (TTL)**.

7. Click **Apply**.

Network changes and changes you make on this page take effect after the next multicast announcement.

Multicast options

Multicast Options	
iLO Federation Management	Enabled
Multicast Discovery *	Enabled
Multicast Announcement Interval (seconds/minutes) *	5m
IPv6 Multicast Scope	Site
Multicast Time To Live (TTL)	5

Apply

- **iLO Federation Management**—Enables or disables the iLO Federation features. The default setting is **Enabled**. Selecting **Disabled** disables the iLO Federation features for the local iLO system.
- **Multicast discovery**—Enables or disables multicast discovery. The default setting is **Enabled**. Selecting **Disabled** disables the iLO Federation features for the local iLO system. Disabling multicast discovery is not supported on Synergy compute modules. To limit the impact of multicast traffic on a network with Synergy compute modules, adjust the **IPv6 Multicast Scope** and **Multicast Time To Live (TTL)** settings.
- **Multicast Announcement Interval (seconds/minutes)**—Sets the frequency at which the iLO system announces itself on the network. Each multicast announcement is approximately

300 bytes. Select a value of 30 seconds to 30 minutes. The default value is 10 minutes. Selecting **Disabled** disables the iLO Federation features for the local iLO system.

- **IPv6 Multicast Scope**—The size of the network that will send and receive multicast traffic. Valid values are **Link**, **Site**, and **Organization**. The default value is **Site**.
- **Multicast Time To Live (TTL)**—Specifies the number of switches that can be traversed before multicast discovery stops. The default value is 5.

iLO Federation groups

iLO Federation group characteristics

iLO Federation groups allow iLO systems to encrypt and sign messages to other iLO systems in the same group.

- All iLO systems are automatically added to the **DEFAULT** group, which is granted the Login privilege for each group member. You can edit or delete the **DEFAULT** group membership.
- iLO Federation groups can overlap, span racks and data centers, and can be used to create management domains.
- An iLO system can be a member of up to 10 iLO Federation groups.
- There is no limit on the number of iLO systems that can be in a group.
- You must have the Configure iLO Settings privilege to configure group memberships.
- You can use the iLO web interface to configure group memberships for a local iLO system or a group of iLO systems.
- You can use RIBCL XML scripts to view and configure group memberships.
For more information, see the iLO Federation user guide.
- You can use the iLO RESTful API to configure group memberships.
For more information, see the iLO RESTful API documentation at the following website:
<http://www.hpe.com/support/restfulinterface/docs>.
- Hewlett Packard Enterprise recommends installing the same version of the iLO firmware on iLO systems that are in the same iLO Federation group.

iLO Federation group memberships for local iLO systems

When you configure group memberships for a local iLO system, you specify the privileges that members of a group have for configuring the local managed server.

For example, if you add the local iLO system to **group1** and assign the Virtual Power and Reset privilege, the users of other iLO systems in **group1** can change the power state of the managed server.

If the local iLO system does not grant the Virtual Power and Reset privilege to **group1**, the users of other iLO systems in **group1** cannot use the group power control features to change the power state of the managed server.

If the system maintenance switch is set to disable iLO security on the local iLO system, the users of other iLO systems in **group1** can change the state of the managed server, regardless of the assigned group privileges.

Group memberships for the local iLO system are configured on the **Administration**→**iLO Federation** page.

You can perform the following tasks for a local iLO system:

- View group memberships.
- Add and edit group memberships.
- Remove group memberships.

More information

[Managing iLO Federation group memberships \(local iLO system\)](#)

[Adding iLO Federation group memberships \(local iLO system\)](#)

[Editing iLO Federation group memberships \(local iLO system\)](#)

[Removing a local iLO system from an iLO Federation group](#)

iLO Federation group memberships for a set of iLO systems

When you add group memberships for multiple iLO systems at one time, you specify the privileges that members of the group have for configuring the other members of the group.

For example, if you configure **group2** based on the **DEFAULT** group, and you assign the Virtual Power and Reset privilege, the users of iLO systems in **group2** can change the power state of all of the servers in the group.

You can add group memberships for multiple iLO systems on the **iLO Federation→Group Configuration** page.

You can perform the following tasks for a group of iLO systems:

- Create a group with the same members as an existing group, but with different privileges.
- Create a group with members that you select by using the iLO Federation filters.

More information

[Adding iLO Federation group memberships \(multiple iLO systems\)](#)

iLO Federation group privileges

When an iLO system added to a group, the group can be granted the following privileges:

-  **Login Privilege**—Group members can log in to iLO.
-  **Remote Console Access**—Group members can remotely access the managed server Remote Console, including video, keyboard, and mouse control.
-  **Virtual Media**—Group members can use scripted Virtual Media with the managed server.
-  **Virtual Power and Reset**—Group members can power-cycle or reset the managed server.
-  **Configure iLO Settings**—Group members can configure most iLO settings, including security settings, and can remotely update firmware.
-  **Administer User Accounts**—Group members can add, edit, and delete iLO user accounts.

Managing iLO Federation group memberships (local iLO system)

Viewing iLO Federation group memberships (local iLO system)

Navigate to the **Administration→iLO Federation** page.

The **Group Membership for this iLO** table lists the name of each group that includes the local iLO system, and the privileges granted to the group by the local iLO system.

Group Membership for this iLO						
Group						
<input type="checkbox"/> CloneClub						
<input type="checkbox"/> DEFAULT						
<input type="checkbox"/> Test						

[Join Group](#) [Edit](#) [Delete](#)

You can also use RIBCL scripts to view information about groups. For more information, see the iLO Federation user guide.

More information

[iLO Federation group privileges](#)

Adding iLO Federation group memberships (local iLO system)

Prerequisites

Configure iLO Settings privilege

Adding a group membership

1. Navigate to the **Administration**→**iLO Federation** page.
2. Click **Join Group**.
3. Enter the following information on the **Add/Edit Federation Group** page:
 - **Group Name**—The group name, which can be 1 to 31 characters long.
 - **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
 - **Group Key Confirm**—Confirm the group password.

If you enter the name and key for an existing group, the local iLO system is added to that group. If you enter the name and key for a group that does not exist, the group is created and the local iLO system is added to the new group.

4. Select from the following privileges:
 - **Administer User Accounts**
 - **Remote Console Access**
 - **Virtual Power and Reset**
 - **Virtual Media**
 - **Configure iLO Settings**
 - **Login Privilege**

The privileges granted to the group by the local iLO system control the tasks that users of other iLO systems in the group can perform on the managed server.

5. Click **Join Group**.

More information

[iLO Federation settings](#)

[Adding iLO Federation group memberships \(multiple iLO systems\)](#)

[iLO Federation groups](#)

[Access options](#)

Editing iLO Federation group memberships (local iLO system)

Prerequisites

Configure iLO Settings privilege

Editing a group membership

1. Navigate to the **Administration**→**iLO Federation** page.
2. Select a group membership, and then click **Edit** to open the **Add/Edit Federation Group** page.
3. To change the group name, enter a new name in the **Group Name** box.
The group name can be 1 to 31 characters long.
4. To change the group key, enter a new value in the **Group Key** and **Group Key Confirm** boxes.
The group key can be from the configured minimum password length to 31 characters long.
5. Select or clear the check boxes for the privileges you want to update.
The privileges granted to the group by the local iLO system control the tasks that users of other iLO systems in the group can perform on the managed server.
6. Click **Update Group**.

More information

[iLO Federation settings](#)

[iLO Federation groups](#)

Removing a local iLO system from an iLO Federation group

Prerequisites

Configure iLO Settings privilege

Removing a group membership

1. Navigate to the **Administration**→**iLO Federation** page.
2. Select the check box next to the group membership that you want to delete.
3. Click **Delete**.
4. When prompted to confirm the request, click **OK**.

Adding iLO Federation group memberships (multiple iLO systems)

Adding an iLO Federation group based on an existing group

Use this procedure to create an iLO Federation group with the same members as an existing group. For example, you might want to create a group that contains the same systems that are in the **DEFAULT** group, but with additional privileges.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Adding a group membership

1. Navigate to the **iLO Federation**→**Group Configuration** page.

If no iLO Federation groups exist, this page displays the following message: There are no configured groups. Use the **Administration**→**iLO Federation** page to create a group.

2. Select a group from the **Selected Group** menu.

All of the systems in the selected group will be added to the group you create on this page.

3. Enter the following information:

- **Group Name**—The group name, which can be 1 to 31 characters long.
- **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
- **Group Key Confirm**—Confirm the group password.

If you enter the name of a group that exists, iLO prompts you to enter a unique group name.

4. Select from the following privileges:

- **Administer User Accounts**
- **Remote Console Access**
- **Virtual Power and Reset**
- **Virtual Media**
- **Configure iLO Settings**
- **Login Privilege**

This step defines the privileges that members of the group have for configuring the other members of the group.

5. Optional: Enter the **Login Name** and **Password** for a user account on the remote systems you want to manage.

This information is required if the selected group does not have the Configure iLO Settings privilege on the remote systems you want to manage.

To enter credentials for multiple remote systems, create a user account with the same login name and password on each system.

6. Click **Create Group**.

The group creation process takes a few minutes. The group will be fully populated within the amount of time configured for the **Multicast Announcement Interval**.

More information

[iLO Federation group privileges](#)

[Adding iLO Federation group memberships \(local iLO system\)](#)

[Configuring the multicast options for one iLO system at a time](#)

[Access options](#)

Creating a group from a filtered set of servers

Use this procedure to create an iLO Federation group from a list of filtered servers. For example, you might want to create a group that contains all of the servers with a specific version of the iLO 4 firmware.

When you create a group from a list of filtered servers, only the servers listed in the **Affected Systems** list at the time the group is created are added to the group. If you configure servers that meet the filter criteria after the group is created, they are not added to the group.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Creating a group

1. Create a set of systems by using the filters on the **iLO Federation** pages.

2. Navigate to the **iLO Federation**→**Group Configuration** page.

The filters you apply when you create a set of systems are listed at the top of the page. To remove a filter, click the X icon.



If no iLO Federation groups exist, this page displays the following message: There are no configured groups. Use the **Administration**→**iLO Federation** page to create a group.

3. Select a group from the **Selected Group** menu.

All of the systems in the selected group that meet the selected filter criteria will be added to the new group.

4. Enter the following information:

- **Group Name**—The group name, which can be 1 to 31 characters long.
- **Group Key**—The group password, which can be from the configured minimum password length to 31 characters long.
- **Group Key Confirm**—Confirm the group password.

5. Select from the following privileges:

- **Administer User Accounts**
- **Remote Console Access**
- **Virtual Power and Reset**
- **Virtual Media**
- **Configure iLO Settings**
- **Login Privilege**

This step defines the privileges that members of the group have for configuring the other members of the group.

6. Optional: Enter the **Login Name** and **Password** for a user account on the remote systems you want to manage.

This information is required if the selected group does not have the Configure iLO Settings privilege on the remote systems you want to manage.

To enter credentials for multiple remote systems, create a user account with the same login name and password on each system.

7. To save the configuration, click **Create Group**.

The group creation process takes a few minutes. The group will be fully populated within the amount of time configured for the **Multicast Announcement Interval**.

More information

[Selected Group list filters](#)

[Adding iLO Federation group memberships \(local iLO system\)](#)

[iLO Federation group privileges](#)

[Access options](#)

Servers affected by a group membership change

The **Affected Systems** section on the **Group Configuration** page provides the following details about the servers affected when you make a group membership change:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More information

[Exporting iLO Federation information to a CSV file](#)

Configuring Enclosure iLO Federation Support

If you want to use the iLO Federation features with server blades in a BladeSystem c-Class enclosure, the **Enclosure iLO Federation Support** setting must be enabled in the Onboard Administrator software. This setting is required to allow peer-to-peer communication between the server blades in an enclosure. **Enclosure iLO Federation Support** is enabled by default.

Prerequisites

Onboard Administrator 4.11 or later is installed.

Configuring Enclosure iLO Federation Support

1. Log in to the Onboard Administrator web interface (<https://<OA hostname or IP address>>).
2. Navigate to the **Enclosure Information**→**Enclosure Settings**→**Network Access** page, and then click the **Protocols** tab.

3. Select the **Enable Enclosure iLO Federation Support** check box, and then click **Apply**.

Protocol Restrictions: *These protocol settings can be used to deny or allow access to the enclosure*

Enable Web Access (HTTP/HTTPS)
 Enable Secure Shell
 Enable Telnet
 Enable XML Reply [\(view\)](#)
 Enable Enclosure iLO Federation Support
Enclosure-enabled iLO Federation bays: 1
 Enable FQDN link support for accessing iLOs and interconnects [?](#)

Apply

TIP: You can also use the CLI to enable or disable the **Enable Enclosure iLO Federation Support** setting. To enable the setting, enter `ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`. To disable the setting, enter `DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`. For more information, see the Onboard Administrator CLI user guide.

Verifying server blade support for iLO Federation

1. Log in to the Onboard Administrator web interface (<https://<OA hostname or IP address>>).
2. Navigate to the **Device Bays**→<Device Name>→**iLO** page.
3. Verify that **iLO Federation Capable** is set to **Yes**.

Management Processor Information	
Name	
Address	
MAC Address	
Model	[Unknown]
Firmware Version	2.50
iLO Federation Capable	Yes

6 Configuring iLO access settings

iLO access settings

You can modify iLO access settings, including service settings and access options.

The values you enter on the **Access Settings** page apply to all iLO users.

The default access settings values are suitable for most environments. The values you can modify on the **Access Settings** page allow customization of the iLO external access methods for specialized environments.

Configuring iLO service settings

Prerequisites

Configure iLO Settings privilege

Configuring the service settings

The TCP/IP ports used by iLO are configurable, which enables compliance with site requirements and security initiatives for port settings. These settings do not affect the host system. The range of valid port values in iLO is from 1 to 65535. If you enter the number of a port that is in use, iLO prompts you to enter a different value.

Changing these settings usually requires configuration of the web browser used for standard and SSL communication. When these settings are changed, iLO initiates a reset to activate the changes.

1. Navigate to the **Administration**→**Access Settings** page.
2. Click the **Access Settings** tab.
3. Update the service settings as needed.
4. To end your browser connection and restart iLO, click **Apply**.

It might take several minutes before you can re-establish a connection.

Service settings

Service	
Secure Shell (SSH) Access	Enabled ▾
Secure Shell (SSH) Port	22
Remote Console Port	17990
Web Server Non-SSL Port	80
Web Server SSL Port	443
Virtual Media Port	17988
SNMP Access	Enabled ▾
SNMP Port	161
SNMP Trap Port	162
IPMI/DCMI over LAN Access	Enabled ▾
IPMI/DCMI over LAN Port	623

Apply

You can configure the following settings in the **Service** section on the **Access Settings** page.

- **Secure Shell (SSH) Access**—Allows you to enable or disable the SSH feature. SSH provides encrypted access to the iLO CLP. The default value is Enabled.
- **Secure Shell (SSH) Port**—The default value is 22.
- **Remote Console Port**—The default value is 17990.
- **Web Server Non-SSL Port (HTTP)**—The default value is 80.
- **Web Server SSL Port (HTTPS)**—The default value is 443.
- **Virtual Media Port**—The default value is 17988.
- **SNMP Access**—Specifies whether iLO responds to external SNMP requests. The default value is Enabled.

If you set **SNMP Access** to Disabled, iLO continues to operate, and the information displayed in the iLO web interface is updated. In this state, no alerts are generated and SNMP access is not permitted. When **SNMP Access** is set to Disabled, most of the boxes on the **Administration**→**Management**→**SNMP Settings** page are unavailable and will not accept input.
- **SNMP Port**—The industry-standard (default) SNMP port is 161 for SNMP access.

If you customize the **SNMP Port** value, some SNMP clients might not work correctly with iLO unless those clients support the use of a nonstandard SNMP port.
- **SNMP Trap Port**—The industry-standard (default) SNMP trap port is 162 for SNMP alerts (or traps).

If you customize the **SNMP Trap Port**, some SNMP monitoring applications (like HPE SIM) might not work correctly with iLO unless those applications support the use of a nonstandard SNMP trap port.

To use SNMP v3 with HPE SIM 7.2 or later, change the **SNMP Trap Port** value to 50005.

- **IPMI/DCMI over LAN Access**—Allows you to send industry-standard IPMI and DCMI commands over the LAN. The default value is Enabled.

If you set this value to Disabled, iLO disables IPMI/DCMI over the LAN. Server-side IPMI/DCMI applications are still functional when this option is disabled.

If you set this value to Enabled, iLO allows you to use a client-side application to send IPMI/DCMI commands over the LAN.
- **IPMI/DCMI over LAN Port**—Sets the IPMI/DCMI port number. The default value is 623.

Configuring iLO access options

Prerequisites

Configure iLO Settings privilege

Configuring access options

1. Navigate to the **Administration**→**Access Settings** page.
2. Click the **Access Settings** tab.
3. Update the access options as needed.
4. Click **Apply**.

If you set the **iLO Functionality** setting to **Disabled**, clicking **Apply** ends your browser connection and restarts iLO.

It might take several minutes before you can re-establish a connection.

Access options

Access Options	
Idle Connection Timeout (minutes)	120
iLO Functionality	Enabled
iLO ROM-Based Setup Utility	Enabled
Require Login for iLO RBSU	Disabled
Show iLO IP during POST	Enabled
Serial Command Line Interface Status	Enabled - Authentication Required
Serial Command Line Interface Speed	9600
Virtual Serial Port Log	Disabled
Minimum Password Length	5
Server Name	
Server FQDN / IP Address	
Authentication Failure Logging	Disabled
Authentication Failure Delay Time	2 seconds
Authentication Failures Before Delay	5 Failures cause no delay

Apply

You can configure the following settings in the **Access Options** section on the **Access Settings** page.

Idle Connection Timeout (minutes)

This setting specifies how long a user can be inactive before an iLO web interface or Remote Console session ends automatically.

The iLO web interface and the Remote Console track idle time separately because each connection is a separate session. This setting has no effect on a Remote Console session if a Virtual Media device is connected.

The following values are valid:

- **15, 30, 60, or 120 minutes**—The default value is 30 minutes.
- **Infinite**—Inactive users are not logged out.

Failure to log out of iLO by either browsing to a different site or closing the browser also results in an idle connection. The iLO firmware supports a finite number of connections. Misuse of the **Infinite** timeout option might make iLO inaccessible to other users. Idle connections are recycled after they time out.

This setting applies to local and directory users. Directory server timeout settings might preempt the iLO setting.

Changes to the setting might not take effect immediately in current user sessions, but will be enforced immediately in all new sessions.

iLO Functionality

This setting specifies whether iLO functionality is available.

The following settings are valid:

- **Enabled** (default)—The iLO network is available and communications with operating system drivers are active.
- **Disabled**—The iLO network and communications with operating system drivers are terminated when **iLO Functionality** is disabled.

For ProLiant Gen8 servers only: To re-enable iLO functionality, disable iLO security with the system maintenance switch, and then use the iLO RBSU to set **iLO Functionality** to **Enabled**.

For more information about using the system maintenance switch, see the maintenance and service guide for your server model.

For ProLiant Gen9 servers only: To re-enable iLO functionality, use the iLO 4 Configuration Utility (in the UEFI System Utilities) to set **iLO Functionality** to **Enabled**. For more information, see the UEFI System Utilities user guide.

NOTE: iLO functionality cannot be disabled on ProLiant server blades or Synergy compute modules.

iLO ROM-Based Setup Utility

This setting enables or disables the iLO RBSU or the iLO 4 Configuration Utility. The following settings are valid:

- **Enabled** (default)—On servers that support the iLO RBSU, pressing **F8** during POST starts the iLO RBSU. On servers that support UEFI, the iLO 4 Configuration Utility is available when you access the UEFI System Utilities.
- **Disabled**—On servers that support the iLO RBSU, pressing **F8** during POST will not start the iLO RBSU. On servers that support UEFI, the iLO 4 Configuration Utility is not available when you access the UEFI System Utilities.

This setting cannot be set to **Enabled** if option ROM prompting is disabled in the system BIOS.

NOTE: This option is called **iLO 4 Configuration Utility** in the UEFI System Utilities.

Require Login for iLO RBSU

This setting determines whether a user-credential prompt is displayed when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.

The following settings are valid:

- **Enabled**—A login dialog box opens when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.
- **Disabled** (default)—No login is required when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.

NOTE: This option is called **Require Login for iLO 4 Configuration** in the UEFI System Utilities.

Show iLO IP during POST

This setting enables the display of the iLO network IP address during host server POST. The following settings are valid:

- **Enabled** (default)—The iLO IP address is displayed during POST.
- **Disabled**—The iLO IP address is not displayed during POST.

Serial Command Line Interface Status

This setting enables you to change the login model of the CLI feature through the serial port. The following settings are valid:

- **Enabled-Authentication Required** (default)—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. Valid iLO user credentials are required.
- **Enabled-No Authentication**—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. iLO user credentials are not required.
- **Disabled**—Disables access to the SMASH CLP command line from the host serial port. Use this option if you are planning to use physical serial devices.

Serial Command Line Interface Speed

This setting enables you to change the speed of the serial port for the CLI feature.

The following speeds (in bits per second) are valid:

- **9600** (default)
- **19200**
- **38400**—iLO RBSU and the iLO 4 Configuration Utility do not support this value.
- **57600**
- **115200**

! **IMPORTANT:** For Synergy compute modules only: Ensure that this value is set to 9600. If you use another value, you cannot access the Serial Command Line Interface from the Synergy Console and Composer CLI.

The serial port configuration must be set to no parity, eight data bits, and one stop bit (N/8/1) for correct operation.

Set this value to match the serial port speed configured in the iLO RBSU or the iLO 4 Configuration Utility.

Virtual Serial Port Log

This setting enables or disables logging of the Virtual Serial Port.

The following settings are valid:

- **Enabled**—When enabled, Virtual Serial Port activity is logged to a 150-page circular buffer in the iLO memory, and can be viewed using the CLI command `vsp log`. The Virtual Serial Port buffer size is 128 KB.
- **Disabled** (default)—Virtual Serial Port activity is not logged.

This feature is part of a licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Minimum Password Length

This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length must be a value from 0 to 39 characters long. The default value is 8.

Server Name

This setting enables you to specify the host server name. You can assign this value manually, but it might be overwritten by the host software when the operating system loads.

- You can enter a server name that is up to 49 bytes.
- To force the browser to refresh and display the new value, save this setting, and then press **F5**.

Server FQDN/IP Address

This setting enables you to specify the server FQDN or IP address. You can assign this value manually, but it might be overwritten by the host software when the operating system loads.

- You can enter an FQDN or IP address that is up to 255 bytes.
- To force the browser to refresh and display the new value, save this setting, and then press **F5**.

Authentication Failure Logging

This setting enables you to configure logging criteria for failed authentications. The following settings are valid:

- **Enabled-Every Failure**—A failed login log entry is recorded after every failed login attempt.
- **Enabled-Every 2nd Failure**—A failed login log entry is recorded after every second failed login attempt.
- **Enabled-Every 3rd Failure** (default)—A failed login log entry is recorded after every third failed login attempt.
- **Enabled-Every 5th Failure**—A failed login log entry is recorded after every fifth failed login attempt.
- **Disabled**—No failed login log entry is recorded.

For information about using this setting with SSH clients, see [“iLO login with an SSH client” \(page 67\)](#).

Authentication Failure Delay Time

This setting enables you to configure the duration of the iLO login delay after a failed login attempt. The following values are valid: 2, 5, 10, and 30 seconds.

The default value is 10 seconds.

This feature is supported in iLO 4 2.20 and later.

Authentication Failures Before Delay

This setting enables you to configure the number of failed login attempts that are allowed before iLO imposes a login delay. The following values are valid: 1, 3, 5, or every failed login attempt.

When you upgrade from an earlier version of the iLO firmware to iLO 4 2.20 or later, the default value is every failed login attempt. With this setting, a login delay is imposed after the first failed login attempt.

When you use a server that shipped with iLO 4 2.20 or later, or you reset the iLO 2.20 or later firmware to the factory default settings, the default value is 1. With this configuration, a login delay is not imposed until the second failed login attempt.

This feature is supported in iLO 4 2.20 and later.

iLO login with an SSH client

When you log in to iLO with an SSH client, the number of displayed login prompts matches the value of the **Authentication Failure Logging** option (3 if it is disabled). Your SSH client configuration might affect the number of prompts, because SSH clients also implement delays after a login failure.

For example, to generate an SSH authentication failure log with the default value (**Enabled-Every 3rd Failure**), if the SSH client is configured with the number of password prompts set to three, three consecutive login failures occur as follows:

1. Run the SSH client and log in with an incorrect login name and password.
You receive three password prompts. After the third incorrect password, the connection ends and the first login failure is recorded. The SSH login failure counter is set to 1.
2. Run the SSH client and log in with an incorrect login name and password.
You receive three password prompts. After the third incorrect password, the connection ends and the second login failure is recorded. The SSH login failure counter is set to 2.
3. Run the SSH client and log in with an incorrect login name and password.
You receive three password prompts. After the third incorrect password, the connection ends and the third login failure is recorded. The SSH login failure counter is set to 3.

The iLO firmware records an SSH failed login log entry, and sets the SSH login failure counter to 0.

7 Configuring the iLO security features

iLO security features

iLO provides the following security features:

- [User-defined TCP/IP ports](#).
- [User actions logged in the iLO Event Log](#).
- [Progressive delays for failed login attempts](#).
- [Support for X.509 CA signed certificates](#).
- [Support for securing iLO RBSU and the iLO 4 Configuration Utility](#).
- [Encrypted communication that uses SSL certificate administration](#).
- [Support for Kerberos authentication and directory services](#).

General security guidelines for iLO

- For maximum security, configure iLO on a separate management network. For more information, see [“Connecting iLO to the network” \(page 27\)](#).
- Do not connect iLO directly to the Internet.
- Use a browser that supports a 128-bit cipher.

iLO RBSU and iLO 4 Configuration Utility security

iLO RBSU and the iLO 4 Configuration Utility enable you to view and modify the iLO configuration. You can configure iLO RBSU and iLO 4 Configuration Utility login and access settings by using iLO RBSU, the iLO 4 Configuration Utility, the iLO web interface, or RIBCL scripts. If the system maintenance switch is set to disable iLO security, any user can access iLO RBSU or the iLO 4 Configuration Utility, regardless of the configured access settings.

iLO RBSU and the iLO 4 Configuration Utility have the following security levels:

- **Login Not Required** (default)

Anyone who has access to the host during POST can enter iLO RBSU or the iLO 4 Configuration Utility to view and modify configuration settings. This setting is acceptable if host access is controlled. If host access is not controlled, any user can make configuration changes by using the active configuration menus.

- **Login Required** (more secure)

If iLO RBSU or iLO 4 Configuration Utility login is required, only users with the correct access privileges can access the active configuration menus.

- **Disabled** (most secure)

If iLO RBSU or the iLO 4 Configuration Utility is disabled, user access is prohibited. This configuration prevents modification by using the iLO RBSU or the iLO 4 Configuration Utility.

More information

[iLO access settings](#)

[iLO ROM-based utilities](#)

[iLO security with the system maintenance switch](#)

iLO security with the system maintenance switch

The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control over the server system board. Disabling iLO security allows login access with all privileges, without a user ID and password.

The system maintenance switch is located inside the server and cannot be accessed without opening the server enclosure. When you work with the system maintenance switch, ensure that the server is powered off and disconnected from the power source. Set the switch to enable or disable iLO security, and then power on the server.

The system maintenance switch position that controls iLO security is sometimes called the *iLO Security Override switch*.

Reasons to disable iLO security

- iLO functionality is disabled and must be re-enabled (Gen8 servers only).
- All user accounts that have the Administer User Accounts privilege are locked out.
- An invalid configuration prevents iLO from being displayed on the network, and iLO RBSU or the iLO 4 Configuration Utility is disabled.
- The boot block must be flashed.

Hewlett Packard Enterprise does not anticipate that you will need to update the boot block. If an update is required, you must be physically present at the server to reprogram the boot block and reset iLO. The boot block is exposed until iLO is reset. For maximum security, Hewlett Packard Enterprise recommends disconnecting iLO from the network until the reset is complete.

- The iLO NIC is turned off, and it is not possible or convenient to run iLO RBSU or the iLO 4 Configuration Utility to turn it back on.
- Only one user name is configured, and the password is forgotten.

Effects of disabling iLO security

- All security authorization verifications are disabled.
- If the host server is reset, iLO RBSU or the iLO 4 Configuration Utility runs.
- iLO is not disabled and might be displayed on the network as configured.
- If iLO functionality is disabled, iLO does not log out active users and complete the disable process until the power is cycled on the server.
- The boot block is exposed for programming.
- A warning message is displayed on iLO web interface pages, indicating that iLO security is disabled.
- An iLO log entry is added to record the iLO security change.
- If an SNMP Alert Destination is configured, an SNMP alert is sent when iLO starts after you use the system maintenance switch to enable or disable iLO security.

For information about how to enable and disable iLO security with the system maintenance switch, see the maintenance and service guide for your server.

TPM and TM

Trusted Platform Modules and Trusted Modules are computer chips that securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM or TM to store platform measurements to make sure that the platform remains trustworthy.

On a supported system, ROM decodes the TPM or TM record and passes the configuration status to iLO, the iLO RESTful API, the CLP, and the XML interface.

Viewing the TPM or TM status

Navigate to the **Information**→**Overview** page.

TPM or TM status values

- **Not Supported**—A TPM or TM is not supported.
- **Not Present**—A TPM or TM is not installed.
- **Present** (Gen8 servers)—This value indicates one of the following statuses:
 - A TPM or TM is installed and disabled.
 - A TPM or TM is installed and enabled.
 - A TPM or TM is installed and enabled, and Option ROM Measuring is enabled.
- **Present-Enabled** (Gen9 servers)—A TPM or TM is installed and enabled.

User accounts and access

iLO supports the configuration of up to 12 local user accounts. Each account can be managed through the following features:

- Privileges
- Login security

You can configure iLO to use a directory to authenticate and authorize its users. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise. The directory also provides a central point of administration for iLO devices and users, and the directory can enforce a stronger password policy. iLO enables you to use local users, directory users, or both.

The following directory configuration options are available:

- A directory extended with Hewlett Packard Enterprise schema
- The directory default schema

More information

[Managing user accounts and directory groups](#)

[Kerberos authentication and Directory services](#)

User privileges

iLO allows you to control user account access to iLO features through the use of privileges. When a user attempts to use a feature, iLO verifies that the user has the required privilege to use that feature.

More information

[iLO user privileges](#)

Login security

iLO provides the following login security features:

- **iLO 4 versions earlier than 2.20**—After an initial failed login attempt, iLO imposes a delay of 10 seconds. Each subsequent failed attempt increases the delay by 10 seconds. A

message is displayed during each delay; this behavior continues until a valid login occurs. This feature helps to prevent dictionary attacks against the browser login port.

- **iLO 4 version 2.20 and later**—iLO can be configured to impose a delay after a configured number of failed login attempts. Each subsequent failed attempt increases the delay by the configured number of seconds. A message is displayed during each delay; this behavior continues until a valid login occurs. This feature helps to prevent dictionary attacks against the browser login port. You can configure the login delay settings on the **Administration→Access Settings** page.
- iLO saves a detailed log entry for failed login attempts. You can configure the Authentication Failure Logging frequency on the **Administration→Access Settings** page.

More information

[iLO access settings](#)

Administering SSH keys

The **Secure Shell Key** page displays the hash of the SSH public key associated with each user. Each user can have only one key assigned. Use this page to view, add, or delete SSH keys.

Authorizing a new SSH key by using the web interface

Prerequisites

Administer User Accounts privilege

Authorizing a new key with the iLO web interface

1. Generate a 2,048-bit DSA or RSA key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Navigate to the **Administration→Security** page.
4. Click the **Secure Shell Key** tab.
5. Select the check box to the left of the user to which you want to add an SSH key.

Authorized SSH Keys		
Login Name	User Name	Public Key Hash
<input type="checkbox"/>	Administrator	<No SSH public key installed>
<input checked="" type="checkbox"/>	admin	<No SSH public key installed>
Authorize New Key		Delete Selected Key(s)

6. Click **Authorize New Key**.
7. Copy and paste the public key into the **Public Key Import Data** box.

Public Key Import Data

Paste the PEM encoded public key in the area below, and click 'Import Public Key'

Import Public Key

The key must be a 2,048-bit DSA or RSA key.

8. Click **Import Public Key**.

More information

[SSH keys](#)

Authorizing a new SSH key by using the CLI

Prerequisites

Administer User Accounts privilege

Authorizing a new key with the CLI

1. Generate a 2,048-bit DSA or RSA SSH key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Verify that **Secure Shell (SSH) Access** is enabled on the **Access Settings** page.
4. Use `Putty.exe` to open an SSH session using port 22.
5. Change to the `cd /Map1/Config1` directory.
6. Enter the following command:

```
load sshkey type "oemhp_loadSSHkey -source
<protocol://username:password@hostname:port/filename>"
```

When you use this command:

- The protocol value is required and must be HTTP or HTTPS.
- The hostname and filename values are required.
- The `username:password` and `port` values are optional.
- `oemhp_loadSSHkey` is case-sensitive.

The CLI performs a cursory syntax verification of the values you enter. Visually verify that the URL is valid. The following example shows the command structure:

```
oemhp_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
```

More information

[SSH keys](#)

iLO access settings

Deleting SSH keys

Prerequisites

Administer User Accounts privilege

Deleting an SSH key

1. Navigate to the **Administration**→**Security** page.
2. Click the **Secure Shell Key** tab.
3. Select the check box to the left of the user for which you want to delete an SSH key.
4. Click **Delete Selected Key(s)**.

The selected SSH key is removed from iLO. When an SSH key is deleted from iLO, an SSH client cannot authenticate to iLO by using the corresponding private key.

Authorizing SSH keys from an HPE SIM server

The `mxagentconfig` utility enables you to authorize SSH keys from an HPE SIM server.

- SSH must be enabled on iLO before you use `mxagentconfig` to authorize a key.
- The user name and password entered in `mxagentconfig` must correspond to an iLO user who has the Configure iLO Settings privilege. The user can be a directory user or a local user.
- The key is authorized on iLO and corresponds to the user name specified in the `mxagentconfig` command.

For more information about `mxagentconfig`, see the iLO scripting and CLI guide.

More information

SSH keys

SSH keys

When you add an SSH key to iLO, you paste the SSH key file into iLO. The file must contain the user-generated public key. The iLO firmware associates each key with the selected local user account. If a user is removed after an SSH key is authorized for that user, the SSH key is removed.

The following SSH key formats are supported:

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuA1NLIivLFP3I0KZ
ZtzF0VInP5x2VFVYmTvdVjD92CT1xxAtarOPON2qUqoOajKrtBWlmxcfqsLCT3wI
3ldxQvPYnhTYyHPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgt8/UA
AAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAGCbnhADYXu+Mv4xuXccXWP0Pcj47
7Yizgos3jt/Z0ezFX6/cN/RwwZwPC1HcsMuwsVBIqi7bvn1XczFPK0t06gVWcjFt
eBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHg8Z
JazhY920PpkD4hNbAAAAGDN3lba1qFV10U1Rjj21MjXgr6em9TETSOO5b7SQ8hx/
Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYaiF
DLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtSTV
---- END SSH2 PUBLIC KEY ----
```

OpenSSH key format

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDI1I+RkA1UXjVS28hNSk8YDljTaJpw1V0lBirrLGPdSt0avNSz0DNQuU7gTPfjj/8c
XyHe3y950a3rics1fARYLiNFGqFjr7w2ByQuoYuaxBzggh1YMQcmprc/W/kDMC0dVof2XnfcLpcVDIm3ahVPRkxFV9WKKAAAAVAI
3J61F+oVKrbNovhoHh8pFFuA9LAAAAGA8pU5/M9F0s5QxqkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpA1xAp6eDZKFvj3ZIy
NjCQODeYYqOvVU45AkSkLBMGjpF05cVtnWEGEvrW7mAvtG2zwMEDFSREW/v526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxD
```

iLO legacy format

The iLO legacy format keys are OpenSSH keys surrounded by the BEGIN/END headers needed for RIBCL. This format must be one line between the BEGIN SSH KEY and END SSH KEY text.

```
-----BEGIN SSH KEY-----
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cm1asav6ApuCRET1UvP7qcmBw+sTDrx91V22Xvonw1jdFiOM/0VvuzVhM9cKdGMC7sCQr
FV3zWDMJc1b5ZdYQSDt44X6bvl5QcAR0wNGBN9zHL6YsbXvNAsXN7uBm7jXwHwrApWvGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQ
Dofa47q8p1Rdr6epnJXSNrwJrvaQAAIBY7Mka2uH8210KYTbNMi0o5m0qmcg+tg5s9GC+hvvYy/S7agpIdfJzqkpHF5EPbm0j
KzzVxmsan0+ppju71rE3xUxojevl0kTERSCM xLa+OVVbNcgTe0xpv/cF6ZvsHs0UWz6gXIMCQ9P118VM0w/tyLp42YXOaLZzG
fi5pKAAAIEA17Fs07sDbPj02a5j03qFx7621Wv5iPRZ9cEt5WJEYwMO/ICaJVDNVOpqF9spoNb53W11pUARJg1ss8Ruy7Yb
8Z1urWWAF3fYy7R/S1QqrSRYDPLM5eBkkL028B8C6++HjLuc+hBvj90tsqeNvhpcf09qrjYomYwnDC4m1TT4= ASmith
-----END SSH KEY-----
```

Note the following when working with SSH keys:

- The previously listed sample formats are supported with the iLO web interface and the CLI. Only the iLO legacy format is supported with RIBCL scripts.
- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.
- The iLO firmware provides storage to accommodate SSH keys that have a length of 1366 bytes or less. If the key is larger than 1366 bytes, the authorization might fail. If a failure occurs, use the SSH client software to generate a shorter key.
- If you use the iLO web interface to enter the public key, you select the user associated with the public key. If you use the CLI to enter the public key, the public key is linked to the user name that you entered to log in to iLO. If you use HPQLOCFG to enter the public key, you append the iLO user name to the public key data. The public key is stored with that user name.

More information

[Authorizing a new SSH key by using the web interface](#)

[Authorizing a new SSH key by using the CLI](#)

Administering SSL certificates

SSL protocol is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. This protocol uses a key to encrypt and decrypt the data. Generally, the longer the key, the better the encryption.

A certificate is a small data file that connects an SSL key to a server. It contains the name of the server and the server's public key. Only the server has the corresponding private key, and this is how it is authenticated.

A certificate must be signed to be valid. If it is signed by a CA, and that CA is trusted, all certificates signed by the CA are also trusted. A self-signed certificate is one in which the owner of the certificate acts as its own CA.

By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables iLO to work without additional configuration steps. Importing a trusted certificate can enhance the iLO security features. Users with the Configure iLO Settings privilege can customize and import a trusted certificate that is signed by a CA.

Viewing SSL certificate information

To view certificate information, navigate to the **Administration**→**Security**→**SSL Certificate** page.

SSL certificate details

- **Issued To**—The entity to which the certificate was issued
- **Issued By**—The CA that issued the certificate
- **Valid From**—The first date that the certificate is valid
- **Valid Until**—The date that the certificate expires
- **Serial Number**—The serial number that the CA assigned to the certificate

Obtaining and importing an SSL certificate

iLO allows you to create a Certificate Signing Request that you can send to a Certificate Authority to obtain a trusted SSL certificate to import into iLO.

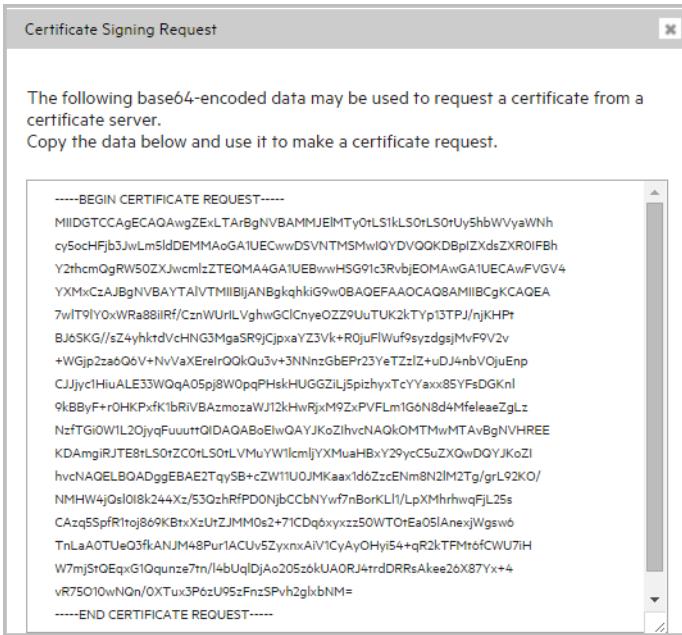
An SSL certificate works only with the keys generated with its corresponding CSR. If iLO is reset to the factory default settings, or another CSR is generated before the certificate that corresponds to the previous CSR is imported, the certificate does not work. In that case, a new CSR must be generated and used to obtain a new certificate from a CA.

Prerequisites

Configure iLO Settings privilege

Obtaining an SSL certificate

1. Navigate to the **Administration**→**Security**→**SSL Certificate** page.
2. Click **Customize Certificate**.
3. On the **SSL Certificate Customization** page, enter the following:
 - **Country (C)**
 - **State (ST)**
 - **City or Locality (L)**
 - **Organization Name (O)**
 - **Organizational Unit (OU)**
 - **Common Name (CN)**
4. Click **Generate CSR**.
A message notifies you that a certificate is being generated and that the process might take up to 10 minutes.
5. After a few minutes (up to 10), click **Generate CSR** again.
The CSR is displayed.



The CSR contains a public and private key pair that validates communications between the client browser and iLO. Key sizes up to 2,048 bits are supported. The generated CSR is held in memory until a new CSR is generated, iLO is reset to the factory default settings, or a certificate is imported.

6. Select and copy the CSR text.
7. Open a browser window and navigate to a third-party CA.
8. Follow the onscreen instructions and submit the CSR to the CA.

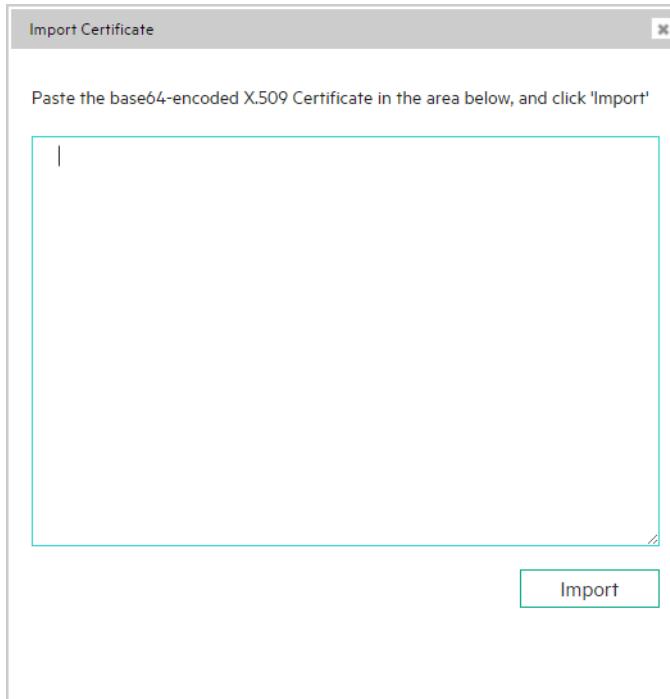
When you submit the CSR to the CA, your environment might require the specification of Subject Alternative Names (SAN). This information is typically included in the **Additional Attributes** box. If necessary, enter the iLO DNS short name and IP address in the **Additional Attributes** box by using the following syntax: `san : dns=<IP address>&dns=<server name>`.

The CA generates a certificate in PKCS #10 format.

9. After you obtain the certificate, make sure that:
 - The CN matches the iLO FQDN.
This value is listed as the **iLO Hostname** on the **Information→Overview** page.
 - The certificate is a Base64-encoded X.509 certificate.
 - The first and last lines are included in the certificate.

Importing a trusted certificate

1. Navigate to the **Administration→Security→SSL Certificate** page.
2. Click the **Import Certificate** button.



3. In the **Import Certificate** window, paste the certificate into the text box, and then click **Import**. iLO supports SSL certificates that are up to 3 KB (including the 609 bytes or 1,187 bytes used by the private key, for 1,024-bit and 2,048-bit certificates, respectively).
4. Reset iLO.
For instructions, see [“iLO diagnostics” \(page 193\)](#).

CSR input details

Enter the following details when you create a CSR:

- **Country (C)**—The two-character country code that identifies the country where the company or organization that owns this iLO subsystem is located. Enter the two-letter abbreviation in capital letters.
- **State (ST)**—The state where the company or organization that owns this iLO subsystem is located.
- **City or Locality (L)**—The city or locality where the company or organization that owns this iLO subsystem is located.
- **Organization Name (O)**—The name of the company or organization that owns this iLO subsystem.
- **Organizational Unit (OU)**—(Optional) The unit within the company or organization that owns this iLO subsystem.
- **Common Name (CN)**—The FQDN of this iLO subsystem.

The FQDN is entered automatically in the **Common Name (CN)** box.

You must configure the **Domain Name** on the **Network General Settings** page to enable iLO to enter the FQDN into the CSR.

More information

[Configuring NIC and TCP/IP settings \(iLO RBSU\)](#)

Directory authentication and authorization

The iLO firmware supports Kerberos authentication with Microsoft Active Directory. It also supports directory integration with an Active Directory server. When you configure directory integration, you can use the schema-free option or the HPE Extended Schema. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port.

Configuring the authentication and directory server settings is one step in the process of configuring iLO to use a directory or Kerberos authentication.

For information about setting up your environment to use these features, see [“Kerberos authentication and Directory services” \(page 278\)](#).

Prerequisites for configuring authentication and directory server settings

- Your iLO user account has the Configure iLO Settings privilege.
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- The environment is configured to support Kerberos authentication or directory integration. For more information, see [“Kerberos authentication and Directory services” \(page 278\)](#)
- The Kerberos keytab file is available (Kerberos authentication only).

Configuring Kerberos authentication settings in iLO

1. Navigate to the **Administration**→**Security**→**Directory** page.
2. Select the **Enabled** option for **Kerberos Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as Kerberos authentication.
4. Enter the **Kerberos Realm** name.
5. Enter the **Kerberos KDC Server Address**.
6. Enter the **Kerberos KDC Server Port**.
7. To add the Kerberos Keytab file, click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome), and then follow the onscreen instructions.
8. Click **Apply Settings**.

More information

[Local user accounts with Kerberos authentication and directory integration](#)

[Kerberos authentication and Directory services](#)

[Generating a keytab file for iLO in a Windows environment](#)

Kerberos settings

- **Kerberos Authentication**—This setting enables or disables Kerberos login. If Kerberos login is enabled and configured correctly, the **Zero Sign In** button appears on the login page.
- **Kerberos Realm**—The name of the Kerberos realm in which the iLO processor operates. This value can be up to 128 characters. The realm name is usually the DNS name converted to uppercase letters. Realm names are case-sensitive.
- **Kerberos KDC Server Address**—The IP address or DNS name of the KDC server. This value can be up to 128 characters. Each realm must have at least one KDC that contains an authentication server and a ticket grant server. These servers can be combined.

- **Kerberos KDC Server Port**—The TCP or UDP port number on which the KDC is listening. The default value is 88.
- **Kerberos Keytab**—A binary file that contains pairs of service principal names and encrypted passwords. In the Windows environment, you use the `ktpass` utility to generate the keytab file.

Configuring schema-free directory settings in iLO

1. Navigate to the **Administration**→**Security**→**Directory** page.
2. Select the **Use Directory Default Schema** option for **LDAP Directory Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as directory integration.
4. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.
5. Enter the directory server port number in the **Directory Server LDAP Port** box.
6. Enter valid search contexts in one or more of the **Directory User Context** boxes.
7. Click **Apply Settings**.
8. To test the communication between the directory server and iLO, click **Test Settings**.
9. Optional: To configure directory groups, click **Administer Groups** to navigate to the **User Administration** page.

More information

[Schema-free directory authentication](#)

[Local user accounts with Kerberos authentication and directory integration](#)

[Directory user contexts](#)

[Running directory tests](#)

Schema-free directory settings

- **Use Directory Default Schema**—Selects directory authentication and authorization by using user accounts in the directory. Select this option when the directory is not extended with the HPE Extended Schema. User accounts and group memberships are used to authenticate and authorize users.
- **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.
If you enter the FQDN, ensure that the DNS settings are configured in iLO.
Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.
- **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.
- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

Configuring HPE Extended Schema directory settings in iLO

1. Navigate to the **Administration**→**Security**→**Directory** page.
2. Select the **Use Extended Schema** option for **LDAP Directory Authentication**.
3. Select the **Enabled** option for **Local User Accounts** if you want to use local user accounts at the same time as directory integration.
4. Enter the FQDN or IP address of a directory server in the **Directory Server Address** box.

5. Enter the directory server port number in the **Directory Server LDAP Port** box.
6. Enter the location of this iLO instance in the directory tree in the **LOM Object Distinguished Name** box.
7. Enter valid search contexts in one or more of the **Directory User Context** boxes.
8. Click **Apply Settings**.
9. To test the communication between the directory server and iLO, click **Test Settings**.
10. Optional: To configure directory groups, click **Administer Groups** to navigate to the **User Administration** page.

More information

[HPE Extended Schema directory authentication](#)

[Local user accounts with Kerberos authentication and directory integration](#)

[Directory user contexts](#)

[Running directory tests](#)

HPE Extended Schema directory settings

- **Use HPE Extended Schema**—Selects directory authentication and authorization by using directory objects created with the HPE Extended Schema. Select this option when the directory has been extended with the HPE Extended Schema. The HPE Extended Schema works only with Microsoft Windows.
- **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.
If you enter the FQDN, ensure that the DNS settings are configured in iLO.
Hewlett Packard Enterprise recommends using DNS round-robin when you define the directory server.
- **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. If your directory service is configured to use a different port, you can specify a different value. Make sure that you enter a secured LDAP port. iLO cannot connect to an unsecured LDAP port.
- **LOM Object Distinguished Name**—Specifies where this iLO instance is listed in the directory tree (for example, `cn=Mail Server, ou=Management Devices, o=ab`). This option is available when **Use HPE Extended Schema** is selected.
User search contexts are not applied to the LOM object DN when iLO accesses the directory server.
- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

Directory user contexts

You can identify the objects listed in a directory by using unique DNs. However, DNs can be long, users might not know their DNs, or users might have accounts in different directory contexts.

When you use user contexts, iLO attempts to contact the directory service by DN, and then applies the search contexts in order until login is successful.

- **Example 1**—If you enter the search context `ou=engineering, o=ab`, you can log in as `user` instead of logging in as `cn=user, ou=engineering, o=ab`.
- **Example 2**—If the IM, Services, and Training departments manage a system, the following search contexts enable users in these departments to log in by using their common names:
Directory User Context 1:`ou=IM, o=ab`
Directory User Context 2:`ou=Services, o=ab`
Directory User Context 3:`ou=Training, o=ab`
If a user exists in both the IM organizational unit and the Training organizational unit, login is first attempted as `cn=user, ou=IM, o=ab`.
- **Example 3 (Active Directory only)**—Microsoft Active Directory allows an alternate user credential format. A user can log in as `user@domain.example.com`. Entering the search context `@domain.example.com` allows the user to log in as `user`. Only a successful login attempt can test search contexts in this format.

Local user accounts with Kerberos authentication and directory integration

Local user accounts can be active when you configure iLO to use a directory or Kerberos authentication. In this configuration, you can use local and directory-based user access.

Consider the following:

- When local user accounts are enabled, configured users can log in by using locally stored user credentials.
- When local accounts are disabled, user access is limited to valid directory credentials.
- Do not disable local user access until you have validated access through Kerberos or a directory.
- When you use Kerberos authentication or directory integration, Hewlett Packard Enterprise recommends enabling local user accounts and configuring a user account with administrator privileges. This account can be used if iLO cannot communicate with the directory server.
- Access through local user accounts is enabled when directory support is disabled or an iLO license is revoked.

Running directory tests

Directory tests enable you to validate the configured directory settings. The directory test results are reset when directory settings are saved, or when the directory tests are started.

1. Click **Test Settings** on the **Security→Directory** page.

The **Directory Tests** page displays the results of a series of simple tests designed to validate the current directory settings. It also includes a log that shows test results and detected issues. After your directory settings are configured correctly, you do not need to rerun these tests. The **Directory Tests** page does not require you to log in as a directory user.

2. In the **Directory Test Controls** section, enter the DN and password of a directory administrator in the **Directory Administrator Distinguished Name** and **Directory Administrator Password** boxes.

HPE recommends that you use the same credentials that you used when creating the iLO objects in the directory. These credentials are not stored by iLO; they are used to verify the iLO object and user search contexts.

3. In the **Directory Test Controls** section, enter a test user name and password in the **Test User Name** and **Test User Password** boxes.

4. Click **Start Test**.

Several tests begin in the background, starting with a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

While the tests are running, the page refreshes periodically. You can stop the tests or manually refresh the page at any time.

If a directory test reports the **Failed** status, see “[Directory issues](#)” (page 330).

More information

[Directory issues](#)

Directory test input values

Enter the following values when you run directory tests:

- **Directory Administrator Distinguished Name**—Searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.
- **Directory Administrator Password**—Authenticates the directory administrator.
- **Test User Name** and **Test User Password**—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.

Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. These credentials are not stored by iLO.

Directory test status values

iLO displays the following status values for directory tests:

- **In Progress**—Indicates that directory tests are currently being performed in the background. Click **Stop Test** to cancel the current tests, or click **Refresh** to update the contents of the page with the latest results. Using the **Stop Test** button might not stop the tests immediately.
- **Not Running**—Indicates that directory tests are current, and that you can supply new parameters to run the tests again. Use the **Start Test** button to start the tests and use the current test control values. Directory tests cannot be started after they are already in progress.
- **Stopping**—Indicates that directory tests have not yet reached a point where they can stop. You cannot restart tests until the status changes to **Not Running**. Use the **Refresh** button to determine whether the tests are complete.

Directory test results

The **Directory Test Results** section shows the directory test status with the date and time of the last update.

- **Overall Status**—Summarizes the results of the tests.
 - **Not Run**—No tests were run.
 - **Inconclusive**—No results were reported.
 - **Passed**—No failures were reported.
 - **Problem Detected**—A problem was reported.

- **Failed**—A specific subtest failed. Check the onscreen log to identify the problem.
- **Warning**—One or more of the directory tests reported a **Warning** status.
- **Test**—The name of each test.
For more information about the directory tests, see “[iLO directory tests](#)” (page 83).
- **Result**—Reports status for a specific directory setting or an operation that uses one or more directory settings. These results are generated when a sequence of tests is run. The results stop when the tests run to completion, when a test failure prevents further progress, or when the tests are stopped. Test results follow:
 - **Passed**—The test ran successfully. If more than one directory server was tested, all servers that ran this test were successful.
 - **Not Run**—The test was not run.
 - **Failed**—The test was unsuccessful on one or more directory servers. Directory support might not be available on those servers.
 - **Warning**—The test ran and reported a warning condition, for example, a certificate error. Check the **Notes** column for suggested actions to correct the warning condition.
- **Notes**—Indicates the results of various phases of the directory tests. The data is updated with failure details and information that is not readily available, like the directory server certificate subject and which roles were evaluated successfully.

iLO directory tests

- **Directory Server DNS Name**—If the directory server is defined in FQDN format (directory.company.com), iLO resolves the name from FQDN format to IP format, and queries the configured DNS server.
If the test is successful, iLO obtained an IP address for the configured directory server. If iLO cannot obtain an IP address for the directory server, this test and all subsequent tests fail.
If the directory server is configured with an IP address, iLO skips this test.
- **Ping Directory Server**—iLO initiates a ping to the configured directory server.
The test is successful if iLO receives the ping response; it is unsuccessful if the directory server does not reply to iLO.
If the test fails, iLO will continue with the subsequent tests.
- **Connect to Directory Server**—iLO attempts to negotiate an LDAP connection with the directory server.
If the test is successful, iLO was able to initiate the connection.
If the test fails, iLO was not able to initiate an LDAP connection with the specified directory server. Subsequent tests will stop.
- **Connect using SSL**—iLO initiates SSL handshake and negotiation and LDAP communications with the directory server through port 636.
If the test is successful, the SSL handshake and negotiation between iLO and the directory server were successful.
- **Bind to Directory Server**—This test binds the connection with the user name specified in the test boxes. If no user is specified, iLO does an anonymous bind.
If the test is successful, the directory server accepted the binding.

- **Directory Administrator Login**—If **Directory Administrator Distinguished Name** and **Directory Administrator Password** were specified, iLO uses these values to log in to the directory server as an administrator. These boxes are optional.
- **User Authentication**—iLO authenticates to the directory server with the specified user name and password.
 - If the test is successful, the supplied user credentials are correct.
 - If the test fails, the user name and/or password is incorrect.
- **User Authorization**—This test verifies that the specified user name is part of the specified directory group, and is part of the directory search context specified during directory services configuration.
- **Directory User Contexts**—If **Directory Administrator Distinguished Name** was specified, iLO tries to search the specified context.
 - If the test is successful, iLO found the context by using the administrator credentials to search for the container in the directory.
 - Contexts that begin with "@" can be tested only by user login.
 - A failure indicates that the container could not be located.
- **LOM Object Exists**—This test searches for the iLO object in the directory server by using the **LOM Object Distinguished Name** configured on the **Security→Directory** page.

NOTE: You can enter a **LOM Object Distinguished Name** on the **Security→Directory** page only when **Use HPE Extended Schema** is selected. This test is run even if **LDAP Directory Authentication** is disabled.

If the test is successful, iLO found the object that represents itself.

iLO encryption settings

SSL

iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. Encryption of HTTP data provided by SSL ensures that the data is secure as it is transmitted across the network.

Ciphers supported by iLO

- 256-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES256-SHA)
- 256-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES256-SHA)
- 256-bit AESGCM with RSA, and a AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 256-bit AES with RSA, and a SHA1 MAC (AES256-SHA)
- 128-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-AES128-SHA)

- 128-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- 128-bit AES with RSA, DH, and a SHA1 MAC (DHE-RSA-AES128-SHA)
- 128-bit AESGCM with RSA, and a AEAD MAC (AES128-GCM-SHA256)
- 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)
- 128-bit AES with RSA, and a SHA1 MAC (AES128-SHA)
- 168-bit 3DES with RSA, ECDH, and a SHA1 MAC (ECDHE-RSA-DES-CBC3-SHA)
- 168-bit 3DES with RSA, DH, and a SHA1 MAC (EDH-RSA-DES-CBC3-SHA)
- 168-bit 3DES with RSA, and a SHA1 MAC (DES-CBC3-SHA)

iLO supports the following ciphers when **FIPS Mode** or **Enforce AES/3DES Encryption** is enabled and iLO is restricted to TLS version 1.2.

- 256-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 256-bit AESGCM with RSA, and a AEAD MAC (AES256-GCM-SHA384)
- 256-bit AES with RSA, and a SHA256 MAC (AES256-SHA256)
- 128-bit AESGCM with RSA, ECDH, and a AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AESGCM with RSA, DH, and a AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- 128-bit AESGCM with RSA, and a AEAD MAC (AES128-GCM-SHA256)
- 128-bit AES with RSA, and a SHA256 MAC (AES128-SHA256)

SSH

iLO provides enhanced encryption through the SSH port for secure CLP transactions.

In the iLO factory default configuration:

- iLO supports AES256-CBC, AES128-CBC, 3DES-CBC, and AES256-CTR ciphers through the SSH port.
- iLO accepts diffie-hellman-group14-sha1 and diffie-hellman-group1-sha1 key exchange, and uses hmac-sha1, hmac-sha2-256, and hmac-md5 MACs.

When **FIPS Mode** or **Enforce AES/DES Encryption** is enabled:

- iLO supports the AES256-CTR cipher through the SSH port.
- iLO accepts diffie-hellman-group14-sha1 key exchange, and uses hmac-sha2-256 or hmac-sha1 MACs.

FIPS mode

iLO 4 firmware version 1.20 and later supports FIPS mode. FIPS is a set of computer security standards mandated for use by United States government agencies and contractors. When FIPS mode is enabled, iLO operates in a mode intended to comply with the requirements of FIPS 140-2 level 1.

FIPS mode is not the same as FIPS validated. FIPS validated refers to software that received validation by completing the Cryptographic Module Validation Program.

To date, iLO 3 version 1.50 and iLO 4 version 2.11 are FIPS validated.

It is important to decide if a FIPS-validated version of the iLO firmware is required for your environment, or if running iLO in FIPS mode will suffice. Because of the lengthy validation process, a FIPS-validated version of the iLO firmware has probably been superseded by a nonvalidated version with new features and security enhancements, which means that a FIPS-validated version of iLO might be less secure than the latest version.

AES/3DES encryption

iLO can be configured to enforce AES/3DES encryption. If enabled, iLO enforces the use of these enhanced ciphers (both AES and 3DES) over the secure channels, including secure HTTP transmissions through the browser, SSH port, and XML port. When AES/3DES encryption is enabled, you must use a cipher equal to or greater than AES/3DES to connect to iLO through these secure channels. The AES/3DES encryption enforcement setting does not affect communications and connections over less-secure channels.

By default, Remote Console data uses 128-bit RC4 bidirectional encryption. The HPQLOCFG utility uses 128-bit RC4 with 160-bit SHA1 and 2048-bit RSA KeyX encryption to send RIBCL scripts to iLO over the network.

Viewing encryption enforcement settings

Navigate to the **Administration**→**Security**→**Encryption** page.

The **Encryption Settings** page displays the cipher in use, and allows you to configure **FIPS Mode** or **Enforce AES/3DES Encryption**.

Encryption settings



- **Current Negotiated Cipher**—The cipher in use for the current browser session. After you log in to iLO through the browser, the browser and iLO negotiate a cipher setting to use during the session.
- **Encryption Enforcement Settings**—The current encryption settings for iLO:
 - **FIPS Mode**—Indicates whether FIPS mode is enabled or disabled for this iLO system.
 - **Enforce AES/3DES Encryption**—Indicates whether AES/3DES encryption is enforced for this iLO system.

When enabled, iLO only accepts connections that use the AES or 3DES ciphers.

Modifying the AES/DES encryption setting

Prerequisites

Configure iLO Settings privilege

Modifying the AES/DES encryption setting

1. Navigate to the **Administration**→**Security**→**Encryption** page.
2. Change the **Enforce AES/3DES Encryption** setting to **Enabled** or **Disabled**.
3. To end your browser connection and restart iLO, click **Apply**.

It might take several minutes before you can re-establish a connection.

When changing the **Enforce AES/3DES Encryption** setting to **Enabled**, close all open browsers after clicking **Apply**. Any browsers that remain open might continue to use a non-AES/3DES cipher.

Connecting to iLO by using AES or 3DES encryption

After you enable the **Enforce AES/3DES Encryption** setting, iLO requires that you connect through secure channels (web browser, SSH connection, or XML channel) by using an AES/3DES cipher.

- **Web browser**—You must configure the browser with a cipher equal to or greater than AES/3DES. If the browser is not using AES or 3DES ciphers, iLO displays an error message. The error text varies depending on the installed browser.
Different browsers use different methods for selecting a negotiated cipher. For more information, see the browser documentation. Log out of iLO through the current browser before changing the browser cipher setting. Any changes made to the browser cipher setting while you are logged in to iLO might enable the browser to continue using a non-AES/3DES cipher.
- **SSH connection**—For instructions on setting the cipher to use, see the SSH utility documentation.
- **XML channel**—HPQLOCFG uses a secure 3DES cipher by default. For example, HPQLOCFG displays the following cipher in the XML output:

```
Connecting to Server...
Negotiated cipher: 128-bit Rc4 with 160-bit SHA1 and 2048-bit RsaKeyx
```

Configuring a FIPS-validated environment with iLO

Use the following instructions to operate iLO in a FIPS-validated environment. To use FIPS mode, see “[Enabling FIPS mode](#)” (page 87).

To set up an environment with a FIPS-validated version of iLO, follow the steps in the Security Policy document that was part of the iLO FIPS validation process. The validated Security Policy document is available on the NIST website at <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>. The iLO FIPS information is listed under certificate 2574.

Enabling FIPS mode

Use this procedure to operate iLO in FIPS mode. To configure iLO in a FIPS-validated environment, see “[Configuring a FIPS-validated environment with iLO](#)” (page 87).

Prerequisites

Configure iLO Settings privilege

Setting FIPS mode to enabled

1. Optional: Capture the current iLO configuration by using HPONCFG.
For more information, see the iLO scripting and CLI guide.
2. Navigate to the **Administration**→**Security**→**Encryption** page.
3. Set FIPS mode to **Enabled**.

⚠ **CAUTION:** Enabling FIPS mode resets critical iLO security settings to the factory default values, and clears all user and license data.

4. Click **Apply**.
iLO prompts you to confirm the request.
5. To confirm the request to enable FIPS mode, click **OK**
iLO reboots in FIPS mode. Wait at least 90 seconds before attempting to re-establish a connection.
6. Install a trusted certificate for iLO.
The default issued SSL certificate is not allowed in FIPS mode.
7. Verify that **IPMI/DCMI over LAN Access** and **SNMP Access** are disabled on the **Access Settings** page.

⚠ **IMPORTANT:** Some iLO interfaces, such as the standards-compliant implementations of IPMI and SNMP, are not FIPS-compliant and cannot be made FIPS-compliant.

8. Optional: Restore the iLO configuration by using HPONCFG.
For more information, see the iLO scripting and CLI guide.

💡 **TIP:** You can use the Login Security Banner feature to notify iLO users that a system is using FIPS mode.

You can also use XML configuration and control scripts to enable FIPS mode. For more information, see the iLO scripting and CLI guide.

More information

[Configuring the Login Security Banner](#)

[Obtaining and importing an SSL certificate](#)

[iLO access settings](#)

Disabling FIPS mode

If you want to disable FIPS mode for iLO (for example, if a server is decommissioned), you must set iLO to the factory default settings. You can perform this task by using RIBCL scripts, iLO RBSU, or the iLO 4 Configuration Utility.

For information about changing this setting with RIBCL scripts, see the iLO scripting and CLI guide.

When you disable FIPS mode, all potentially sensitive data is erased, including all logs and settings.

More information

[Resetting iLO to the factory default settings \(iLO RBSU\)](#)

[Resetting iLO to the factory default settings \(iLO 4 Configuration Utility\)](#)

HPE SSO

HPE SSO enables you to browse directly from an HPE SSO-compliant application (such as HPE SIM and HPE OneView) to iLO, bypassing an intermediate login step.

To use this feature:

- You must have a supported version of an HPE SSO-compliant application.
- You might need iLO 4.1.20 or later.
- Configure iLO to trust the SSO-compliant application.

iLO contains support for HPE SSO applications to determine the minimum HPE SSO certificate requirements. Some HPE SSO-compliant applications automatically import trust certificates when they connect to iLO. For applications that do not perform this function automatically, use the HPE SSO page to configure the SSO settings through the iLO web interface. You must have the Configure iLO Settings privilege to change these settings.

This feature and many others are part of a licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Configuring iLO for HPE SSO

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Configuring HPE SSO

1. Navigate to the **Administration**→**Security**→**HPE SSO** page.
2. Configure the **Single Sign-On Trust Mode** setting.
If you enable support for HPE SSO, Hewlett Packard Enterprise recommends using the **Trust by Certificate** mode.
3. Configure iLO privileges for each role in the **Single Sign-On Settings** section.
4. To save the SSO settings, click **Apply**.
5. If you selected **Trust by Certificate** or **Trust by Name**, add the trusted certificate or DNS name to iLO.
6. After you configure SSO in iLO, log in to an HPE SSO-compliant application and browse to iLO. For example, log in to HPE SIM, navigate to the **System** page for the iLO processor, and then click the iLO link in the **More Information** section.

Although a system might be registered as a trusted server, SSO might be refused because of the current trust mode or certificate status. For example, if an HPE SIM server name is registered, and the trust mode is **Trust by Certificate**, but the certificate is not imported, SSO is not allowed from that server. Likewise, if an HPE SIM server certificate is imported, but the certificate has expired, SSO is not allowed from that server. The list of trusted servers is not used when SSO is disabled. iLO does not enforce SSO server certificate revocation.

More information

[Single Sign-On Trust Mode options](#)

[SSO user privileges](#)

[Adding trusted certificates](#)

[Importing a direct DNS name](#)

Single Sign-On Trust Mode options

The **Single Sign-On Trust Mode** affects how iLO responds to HPE SSO requests.

- **Trust None (SSO disabled)** (default)—Rejects all SSO connection requests
- **Trust by Certificate** (most secure)—Enables SSO connections from an HPE SSO-compliant application by matching a certificate previously imported to iLO
- **Trust by Name**—Enables SSO connections from an HPE SSO-compliant application by matching a directly imported IP address or DNS name.
- **Trust All** (least secure)—Accepts any SSO connection initiated from any HPE SSO-compliant application.

SSO user privileges

When you log in to an HPE SSO-compliant application, you are authorized based on your HPE SSO-compliant application role assignment. The role assignment is passed to iLO when SSO is attempted.

SSO attempts to receive only the privileges assigned in this section. iLO directory settings do not apply.

The default privilege settings follow:

- **User**—Login only
- **Operator**—Login, Remote Console, Power and Reset, and Virtual Media
- **Administrator**—Login, Remote Console, Power and Reset, Virtual Media, Configure iLO, and Administer Users

Adding trusted certificates

The certificate repository can hold five typical certificates. However, if typical certificates are not issued, certificate sizes might vary. When all of the allocated storage is used, no more imports are accepted.

Prerequisites

Configure iLO Settings privilege

Adding a certificate

1. Navigate to the **Administration**→**Security**→**HPE SSO** page.
2. Use one of the following methods to add a trusted certificate:

- **Direct import**—Copy the Base64-encoded certificate X.509 data, paste it into the text box above the **Import Certificate** button, and then click the button.
iLO 4.1.20 or later might be required to install the larger certificates used with recent versions of HPE SIM. HPE SIM 7.3.2 or later supports 2048-bit certificates.
- **Indirect import**—Type the DNS name or IP address in the text box above the **Import Certificate from URL** button, and then click the button. iLO contacts the HPE SSO-compliant application over the network, retrieves the certificate, and then saves it.

For information about how to extract an HPE SIM certificate, see “[Extracting the HPE SIM server certificate](#)” (page 91).

For information about how to extract certificates from other HPE SSO-compliant applications, see your HPE SSO-compliant application documentation.

Trusted certificate format

The Base64-encoded X.509 certificate data resembles the following:

```
-----BEGIN CERTIFICATE-----  
... several lines of encoded data ...  
-----END CERTIFICATE-----
```

Extracting the HPE SIM server certificate

You can use the following methods to extract HPE SIM certificates.

- Enter one of the following links in a web browser:
 - For HPE SIM versions earlier than 7.0:
`http://<HPE SIM name or network address>:280/GetCertificate`
`https://<HPE SIM name or network address>:50000/GetCertificate`
 - For HPE SIM 7.0 or later:
`http://<HPE SIM name or network address>:280/GetCertificate?certtype=sso`
`https://<HPE SIM name or network address>:50000/GetCertificate?certtype=sso`
- Export the certificate from HPE SIM:
 - For HPE SIM versions earlier than 7.0:
Select **Options**→**Security**→**Certificates**→**Server Certificate**.
 - For HPE SIM 7.0 or later:
Select **Options**→**Security**→**HPE Systems Insight Manager Server Certificate**, and then click **Export**.
- Use the HPE SIM CLI tools. For example, using the alias `tomcat` for the HPE SIM certificate, enter `mxcert -1 tomcat`.

For more information, see the HPE SIM documentation.

Importing a direct DNS name

Prerequisites

Configure iLO Settings privilege

Importing a direct DNS name

1. Navigate to the **Administration**→**Security**→**HPE SSO** page.
2. Enter the DNS name or network address in the text box above the **Import Direct DNS Name** button, and then click the button.

Viewing trusted certificates and records

Navigate to the **Administration**→**Security**→**HPE SSO** page.

The **Manage Trusted Certificates and Records** table displays the status of the trusted certificates and records configured to use SSO with the current iLO management processor.

Trusted certificate and record details

- **Status**—The status of the record. The possible status values follow:
 - The record is valid.
 - There is a problem with the trust settings or the iLO license. Possible reasons follow:
 - This record contains a DNS name, and the trust mode is set to **Trust by Certificate** (only certificates are valid).
 - **Trust None (SSO disabled)** is selected.
 - A valid license key is not installed.
 - The record is not valid. Possible reasons follow:
 - An out-of-date certificate is stored in this record. Check the certificate details for more information.
 - The iLO clock is not set or is set incorrectly.
 - The iLO clock must be in the **Valid from** and **Valid until** range.
- **Certificate**—Indicates that the record contains a stored certificate. Move the cursor over the icon to view the certificate details, including subject, issuer, and dates.
- **Description**—The server name (or certificate subject).

Removing trusted certificates and records

Prerequisites

Configure iLO Settings privilege

Removing a certificate

1. Navigate to the **Administration**→**Security**→**HPE SSO** page.
2. Select one or more records in the **Manage Trusted Certificates and Records** table.
3. Click **Delete**.
iLO prompts you to confirm that you want to delete the certificate or record.

① IMPORTANT: If you delete the certificate of a remote management system, you might experience impaired functionality when using the remote management system with iLO.

4. Click **Yes**.

Configuring the Login Security Banner

The Login Security Banner feature allows you to configure the security banner displayed on the iLO login page. For example, you could enter a message indicating that a system uses FIPS mode.

Prerequisites

Configure iLO Settings privilege

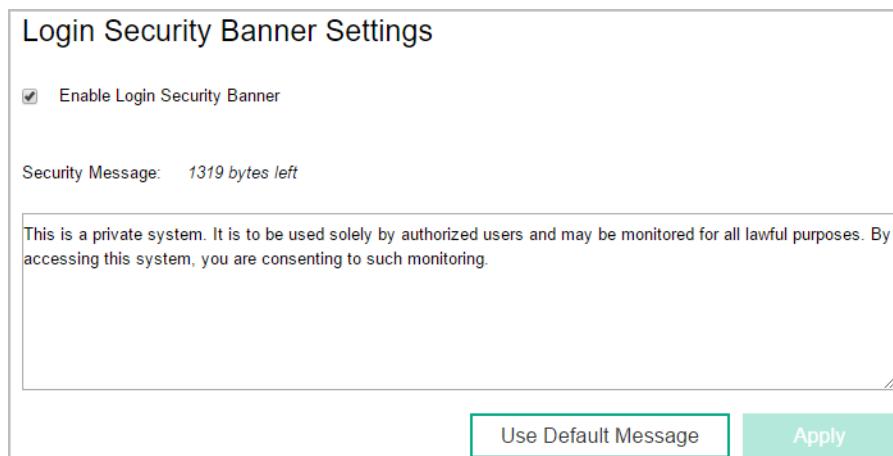
Enabling the Login Security Banner

1. Navigate to the **Administration**→**Security**→**Login Security Banner** page.
2. Select the **Enable Login Security Banner** check box.

iLO uses the following default text for the Login Security Banner:

This is a private system. It is to be used solely by authorized users and may be monitored for all lawful purposes. By accessing this system, you are consenting to such monitoring.

3. Optional: To customize the security message, enter a custom message in the **Security Message** text box.



Enable Login Security Banner

Security Message: 1319 bytes left

This is a private system. It is to be used solely by authorized users and may be monitored for all lawful purposes. By accessing this system, you are consenting to such monitoring.

Use Default Message Apply

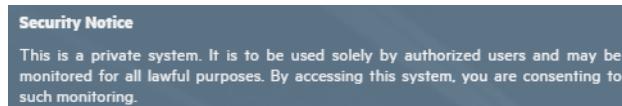
The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.



TIP: To restore the default text, click **Use Default Message**.

4. Click **Apply**.

The security message is displayed at the next login.



Configuring Remote Console Computer Lock settings

This feature locks the OS or logs a user out when a Remote Console session ends or the network link to iLO is lost. If you open a .NET IRC or Java IRC window when this feature is configured, the operating system will be locked when you close the window.

Prerequisites

Configure iLO Settings privilege

Configuring the Remote Console Computer Lock settings

1. Navigate to the **Remote Console**→**Security** page.
2. Select from the following **Remote Console Computer Lock** settings: **Windows**, **Custom**, and **Disabled**.
3. Select a computer lock key sequence.
4. To save the changes, click **Apply**.

Remote Console Computer Lock options

- **Windows**—Use this option to configure iLO to lock a managed server running a Windows operating system. The server automatically displays the **Computer Locked** dialog box when a Remote Console session ends or the iLO network link is lost.
- **Custom**—Use this option to configure iLO to use a custom key sequence to lock a managed server or log out a user on that server. You can select up to five keys from the list. The selected key sequence is sent automatically to the server operating system when a Remote Console session ends or the iLO network link is lost.
- **Disabled** (default)—Use this option to disable the Remote Console Computer Lock feature. When a remote console session ends or the iLO network link is lost, the operating system on the managed server is not locked.

Valid Remote Console Computer Lock keys

You can create a Remote Console Computer Lock key sequence by using the keys listed in [Table 1 \(page 94\)](#):

Table 1 Remote Console Computer Lock keys

ESC	SCRL LCK	1	g
L_ALT	SYS RQ	2	h
R_ALT	F1	3	i
L_SHIFT	F2	4	j
R_SHIFT	F3	5	k
L_CTRL	F4	6	l
R_CTRL	F5	7	m
L_GUI	F6	8	n
R_GUI	F7	9	o
INS	F8	;	p
DEL	F9	=	q
HOME	F10	[r
END	F11	\	s
PG_UP	F12]	t
PG_DN	" " (space)	'	u
ENTER	'	a	v
TAB	,	b	w
BREAK	-	c	x
BACKSPACE	.	d	y
NUM PLUS	/	e	z
NUM MINUS	0	f	

Configuring the Integrated Remote Console Trust setting (.NET IRC)

The .NET IRC is launched through Microsoft ClickOnce, which is part of the Microsoft .NET Framework. ClickOnce requires that any application installed from an SSL connection must be

from a trusted source. If a browser is not configured to trust an iLO processor, and this setting is **Enabled**, ClickOnce notifies you that the application cannot start.

Prerequisites

Configure iLO Settings privilege

Configuring the Integrated Remote Console Trust setting

1. Navigate to the **Remote Console**→**Security** page.
2. Select **Enabled** or **Disabled** for the **IRC requires a trusted certificate in iLO** setting.
3. To save the changes, click **Apply**.

Integrated Remote Console Trust setting options

- **Enabled**—If a trusted SSL certificate has been imported into iLO, the .NET IRC is launched by using an HTTPS connection.
- **Disabled** (default)—The .NET IRC is launched by using a non-SSL connection. SSL is used after the .NET IRC starts to exchange encryption keys.

8 Configuring the iLO network settings

iLO network settings

iLO provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled **iLO**) on the back of the server.
- **Shared Network Port LOM** (nonblade servers only)—Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.

To access the network settings, select the active NIC in the navigation tree, and then view or edit the network settings on the following pages:

- **Network Summary**
- **Network General Settings**
- **IPv4 Settings**
- **IPv6 Settings**
- **SNTP Settings**

If you select the inactive port option, a message notifies you that iLO is not configured to use that port.

Viewing the network configuration summary

To navigate to the **Network Summary** page, select **Network**→**iLO Dedicated Network Port** or **Network**→**Shared Network Port**.

Network configuration summary details

NIC In Use:	iLO Dedicated Network Port
iLO Hostname:	
MAC Address:	
Link State:	Auto-Negotiate
Duplex Option:	Auto-Negotiate

- **NIC in Use**—The name of the active iLO network interface (iLO Dedicated Network Port or Shared Network Port).
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. By default, the hostname is **iLO**, followed by the system serial number and the current domain name. This value is used for the network name and must be unique.
- **MAC Address**—The MAC address of the selected iLO network interface.
- **Link State**—The current link speed of the selected iLO network interface. The default value is Auto-Negotiate.
- **Duplex Option**—The current link duplex setting for the selected iLO network interface. The default value is Auto-Negotiate.

You can configure the iLO hostname and NIC settings on the **Network General Settings** page.

More information

[Configuring NIC and TCP/IP settings \(iLO RBSU\)](#)

[Configuring the NIC settings](#)

IPv4 Summary details

IPv4 Summary	
DHCPv4 Status:	Enabled
	IPv4
Address	
Subnet Mask	
Default Gateway	

- **DHCPv4 Status**—Indicates whether DHCP is enabled for IPv4.
- **Address**—The IPv4 address currently in use. If the value is 0.0.0.0, the IPv4 address is not configured.
- **Subnet Mask**—The subnet mask of the IPv4 address currently in use. If the value is 0.0.0.0, no address is configured.
- **Default Gateway**—The default gateway address in use for the IPv4 protocol. If the value is 0.0.0.0, the gateway is not configured.

More information

[Configuring IPv4 settings](#)

IPv6 Summary details

This section is displayed only for the iLO Dedicated Network Port.

IPv6 Summary			
DHCPv6 Status: Enabled		IPv6 Stateless Address Auto-Configuration (SLAAC): Enabled	
IPv6	Prefix Length	Status	
SLAAC Address	64	Active	
Default Gateway			

- **DHCPv6 Status**—Indicates whether DHCP is enabled for IPv6. The following values are possible:
 - **Enabled**—Stateless and Stateful DHCPv6 are enabled.
 - **Enabled (Stateless)**—Only Stateless DHCPv6 is enabled.
 - **Disabled**—DHCPv6 is disabled.
- **IPv6 Stateless Address Auto-Configuration (SLAAC)**—Indicates whether SLAAC is enabled for IPv6. When SLAAC is disabled, the SLAAC link-local address for iLO is still configured because it is required.
- **Address list**—This table shows the currently configured IPv6 addresses for iLO. It provides the following information:
 - **Source**—Indicates whether the address is a static or SLAAC address.
 - **IPv6**—The IPv6 address.

- **Prefix Length**—The address prefix length.
- **Status**—The address status. The possible values are **Active** (the address is in use by iLO), **Pending** (Duplicate Address Detection is in progress), or **Failed** (Duplicate Address Detection failed. The address is not in use by iLO).
- **Default Gateway**—The default IPv6 gateway address that is in use. For IPv6, iLO keeps a list of possible default gateway addresses. The addresses in this list originate from router advertisement messages and the IPv6 **Static Default Gateway** setting.

The **Static Default Gateway** setting is configured on the IPv6 page.

More information

[Configuring IPv6 settings](#)

Configuring the iLO Hostname Settings

Prerequisites

Configure iLO Settings privilege

Configuring the hostname settings

1. Navigate to the **Network**→**iLO Dedicated Network Port** or **Network**→**Shared Network Port** page.
2. Click the **General** tab.
3. Enter the **iLO Subsystem Name (Hostname)**.

The hostname is the DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`). This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

4. Enter the **iLO Domain Name** if DHCP is not configured.

To use a static domain name when the iLO Dedicated Network port is selected, disable the **Use DHCPv4 Supplied Domain Name** and **Use DHCPv6 Supplied Domain Name** settings on the **IPv4** and **IPv6 Network General Settings** tabs.

To use a static domain name when the iLO Shared Network port is selected, disable the **Use DHCPv4 Supplied Domain Name** setting on the **IPv4 Network General Settings** tab.

5. Click **Submit**.
6. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart the iLO processor.

It might take several minutes before you can re-establish a connection.

iLO hostname and domain name limitations

When you configure the **iLO Hostname Settings**, note the following:

- **Name service limitations**—The subsystem name is used as part of the DNS name.
 - DNS allows alphanumeric characters and hyphens.
 - Name service limitations also apply to the **Domain Name**.
- **Namespace issues**—To avoid these issues:
 - Do not use the underscore character.
 - Limit subsystem names to 15 characters.

- Verify that you can ping the iLO processor by IP address and by DNS/WINS name.
- Verify that NSLOOKUP resolves the iLO network address correctly and that no namespace conflicts exist.
- If you are using both DNS and WINS, verify that they resolve the iLO network address correctly.
- Flush the DNS name if you make any namespace changes.
- If you will use Kerberos authentication, ensure that hostname and domain name meet the prerequisites for using Kerberos. For more information, see “[Kerberos authentication with iLO](#)” (page 278).

Configuring the NIC settings

Enable the iLO Dedicated Network Port or the iLO Shared Network Port and configure the associated NIC settings in the **NIC Settings** section of the **Network General Settings** tab.

Enabling the iLO Dedicated Network Port through the iLO web interface

Prerequisites

Configure iLO Settings privilege

Configuring the NIC settings

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Navigate to the **Network**→**iLO Dedicated Network Port** page.
3. Click the **General** tab.
4. Select the **Use iLO Dedicated Network Port** check box.
5. Select a **Link State**.

The link setting controls the speed and duplex settings of the iLO network transceiver.

NOTE: This setting is not available on server blades.

6. To save the changes, click **Submit**.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

It might take several minutes before you can re-establish a connection.

More information

[iLO network port configuration options](#)

[iLO network connection considerations](#)

[Link State values](#)

Link State values

Choose from the following **Link State** values when you enable the iLO Dedicated Network Port:

- **Automatic** (default)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network
- **1000BaseT, Full-duplex**—Forces a 1 Gb connection that uses full duplex (not supported for BL c-Class servers)

- **1000BaseT, Half-duplex**—Forces a 1 Gb connection that uses half duplex (not supported for BL c-Class servers)
1000BaseT, Half-duplex is not a standard setting, and few switches support it. If you use this setting, ensure that the switch is configured to support 1000BaseT, Half-duplex.
- **100BaseT, Full-duplex**—Forces a 100 Mb connection using full duplex
- **100BaseT, Half-duplex**—Forces a 100 Mb connection using half duplex
- **10BaseT, Full-duplex**—Forces a 10 Mb connection using full duplex
- **10BaseT, Half-duplex**—Forces a 10 Mb connection using half duplex

Enabling the iLO Shared Network Port through the iLO web interface (nonblade servers only)

Prerequisites

Configure iLO Settings privilege

Configuring the NIC settings

1. Connect the Shared Network Port LOM or FlexibleLOM port to a LAN.
2. Navigate to the **Network**→**Shared Network Port** page.
3. Click the **General** tab.
4. Select the **Use Shared Network Port** check box.
5. Depending on the server configuration, select **LOM**, or **FlexibleLOM**.
6. Select a value from the **Port** menu.

Selecting a port number other than port 1 works only if the server and the network adapter both support this configuration. If you enter an invalid port number, port 1 is used.

7. To use a VLAN, select the **Enable VLAN** check box.

When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN.

8. If you enabled VLAN, enter a **VLAN Tag**. All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094.
9. To save the changes, click **Submit**.
10. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

It might take several minutes before you can re-establish a connection.

After iLO resets, the Shared Network Port is active. Any network traffic going to or originating from iLO is directed through the Shared Network Port LOM or FlexibleLOM port.

More information

[iLO network port configuration options](#)
[iLO network connection considerations](#)

iLO network port configuration options

The iLO subsystem provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled **iLO**) on the back of the server.
- **Shared Network Port LOM**—Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.

NOTE: For information about the NICs your server supports, see the server QuickSpecs at <http://www.hpe.com/info/qs/>.

iLO network connection considerations

- Only one of the Dedicated Network Port or Shared Network Port options can be enabled at a time because iLO supports only one active NIC connection.
- By default, the iLO Shared Network Port uses port 1 on the server NIC. Depending on the server configuration, this NIC might be a LOM or FlexibleLOM adapter. The port number corresponds to the label on the NIC, which might be different from the numbering in the operating system.

If the server and the NIC both support port selection, the iLO firmware allows you to select a different port number. This feature is supported with iLO 4.2.00 and later. If a port other than port 1 is selected for Shared Network Port use, and your server does not support that configuration, iLO switches back to port 1 when it starts.

- Access to iLO via IPv6 is not currently supported when the Shared Network Port is enabled.
- On servers that do not have a Dedicated Network Port, the standard hardware configuration provides iLO network connectivity only through the iLO Shared Network Port connection. On these servers, the iLO firmware defaults to the Shared Network Port.
- Due to server auxiliary-power budget limitations, some 1Gb/s copper network adapters used for iLO Shared Network Port functionality might run at 10/100 speed when the server is powered off. To avoid this issue, Hewlett Packard Enterprise recommends configuring the switch that the iLO Shared Network Port is connected to for auto-negotiation.

If the switch port that iLO is connected to is configured for 1Gb/s, some copper iLO Shared Network Port adapters might lose connectivity when the server is powered off. Connectivity will return when the server is powered back on.

- Disabling the iLO Shared Network Port does not completely disable the system NIC—server network traffic can still pass through the NIC port. When the iLO Shared Network Port is disabled, any traffic going to or originating from iLO will not pass through the Shared Network Port.
- If the Shared Network Port is enabled, you cannot modify the link state or duplex options. When using Shared Network Port configurations, these settings must be managed in the operating system.
- If the Shared Network Port is enabled and you use NIC teaming, review the section “[NIC teaming with Shared Network Port configurations](#)” (page 24).

Other available methods for configuring the NIC settings

- **iLO RBSU** (on servers that support iLO RBSU)—For more information, see “[iLO ROM-based utilities](#)” (page 141).
- **iLO 4 Configuration Utility** (on servers that support the UEFI System Utilities)—For more information, see “[iLO ROM-based utilities](#)” (page 141).
- **XML scripting**—For more information, see the iLO scripting and CLI guide.
- **SMASH CLP**—For more information, see the iLO scripting and CLI guide.

Configuring IPv4 settings

Use the iLO Dedicated Network Port or Shared Network Port **IPv4 Settings** page to configure the iLO IPv4 settings.

Prerequisites

Configure iLO Settings privilege

Configuring the IPv4 settings

1. Navigate to the **Network**→**iLO Dedicated Network Port** or **Network**→**Shared Network Port** page.
2. Click the **IPv4** tab.
3. Configure the DHCPv4 settings.
4. Configure the general IPv4 settings.
5. Configure the DNS server information.
6. Configure the WINS server information.
7. Configure the **Ping Gateway on Startup** setting.
8. To save the changes you made on the **IPv4 Settings** page, click **Submit**.
9. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

It might take several minutes before you can re-establish a connection.

More information

[DHCPv4 settings](#)

[General IPv4 settings](#)

[DNS server settings](#)

[WINS server settings](#)

[Ping Gateway on Startup setting](#)

DHCPv4 settings

- **Enable DHCPv4**—Enables iLO to obtain its IP address (and many other settings) from a DHCP server.
- **Use DHCPv4 Supplied Gateway**—Specifies whether iLO uses the DHCP server-supplied gateway. If DHCP is not used, enter a gateway address in the **Gateway IPv4 Address** box.
- **Use DHCPv4 Supplied Static Routes**—Specifies whether iLO uses the DHCP server-supplied static routes. If not, enter the static route destination, mask, and gateway addresses in the **Static Route #1**, **Static Route #2**, and **Static Route #3** boxes.
- **Use DHCPv4 Supplied Domain Name**—Specifies whether iLO uses the DHCP server-supplied domain name. If DHCP is not used, enter a domain name in the **Domain Name** box on the **Network General Settings** page.

- **Use DHCPv4 Supplied DNS Servers**—Specifies whether iLO uses the DHCP server-supplied DNS server list. If not, enter the DNS server addresses in the **Primary DNS Server**, **Secondary DNS Server**, and **Tertiary DNS Server** boxes.
- **Use DHCPv4 Supplied Time Settings**—Specifies whether iLO uses the DHCPv4-supplied NTP service locations.
- **Use DHCPv4 Supplied WINS Servers**—Specifies whether iLO uses the DHCP server-supplied WINS server list. If not, enter the WINS server addresses in the **Primary WINS Server** and **Secondary WINS Server** boxes.

General IPv4 settings

- **IPv4 Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- **Gateway IPv4 Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.
- **Static Route #1**, **Static Route #2**, and **Static Route #3**—The iLO static route destination, mask, and gateway addresses. If **Use DHCPv4 Supplied Static Routes** is used, these values are supplied automatically. If not, enter the static route values.

DNS server settings

- **Primary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Primary DNS Server address.
- **Secondary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary DNS Server address.
- **Tertiary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Tertiary DNS Server address.
- **Enable DDNS Server Registration**—Select or clear this check box to specify whether iLO registers its IPv4 address and name with a DNS server.

WINS server settings

- **Primary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Primary WINS Server address.
- **Secondary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary WINS Server address.
- **Enable WINS Server Registration**—Specifies whether iLO registers its name with a WINS server.

Ping Gateway on Startup setting

This setting causes iLO to send four ICMP echo request packets to the gateway when the iLO processor initializes. This activity ensures that the ARP cache entry for iLO is up-to-date on the router responsible for routing packets to and from iLO.

Configuring IPv6 settings

Use the iLO Dedicated Network Port **IPv6 Settings** page to configure the iLO IPv6 settings.

When using IPv6, note the following:

- IPv6 is not supported in the Shared Network Port configuration.
- If you downgrade the iLO firmware from version 1.30 or later to version 1.2x, the IPv6 settings will be reset to the default values.
- For a list of the iLO features that support IPv6, see “[iLO features that support IPv6](#)” (page 105).

Prerequisites

Configure iLO Settings privilege

Configuring the IPv6 settings

1. Navigate to the **Network→iLO Dedicated Network Port** page.
2. Click the **IPv6** tab.
3. Configure the DHCPv6 settings.
4. Configure the DNS server settings.
5. Configure the general IPv6 settings.
6. To save the changes you made on the **IPv6 Settings** page, click **Submit**.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

It might take several minutes before you can re-establish a connection.

More information

[DHCPv6 settings](#)

[DNS server settings](#)

[General IPv6 settings](#)

DHCPv6 settings

- **iLO Client Applications use IPv6 first**—When both IPv4 and IPv6 service addresses are configured for iLO client applications, this option specifies which protocol iLO tries first when accessing a client application. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.
 - Select this check box if you want iLO to use IPv6 first.
 - Clear this check box if you want iLO to use IPv4 first.If communication fails using the first protocol, iLO automatically tries the second protocol.
- **Enable Stateless Address Auto Configuration (SLAAC)**—Select this check box to enable iLO to create IPv6 addresses for itself from router advertisement messages.
iLO creates its own link-local address even when this option is not selected.

- **Enable DHCPv6 in Stateful Mode (Address)**—Select this check box to allow iLO to request and configure IPv6 addresses provided by a DHCPv6 server.
 - **Use DHCPv6 Rapid Commit**—Select this check box to instruct iLO to use the Rapid Commit messaging mode with the DHCPv6 server. This mode reduces DHCPv6 network traffic, but might cause problems if it is used in networks where more than one DHCPv6 server can respond and provide addresses.
- **Enable DHCPv6 in Stateless Mode (Other)**—Select this check box to enable iLO to request settings for NTP and DNS service location from the DHCPv6 server.
 - **Use DHCPv6 Supplied Domain Name**—Select this check box to use the DHCPv6 server-supplied domain name.
 - **Use DHCPv6 Supplied DNS Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for DNS server locations. This setting can be enabled at the same time as the IPv4 DNS server location options.
 - **Use DHCPv6 Supplied NTP Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for NTP server locations. This setting can be enabled at the same time as the IPv4 NTP server location options.

When **Enable DHCPv6 in Stateful Mode (Address)** is selected, **Enable DHCPv6 in Stateless Mode (Other)** is always selected by default because it is implicit in the DHCPv6 Stateful messages that are required between iLO and the DHCPv6 server.

DNS server settings

- **Primary DNS Server, Secondary DNS Server, and Tertiary DNS Server**—Enter the IPv6 addresses for the DNS service.
When DNS server locations are configured on both the IPv4 and IPv6 pages, both sources are used. Preference is given according to the **iLO Client Applications use IPv6 first** configuration option, primary sources, then secondary, and then tertiary.
- **Enable DDNS Server Registration**—Specify whether iLO registers its IPv6 address and name with a DNS server.

General IPv6 settings

- **Static IPv6 Address 1, Static IPv6 Address 2, Static IPv6 Address 3, and Static IPv6 Address 4**—Enter up to four static IPv6 addresses and prefix lengths for iLO. Do not enter link-local addresses.
- **Static Default Gateway**—Enter a default IPv6 gateway address for cases in which no router advertisement messages are present in the network.
- **Static Route #1, Static Route #2, and Static Route #3**—Enter static IPv6 route destination prefix and gateway address pairs. Specify the prefix length for the destination. Link-local addresses are not allowed for the destination, but are allowed for the gateway.

iLO features that support IPv6

iLO 4 1.20 and later supports IPv6 in the iLO Dedicated Network Port configuration. It is not supported with the Shared Network Port configuration. The IETF introduced IPv6 in response to the ongoing depletion of the IPv4 address pool. In IPv6, addresses are increased to 128 bits in length, to avoid an address shortage problem. iLO supports the simultaneous use of both protocols through a dual-stack implementation. All previously available iLO features are still supported in IPv4.

The following features support the use of IPv6:

- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- IPv6 Static Default Gateway Entry
- DHCPv6 Stateful Address Assignment
- DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
- Integrated Remote Console
- Onboard Administrator Single Sign-On
- HPE SIM Single Sign-On
- Web Server
- SSH Server
- SNTP Client
- DDNS Client
- RIBCL over IPv6
- SNMP
- AlertMail
- Remote Syslog
- WinDBG Support
- HPQLOCFG/HPLOMIG over an IPv6 connection
- Scriptable Virtual Media
- CLI/RIBCL key import over an IPv6 connection
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation
- IPMI

IPv6 support for the iLO scripting interfaces requires the following versions of the iLO utilities:

- HPQLOCFG 1.0 or later
- Lights-Out XML Scripting Sample bundle 4.2.0 or later
- HPONCFG 4.2.0 or later
- LOCFG.PL 4.20 or later
- HPLOMIG 4.20 or later

Configuring iLO SNTP settings

Prerequisites

- Configure iLO Settings privilege
- At least one NTP server is available on your management network.
- If you will use a DHCPv4-provided NTP service configuration, DHCPv4 is enabled on the **IPv4** tab.

- If you will use a DHCPv6-provided NTP service configuration, DHCPv6 Stateless Mode is enabled on the **IPv6** tab.
- For DHCPv6 time settings configurations only: The server is configured to use the iLO Dedicated Network Port. IPv6 is not supported in the Shared Network Port configuration.

Configuring SNTP settings

1. Navigate to the **Network**→**iLO Dedicated Network Port** or **Network**→**Shared Network Port** page.
2. Click the **SNTP** tab.
3. Do one of the following:
 - To use DHCP-provided NTP server addresses, select the **Use DHCPv4 Supplied Time Settings** check box, the **Use DHCPv6 Supplied Time Settings** check box, or both check boxes.
 - Enter NTP server addresses in the **Primary Time Server** and **Secondary Time Server** boxes.
4. If you selected only **Use DHCPv6 Supplied Time Settings**, or if you entered a primary and secondary time server, select the server time zone from the **Time Zone** list.
5. Configure the NTP time propagation setting by selecting or clearing the **Propagate NTP Time to Host** check box (nonblade servers) or the **Propagate NTP or OA Time to Host** check box (blade servers).
6. To save the changes you made on the **SNTP Settings** page, click **Submit**.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

It might take several minutes before you can re-establish a connection.

More information

[Configuring IPv4 settings](#)

[Configuring IPv6 settings](#)

[Configuring NIC and TCP/IP settings \(iLO RBSU\)](#)

[Configuring the NIC settings](#)

[DHCP NTP address selection](#)

[SNTP options](#)

[iLO clock synchronization](#)

[Incorrect time stamp on iLO Event Log entries](#)

SNTP options

- **Use DHCPv4 Supplied Time Settings**—Configures iLO to use a DHCPv4-provided NTP server address.
- **Use DHCPv6 Supplied Time Settings**—Configures iLO to use a DHCPv6-provided NTP server address.
- **Propagate NTP Time to Host** (nonblade servers) or **Propagate NTP or OA Time to Host** (blade servers)—Determines whether the server time is synchronized with the iLO time during the first POST after AC power is applied, a blade is inserted, or iLO is reset to the default settings.

For ProLiant server blades only: When **Propagate NTP or OA Time to Host** is enabled, and NTP is not configured or functional, the server time is synchronized with the Onboard Administrator time.

- **Primary Time Server**—Configures iLO to use a primary time server with the specified address. You can enter the server address by using the server FQDN, IPv4 address, or IPv6 address.
- **Secondary Time Server**—Configures iLO to use a secondary time server with the specified address. You can enter the server address by using the server FQDN, IPv4 address, or IPv6 address.
- **Time Zone**—Determines how iLO adjusts UTC time to obtain the local time, and how it adjusts for Daylight Savings Time (Summer Time). In order for the entries in the iLO Event Log and IML to display the correct local time, you must specify the server location time zone. If you want iLO to use the time the SNTP server provides, without adjustment, select a time zone that does not apply an adjustment to UTC time. In addition, that time zone must not apply a Daylight Savings Time (Summer Time) adjustment. There are several time zones that fit this requirement. One example is **Atlantic/Reykjavik GMT**, which is not east or west of the Prime Meridian, and in which the time does not change in the Spring or Fall. If you select the Atlantic/Reykjavik time zone, iLO web interface pages and log entries display the exact time provided by the SNTP server.

NOTE: Configure the NTP servers to use Coordinated Universal Time (GMT).

iLO clock synchronization

SNTP allows iLO to synchronize its clock with an external time source. Configuring SNTP is optional because the iLO date and time can also be synchronized from the following sources:

- System ROM (during POST only)
- Insight Management Agents (in the OS)
- Onboard Administrator (ProLiant server blades only)
- HPE OneView

Primary and secondary NTP server addresses can be configured manually or via DHCP servers. If the primary server address cannot be contacted, the secondary address is used.

DHCP NTP address selection

When you use DHCP servers to provide NTP server addresses, the **iLO Client Applications use IPv6 first** setting on the **IPv6** page controls the selection of the primary and secondary NTP values. When **iLO Client Applications use IPv6 first** is selected, a DHCPv6-provided NTP service address (if available) is used for the primary time server and a DHCPv4-provided address (if available) is used for the secondary time server.

To change the protocol-based priority behavior to use DHCPv4 first, clear the **iLO Client Applications use IPv6 first** check box.

If a DHCPv6 address is not available for the primary or secondary address, a DHCPv4 address (if available) is used.

More information

[Configuring IPv6 settings](#)

iLO NIC auto-selection

iLO NIC auto-selection enables iLO to choose between the iLO Dedicated Network Port and the iLO Shared Network port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common preconfiguration for your ProLiant Gen9 servers. For example, if you have several servers, some might be installed in a data center where iLO is contacted through the iLO Dedicated Network Port. Other servers might be installed in a data center where iLO is contacted through the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

By default, NIC auto-selection is disabled. For information about configuring this feature, see [“Enabling iLO NIC auto-selection” \(page 110\)](#).

NIC auto-selection support

- ProLiant Gen9 nonblade servers with iLO 4.2.00 or later support NIC auto-selection.
- iLO 4.2.40 and later can be configured to search both Shared Network Ports on servers that support this configuration.
- iLO 4.2.40 and later supports NIC failover. When enabled, iLO automatically begins searching for a NIC connection when the current connection fails. NIC auto-selection must be enabled to use this feature.

iLO startup behavior with NIC auto-selection enabled

When NIC auto-selection is enabled:

- If iLO was just connected to power, it tests the iLO Dedicated Network Port first.
- If iLO was just reset, it tests the last used iLO network port first.
- When testing a network port, if iLO detects network activity, then that port is selected for use. If network activity is not found after approximately 100 seconds, iLO switches to the opposite network port and begins testing there. iLO alternates testing between the iLO Dedicated Network Port and the iLO Shared Network Port until network activity is detected. An iLO reset occurs each time iLO switches between network ports for testing purposes.

△ 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.

- When iLO searches for an active network port, the server UID LED is illuminated. If iLO is reset during the search, the UID LED flashes for 5 seconds and then is illuminated until an active port is selected or iLO is reset.
- When a server supports both LOM and FlexibleLOM Shared Network Port connections to iLO, iLO will test only the option that was selected during configuration. It will not alternate testing between LOM and FlexibleLOM options.

For information about configuring the Shared Network Port options, see [“Enabling the iLO Shared Network Port through the iLO web interface \(nonblade servers only\)” \(page 100\)](#).

- If NIC auto-selection is configured to search for DHCP address assignment activity, but only one of the iLO network ports has DHCP enabled, iLO tests for received data packet activity on the port that is not configured for DHCP.

Enabling iLO NIC auto-selection

NIC auto-selection is disabled by default. Use the following procedure to enable NIC auto-selection:

1. Configure both iLO network ports.

Before enabling and using the NIC auto-selection feature, both iLO network ports must be configured for their respective network environments.

2. Do one of the following:

- Use the CLI command `oemhp_nicautose1` to configure NIC auto-selection.
- To enable NIC auto-selection, add the `ILO_NIC_AUTO_SELECT` tag to your `MOD_NETWORK_SETTINGS` script, and run the script.

Optional: To configure the optional NIC auto-selection features, add the `ILO_NIC_AUTO_SNP_SCAN` and `ILO_NIC_AUTO_DELAY` tags to your `MOD_NETWORK_SETTINGS` script.

For more information, see the iLO scripting and CLI guide.

3. Arrange server cabling as desired, and then reset iLO.

The change to NIC auto-selection does not take effect until iLO is reset.

Configuring NIC failover

1. Configure iLO NIC auto-selection.

2. Do one of the following:

- Use the CLI command `oemhp_nicfailover` to configure NIC failover.
- To configure the NIC failover features, add the `ILO_NIC_FAIL_OVER` tag to your `MOD_NETWORK_SETTINGS` script, and run the script.

For more information, see the iLO scripting and CLI guide.

More information

[Enabling iLO NIC auto-selection](#)

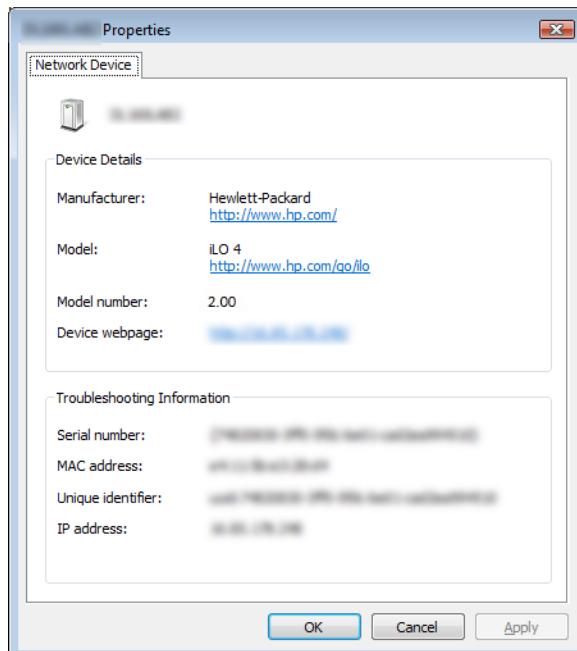
Viewing iLO systems in the Windows Network folder

If UPnP is configured, iLO systems on the same network as a Windows system are displayed in the Windows **Network** folder.

- To start the web interface for an iLO system, right-click the system in the Windows **Network** folder, and then select **View device webpage**.



- To view the properties of an iLO system, right-click the icon in the Windows **Network** folder, and then select **Properties**.



The **Properties** window includes the following:

- **Device Details**—iLO software manufacturer and version information. To start the iLO web interface, click the **Device webpage** link.
- **Troubleshooting Information**—The iLO serial number, MAC address, UUID, and IP address.

9 Configuring iLO management settings

iLO SNMP management

With iLO 3 and earlier, SNMP management used the HPE Insight Management Agents running on the server operating system. With iLO 4, you can use either Agentless Management or the Insight Management Agents. The default configuration uses Agentless Management.

Agentless Management uses out-of-band communication for increased security and stability. With Agentless Management, health monitoring and alerting is built into the system and begins working the moment a power cord is connected to the server. This feature runs on the iLO hardware, independent of the operating system and processor. Additional operating system data is collected when AMS is installed.

If AMS is not installed:

- iLO will not display a full set of data on the **Information→System Information** pages.
- iLO might not display the correct server name in Insight Online and Insight RS.

The **Management – SNMP Settings** page allows you to configure the iLO settings for SNMP, SNMP alerts, and Insight Management integration.

You must have the Configure iLO Settings privilege to change these settings.

Depending on your configuration, you might need to install additional software. For more information, see “[AMS and the Insight Management Agents](#)” (page 114).

For more information about Agentless Management, see the Considerations for choosing Agentless Management white paper at the following website: <http://www.hpe.com/info/ilo/docs>.

[Table 2](#) (page 113) lists the information collected by the available server configurations.

Table 2 Information provided by Agentless Management and Insight Management Agents

Component	Agentless Management without AMS ¹	Agentless Management with AMS ¹	Insight Management Agents ^{1, 2}
Server health	<ul style="list-style-type: none"> Fans Temperatures Power supplies Memory CPU 	<ul style="list-style-type: none"> Fans Temperatures Power supplies Memory CPU 	<ul style="list-style-type: none"> Fans Temperatures Power supplies Memory CPU
Storage	<ul style="list-style-type: none"> Smart Array³ SMART Drive Monitoring (connected to Smart Array) Internal and external drives connected to Smart Array Smart Storage battery monitoring (supported servers only) 	<ul style="list-style-type: none"> Smart Array³ SMART Drive Monitoring (connected to Smart Array, Smart HBA, and AHCI) Internal and external drives connected to Smart Array Smart Storage battery monitoring (supported servers only) NVMe drives⁴ 	<ul style="list-style-type: none"> Smart Array SMART Drive Monitoring (connected to Smart Array, Smart HBA, and AHCI) SAS/SATA HBA/RAID Fibre Channel/iSCSI Tape External storage
Network	<ul style="list-style-type: none"> MAC addresses for embedded NICs Physical link connectivity and link up/link down traps for NICs that have NC-SI over MCTP Fibre Channel adapters that support Hewlett Packard Enterprise vendor-defined MCTP commands⁵ 	<ul style="list-style-type: none"> MAC and IP address for standup and embedded NICs Link up/link down traps⁶ NIC teaming information Supported Fibre Channel adapters 	<ul style="list-style-type: none"> MAC and IP addresses for standup and embedded NICs Link up/link down traps NIC teaming information VLAN information
Other	<ul style="list-style-type: none"> iLO data Firmware inventory Device inventory 	<ul style="list-style-type: none"> iLO data Firmware inventory Device inventory OS information (host SNMP MIB)⁶ Driver/service inventory Logging events to OS logs⁷ 	<ul style="list-style-type: none"> iLO data OS information (host SNMP MIB) Performance data User-configurable thresholds Logging events to OS logs Clustering information
Prefailure warranty alerts	<ul style="list-style-type: none"> Memory Drives (physical and logical) 	<ul style="list-style-type: none"> Memory Drives (physical and logical) 	<ul style="list-style-type: none"> Memory Drives (physical and logical)

¹ The **Agentless Management without AMS** column represents the basic iLO configuration without AMS or the Insight Management Agents. Server configurations with AMS or the Insight Management Agents provide the same information as the basic iLO configuration, as well as the information that is listed in the **Agentless Management with AMS** and **Insight Management Agents** columns.

² Supported servers only. For more information, see the server specifications.

³ This configuration does not write the same OS logs as the Insight Management Agents. For example, RAID device status is not reported.

⁴ Supported with iLO 4.2.30 and later.

⁵ Supported with iLO 4.2.50 and later.

⁶ The data supplied by Agentless Management is not as extensive as the data supplied by the SNMP agents.

⁷ iLO 4 1.05 and later supports AMS-based OS logging for Linux (`/var/log/messages` for Red Hat and `/var/log/syslog` for SUSE Linux Enterprise Server, Debian, and Ubuntu), Windows, and VMware. iLO 4 1.10 and later supports Smart Array logging.

AMS and the Insight Management Agents

Note the following when you consider whether to install AMS or the Insight Management Agents:

- AMS is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.
- Hewlett Packard Enterprise does not recommend installing AMS at the same time as the Insight Management Agents and WMI Providers.
- When you install AMS on Windows systems, the Agentless Management Service Control Panel is installed. You can use the Control Panel to configure SNMP settings, to enable or disable AMS, and to remove AMS.
- AMS writes operating system configuration information and critical events to the Active Health System Log.
- Install the iLO 3/4 Channel Interface Driver before installing AMS.
For more information, see “[iLO drivers and utilities](#)” (page 32).
- The Insight Management Agents are not supported on Synergy compute modules.

Installing AMS or the Insight Management Agents

1. Obtain AMS or the Insight Management Agents from one of the following sources:
 - Download the SPP (Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise Server) from the following website: <http://www.hpe.com/servers/spp>.
 - Download the software from the Hewlett Packard Enterprise Support Center (Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware) at <http://www.hpe.com/support/hpesc>.
 - Download the software from the **vibsdepot** section of the Software Delivery Repository website at <http://www.hpe.com/support/SDR-Linux> (VMware).
AMS is also included in the customized Hewlett Packard Enterprise VMware ISO images that are released on Hewlett Packard Enterprise Software Depot (<http://www.hpe.com/support/SDR-Linux>).
 - Subscribe to the Linux Management Component Pack (Ubuntu). For more information, see <http://www.hpe.com/support/SDR-Linux>
2. Install the software.
For instructions on using the SPP, see the SPP documentation at <http://www.hpe.com/info/spp/documentation>.
For other download types, follow the installation instructions provided with the software.

Verifying the AMS installation

Use the following procedures to verify the AMS installation on Windows, Linux, and VMware systems.

Verifying AMS status: iLO web interface

1. Navigate to the **Information**→**System Information** page.

2. Click the **Summary** tab.

AMS is listed in the **Subsystems and Devices** table. The possible values follow:

- **Not available**—AMS is not available because it was not detected, the server is in POST, or the server is powered off.
- **OK**—AMS is installed and running.

Verifying AMS status: Windows

1. Open the Windows Control Panel.

If the AMS Control Panel is present, then AMS is installed.

2. Open the AMS Control Panel.

3. Click the **Service** tab.

If AMS is enabled, the following message appears:

Agentless Management Service (AMS) is enabled.

Verifying AMS status: SUSE and Red Hat Enterprise Linux

1. To verify that AMS is installed, enter the following command: `rpm -qi hp-ams`.

2. To verify that AMS is running, enter the following command: `service hp-ams status`.

Verifying AMS status: VMware

1. Verify that AMS is installed.

a. Access the VMware host from the VMware vSphere Client.

b. Navigate to the **Inventory**→**Configuration**→**Health Status** tab for the server.

c. Click the plus sign (+) next to **Software Components**.

The software installed on the host is listed. The AMS component includes the string `hp-ams`.

NOTE: The full name of the AMS component is different for each supported version of ESX/ESXi.

2. To verify that AMS is running, enter the following command: `/etc/init.d/hp-ams.sh status`.

Verifying AMS status: Ubuntu

1. To verify that AMS is installed, enter the following command: `dpkg -l hp-ams`.

2. To verify that AMS is running, enter the following command: `sudo service hp-ams status`.

Restarting AMS

- **Windows**—Navigate to the Windows **Services** page and restart AMS.
- **SUSE and Red Hat**—Enter the following command: `service hp-ams restart`.
- **VMware**—Enter the following command: `/etc/init.d/hp-ams.sh restart`.
- **Ubuntu**—Enter the following command: `sudo service hp-ams restart`.

Nagios plug-in for Agentless Management

The Nagios plug-in for Agentless Management interacts with the Agentless Management infrastructure to provide out-of-band monitoring of ProLiant Gen8 servers, ProLiant Gen9 servers, and Synergy compute modules.

Nagios is an open source application that can be used to monitor computer systems, networks, and IT infrastructure.

Download the plug-in from the Nagios website at <https://exchange.nagios.org/>.

Configuring SNMP settings

Prerequisites

Configure iLO Settings privilege

Configuring the SNMP settings

1. Navigate to the **Administration**→**Management** page.
2. On the **SNMP Settings** tab, select the SNMP setting to enable: **Agentless Management** or **SNMP Pass-thru**.
3. If you selected **Agentless Management**, enter the following values. These values are unavailable when the SNMP Pass-thru configuration is selected:
 - **System Location**
 - **System Contact**
 - **System Role**
 - **System Role Detail**
 - **Read Community**
4. Enter the following information:
 - **Trap Community**
 - **SNMP Alert Destination(s)**
 - **SNMP Port**
5. To save the configuration, click **Apply**.

SNMP options

- **SNMP management configuration**—Choose one of the following:
 - **Agentless Management** (default)—Use SNMP agents running on iLO to manage the server. In this configuration, iLO fulfills SNMP requests sent by the client to iLO over the network. This setting does not affect alerts.
 - **SNMP Pass-thru**—Use SNMP agents running on the host operating system to manage the server. SNMP requests sent by the client to iLO over the network are passed to the host operating system. The responses are then passed to iLO and returned to the client over the network. This setting does not affect alerts.
 - **Trap Community**—The configured SNMP trap community string.
 - **SNMP Alert Destination(s)**—The IP addresses or FQDNs of up to three remote management systems that will receive SNMP alerts from iLO.

NOTE: Typically, you enter the HPE SIM server console IP address in one of the **SNMP Alert Destination(s)** boxes.

When SNMP Alert Destinations are configured using FQDNs, and DNS provides both IPv4 and IPv6 addresses for the FQDNs, iLO sends traps to the address specified by the **iLO Client Applications use IPv6 first** setting on the **IPv6** page. If **iLO Client Applications use IPv6 first** is selected, traps will be sent to IPv6 addresses (when available). When **iLO Client Applications use IPv6 first** is not selected, traps will be sent to IPv4 addresses (when available).

- **SNMP Port**—The port used for SNMP communications. This value is read-only, but can be modified on the **Administration**→**Access Settings** page.
To navigate to the **Administration**→**Access Settings** page, click the **SNMP Port** link. For more information, see “[iLO access settings](#)” (page 61).

SNMP options (Agentless Management configuration only)

- **System Location**—A string of up to 49 characters that specifies the physical location of the server.
- **System Contact**—A string of up to 49 characters that specifies the system administrator or server owner. The string can include a name, email address, or phone number.
- **System Role**—A string of up to 64 characters that describes the server role or function.
- **System Role Detail**—A string of up to 512 characters that describes specific tasks that the server might perform.
- **Read Community**—The configured SNMP read-only community string.

Read Community supports the following formats:

- A community string (for example, `public`).
- A community string followed by an IP address or FQDN (for example, `public 192.168.0.1`).

Use this option to specify that SNMP access will be allowed from the specified IP address or FQDN.

For iLO 4.1.10 or later, you can enter an IPv4 address, an IPv6 address, or an FQDN.

SNMPv3 authentication

iLO 4 1.20 or later supports SNMPv3 authentication when you use the Agentless Management configuration.

The following security features of SNMPv3 enable secure data collection from SNMP agents:

- Message integrity prevents tampering during packet transmission.
- Encryption prevents packet snooping.
- Authentication ensures that packets are from a valid source.

By default, SNMPv3 supports the User-based Security Model. With this model, security parameters are configured at both the agent level and the manager level. Messages exchanged between the agent and the manager are subject to a data integrity check and data origin authentication.

iLO supports three user profiles in which you can set the SNMPv3 USM parameters.

Configuring SNMPv3 users

Prerequisites

Configure iLO Settings privilege

Configuring SNMPv3 user profiles

1. Navigate to the **Administration**→**Management** page.
2. On the **SNMP Settings** tab, scroll to the **SNMPv3 Users** section.

SNMPv3 Users		
Security Name:	Authentication Protocol:	Privacy Protocol:
unset		
unset		
unset		

SNMPv3 Engine ID:

Apply

3. Select a user profile in the **SNMPv3 Users** section, and then click **Edit**.

The iLO web interface updates to show the SNMPv3 user options.

SNMPv3 Users	
Security Name:	<input type="text"/>
Authentication Protocol:	MD5 ▾
Authentication Passphrase:	<input type="text"/>
Privacy Protocol:	DES ▾
Privacy Passphrase:	<input type="text"/>

Cancel **Apply**

4. Enter the SNMPv3 user options:
 - **Security Name**
 - **Authentication Protocol**
 - **Authentication Passphrase**
 - **Privacy Protocol**
 - **Privacy Passphrase**
5. To save the user profile, click **Apply**.

More information

[SNMPv3 user options](#)

SNMPv3 user options

- **Security Name**—The user profile name. Enter an alphanumeric string of 1 to 32 characters.
- **Authentication 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 is included as part of the message sent to the recipient. Select **MD5** or **SHA**.
- **Authentication Passphrase**—Sets the passphrase to use for sign operations. Enter a value of 8 to 49 characters.
- **Privacy Protocol**—Sets the encryption algorithm to use for encoding the privacy passphrase. A portion of an SNMP message is encrypted before transmission. Select **AES** or **DES**.
- **Privacy Passphrase**—Sets the passphrase used for encrypt operations. Enter a value of 8 to 49 characters.

Configuring the SNMPv3 Engine ID

The **SNMPv3 Engine ID** sets the unique identifier of an SNMP engine belonging to an SNMP agent entity. You can configure this value when **Agentless Management** is selected.

Prerequisites

Configure iLO Settings privilege

Configuring the SNMPv3 engine ID

1. Navigate to the **Administration**→**Management** page.
2. On the **SNMP Settings** tab, scroll to the **SNMPv3 Users** section.
3. Enter a value in the **SNMPv3 Engine ID** box.

This value must be a hexadecimal string of 6 to 32 characters, not counting the preceding 0x, and must be an even number of characters (for example, 0x01020304abcdef).

4. Click **Apply**.

Configuring SNMP alerts

You can configure the Trap Source Identifier, iLO SNMP alerts, forwarding of Insight Management Agent SNMP alerts, Cold Start Trap broadcast, and SNMPv1 traps.

Prerequisites

Configure iLO Settings privilege

Configuring the SNMP alert settings

1. Navigate to the **Administration**→**Management** page.
2. On the **SNMP Settings** tab, scroll to the **SNMP Alerts** section.
3. Configure the **Trap Source Identifier** by selecting **iLO Hostname** or **OS Hostname**.
4. Enable or disable the following alert types:
 - **iLO SNMP Alerts**
 - **Forward Insight Manager Agent SNMP Alerts**
 - **Cold Start Trap Broadcast**
 - **SNMPv1 Traps**
5. Optional: To generate a test alert and send it to the TCP/IP addresses in the **SNMP Alert Destination(s)** boxes, click **Send Test Alert**.

Test alerts include an Insight Management SNMP trap, and are used to verify the network connectivity of iLO in HPE SIM. Only users with the Configure iLO Settings privilege can send test alerts.

After the alert is generated, a confirmation dialog box opens. Check the HPE SIM console for receipt of the alert.
6. To save the configuration, click **Apply**.

More information

[SNMP alert settings](#)

SNMP alert settings

- **Trap Source Identifier**—Determines the host name that is used in the SNMP-defined **sysName** variable when iLO generates SNMP traps. The default setting is **iLO Hostname**.

NOTE: The host name is an OS construct and does not remain persistent with the server when the hard drives are moved to a new server platform. The iLO **sysName**, however, remains persistent with the system board.

- **iLO SNMP Alerts**—Alert conditions that iLO detects independently of the host operating system can be sent to specified SNMP alert destinations, such as HPE SIM. If this option is disabled, no traps will be sent to the configured SNMP alert destinations.
- **Forward Insight Manager Agent SNMP Alerts**—Alert conditions detected by the host management agents can be forwarded to SNMP alert destinations through iLO. The Insight Management Agents generate these alerts, which are available for each supported operating system. Insight Management Agents must be installed on the host server to receive these alerts.
- **Cold Start Trap Broadcast**—When this option is enabled and no valid trap destinations are configured, Cold Start Trap is broadcast to a subnet broadcast address.

The Cold Start Trap is broadcast when any of the following conditions is met:

- **SNMP Alert Destinations** are not configured.
- iLO failed to resolve all of the **SNMP Alert Destinations** to IP addresses.

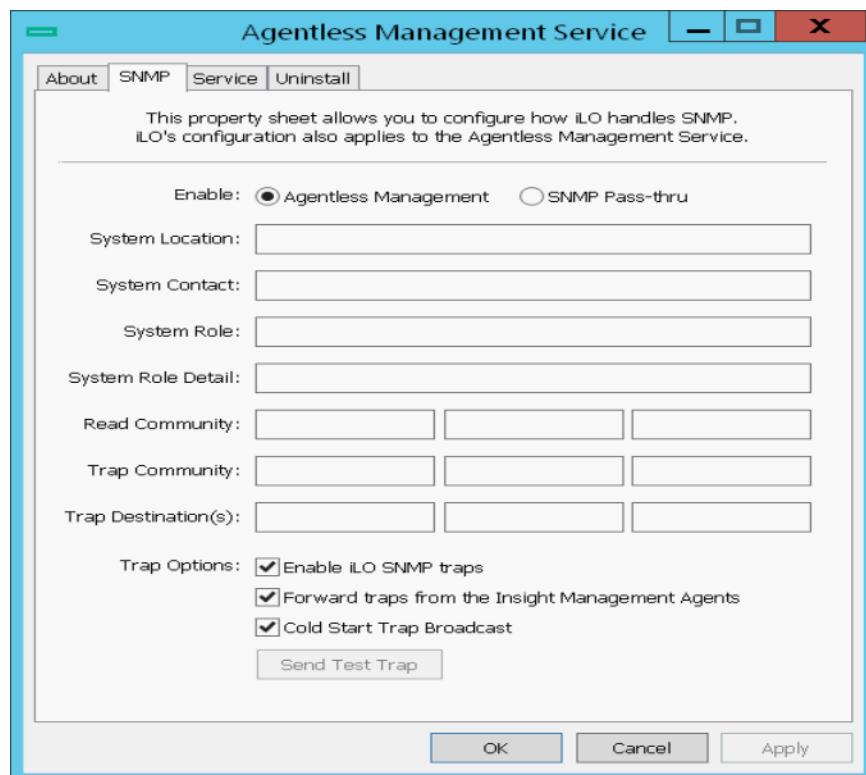
The subnet broadcast address for an IPv4 host is obtained by performing a bitwise logical OR operation between the bit complement of the subnet mask and the host IP address. For

example, the host 192.168.1.1, which has the subnet mask 255.255.252.0, has the broadcast address 192.168.1.1 | 0.0.3.255 = 192.168.3.255.

- **SNMPv1 Traps**—When enabled, SNMPv1 traps are sent to the remote management systems configured in the **SNMP Alert Destination(s)** boxes.

Using the AMS Control Panel to configure SNMP and SNMP alerts (Windows only)

1. Open the Agentless Management Service Control Panel.
2. Click the **SNMP** tab.



3. Update the SNMP settings.
4. Optional: To generate a test alert and send it to the TCP/IP addresses in the **Trap Destination(s)** boxes, click **Send Test Trap**.

Test alerts include an Insight Management SNMP trap and are used to verify the network connectivity of iLO in HPE SIM. Only users that have the Configure iLO Settings privilege can send test alerts.

After the alert is generated, a confirmation dialog box opens. Check the HPE SIM console for receipt of the alert.

5. To save the configuration, click **Apply**.

More information

[SNMP options](#)

[SNMP options \(Agentless Management configuration only\)](#)

[Configuring SNMP alerts](#)

SNMP traps

[Table 3 \(page 122\)](#) lists the SNMP traps that you can generate with iLO 4, ProLiant Gen8 and Gen9 servers, and Synergy compute modules.

Table 3 SNMP traps

SNMP trap name	Description
Cold Start Trap 0	SNMP has been initialized, the system has completed POST, or AMS has started.
Authentication Failure Trap 4	SNMP has detected an authentication failure.
cpqSeCpuStatusChange 1006	An uncorrectable machine check exception has been detected in a processor.
cpqSeUSBStorageDeviceReadErrorOccurred 1010	A read error occurred on an attached USB storage device.
cpqSeUSBStorageDeviceWriteErrorOccurred 1011	A write error occurred on an attached USB storage device.
cpqSeUSBStorageDeviceRedundancyLost 1012	USB storage device redundancy was lost.
cpqSeUSBStorageDeviceRedundancyRestored 1013	USB storage device redundancy was restored.
cpqSeUSBStorageDeviceSyncFailed 1014	The sync operation to restore USB storage device redundancy failed.
cpqDa6CntlrStatusChange 3033	A change has been detected in the status of the Smart Array controller.
cpqDa6LogDrvStatusChange 3034	A change has been detected in the status of a Smart Array logical drive.
cpqDa6AccelStatusChange 3038	A change has been detected in the status of a Smart Array cache module.
cpqDa6AccelBadDataTrap 3039	The Smart Array cache module has lost backup power.
cpqDa6AccelBatteryFailed 3040	The Smart Array cache module backup power has failed.
cpqDa7PhyDrvStatusChange 3046	A change has been detected in the status of a Smart Array physical drive.
cpqDa7SpareStatusChange 3047	A change has been detected in the status of a Smart Array spare drive.
cpqDaPhyDrvSSDWearStatusChange 3049	A change has been detected in the SSD wear status of a Smart Array physical drive.
cpqHe3ThermalConfirmation 6026	The server was shut down due to a thermal anomaly and is now operational.
cpqHe3PostError 6027	One or more POST errors have occurred.
cpqHe3FltTolPowerRedundancyLost 6032	The fault-tolerant power supplies have lost redundancy for the specified chassis.
cpqHe3FltTolPowerSupplyInserted 6033	A fault-tolerant power supply has been inserted.
cpqHe3FltTolPowerSupplyRemoved 6034	A fault-tolerant power supply has been removed.
cpqHe3FltTolFanDegraded 6035	The fault-tolerant fan condition has been set to Degraded .
cpqHe3FltTolFanFailed 6036	The fault-tolerant fan condition has been set to Failed .
cpqHe3FltTolFanRedundancyLost 6037	The fault-tolerant fans have lost redundancy.
cpqHe3FltTolFanInserted 6038	A fault-tolerant fan has been inserted.
cpqHe3FltTolFanRemoved 6039	A fault-tolerant fan has been removed.
cpqHe3TemperatureDegraded 6041	The temperature status has been set to Degraded , and the temperature is outside the normal operating range. Depending on the system configuration, this system might be shut down.

Table 3 SNMP traps (continued)

SNMP trap name	Description
cpqHe3TemperatureOk 6042	The temperature status has been set to OK .
cpqHe4FltTolPowerSupplyOk 6048	The fault-tolerant power supply condition has been reset to OK .
cpqHe4FltTolPowerSupplyDegraded 6049	The fault-tolerant power supply condition has been set to Degraded .
cpqHe4FltTolPowerSupplyFailed 6050	The fault-tolerant power supply condition has been set to Failed .
cpqHeResilientMemMirroredMemoryEngaged 6051	The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.
cpqHe3FltTolPowerRedundancyRestore 6054	The fault-tolerant power supplies have returned to a redundant state.
cpqHe3FltTolFanRedundancyRestored 6055	The fault-tolerant fans have returned to a redundant state.
cpqHe5CorrMemReplaceMemModule 6064	Memory errors have been corrected. Replace the memory module.
cpqHe4FltTolPowerSupplyACpowerloss 6069	The fault-tolerant power supply in the specified chassis and bay reported AC power loss.
cpqHeSysBatteryFailed 6070	The HPE Smart Storage Battery has failed.
cpqHeSysBatteryRemoved 6071	The HPE Smart Storage Battery has been removed.
cpqHeSysPwrAllocationNotOptimized 6072	iLO could not determine the power requirements. The server power allocation is not optimized.
cpqHeSysPwrOnDenied 6073	The server could not power on because the hardware cannot be identified.
cpqHePowerFailureError 6074	A device power failure has been detected.
cpqHeInterlockFailureError 6075	A device is missing or improperly seated on the system board.
cpqSs6FanStatusChange 8029	The storage enclosure fan status changed.
cpqSs6TempStatusChange 8030	The storage enclosure temperature status changed.
cpqSs6PwrSupplyStatusChange 8031	The storage enclosure power status changed.
cpqSsConnectionStatusChange 8032	The storage enclosure status changed.
cpqSm2ServerReset 9001	The server power has been reset.
cpqSm2UnauthorizedLoginAttempts 9003	The maximum unauthorized login attempt threshold has been exceeded.
cpqSm2SelfTestError 9005	iLO 4 has detected a self test error.
cpqSm2SecurityOverrideEngaged 9012	iLO 4 has detected that the security override jumper has been toggled to the engaged position.
cpqSm2SecurityOverrideDisengaged 9013	iLO 4 has detected that the security override jumper has been toggled to the disengaged position.
cpqSm2ServerPowerOn 9017	The server has been powered on.
cpqSm2ServerPowerOff 9018	The server has been powered off.
cpqSm2ServerPowerOnFailure 9019	A request was made to power on the server, but the server could not be powered on because of a failure condition.

Table 3 SNMP traps (continued)

SNMP trap name	Description
cpqSm2IrsCommFailure 9020	Communication with Insight Remote Support or Insight Online has failed.
cpqHo2GenericTrap 11003	Generic trap. Verifies that the SNMP configuration, client SNMP console, and network are operating correctly. You can use the iLO web interface to generate this alert to verify receipt of the alert on the SNMP console.
cpqHo2PowerThresholdTrap 11018	A power threshold has been exceeded.
cpqHoMibHealthStatusArrayChangeTrap 11020	A change in the health status of the server has occurred.
cpqSasPhyDrvStatusChange 5022	AMS detected a change in the status of an SAS or SATA physical drive.
cpqIdeAtaDiskStatusChange 14004	AMS detected a change in the status of an ATA disk drive.
cpqFca3HostCntlrStatusChange 16028	AMS detected a change in the status of a Fibre Channel host controller.
cpqNic3ConnectivityRestored 18011	Connectivity was restored to a logical network adapter.
cpqNic3ConnectivityLost 18012	The status of a logical network adapter changed to Failed .
cpqNic3RedundancyIncreased 18013	AMS detected that a previously failed physical adapter in a connected logical adapter group returned to the OK status.
cpqNic3RedundancyReduced 18014	AMS detected that a physical adapter in a logical adapter group changed to Failed status, but at least one physical adapter remains in OK status.

For more information about these SNMP traps, see the following files in the Insight Management MIB update kit for HPE SIM:

- cpqid.a.mib
- cpqhost.mib
- cpqlth.mib
- cpqsm2.mib
- cpqide.mib
- cpqscsi.mib
- cpqnic.mib
- cpqstsys.mib
- cpqstdeq.mib

Configuring Insight Management integration

Prerequisites

Configure iLO Settings privilege

Configuring the Insight Management settings

1. Navigate to the **Administration**→**Management** page.
2. On the **SNMP Settings** tab, scroll to the **Insight Management Integration** section.
3. Configure the **HPE SMH FQDN/IP Address**.

Insight Management Integration

HPE SMH FQDN / IP Address: https://[REDACTED] :2381

Level of Data Returned: Enabled (iLO+Server Association Data) ▾

[View XML Reply](#) Apply

This value sets the browser destination of the **Insight Agent** link on iLO pages.

Enter the FQDN or IP address of the host server. The protocol (`https://`) and port number (`:2381`) are added automatically to the IP address or DNS name to allow access from iLO. If the URL is set through another method (for example, HPQLOCFG), click the browser refresh button to display the updated URL.

4. Select the **Level of Data Returned**.

This setting controls the content of an anonymous discovery message received by iLO. The information returned is used for HPE SIM HTTP identification requests. The following options are available:

- **Enabled (iLO+Server Association Data)** (default)—Enables HPE SIM to associate the management processor with the host server, and provides sufficient data to enable integration with HPE SIM.
- **Disabled (No Response to Request)**—Prevents iLO from responding to HPE SIM requests.

5. Optional: To view the response that is returned to HPE SIM when it requests iLO management processor identification by using the provided address, click **View XML Reply**.

6. To save the changes, click **Apply**.

For more information about the Insight Management Agents, navigate to the **Information**→**Insight Agent** page.

iLO AlertMail

iLO AlertMail enables you to configure iLO to send alert conditions detected independently of the host operating system to a specified email address. iLO mail alerts include major host system events.

Some email service providers establish filters and rules to block problem emails such as spam, commercial content, and unwanted volume. These tools might block the receipt of messages generated by iLO. These email services are not suitable for receiving iLO AlertMail messages.

Enabling AlertMail

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Configure iLO Settings privilege

Setting AlertMail to Enabled status

1. Navigate to the **Administration**→**Management**→**AlertMail** page.
2. Select the **Enable iLO AlertMail** check box.
3. Enter the following information:
 - **Email Address**
 - **Sender Domain**

- **SMTP Port**
- **SMTP Server**

4. Optional: To send a test message to the configured email address, click **Send Test AlertMail**. This button is available only when AlertMail is enabled.
5. To save the changes, click **Apply**.

AlertMail options

- **Email Address**—The destination email address for iLO email alerts. This string can be up to 63 characters and must be in standard email address format. You can enter only one email address.
- **Sender Domain**—The domain name specified in the sender (From) email address. The sender email address is formed by using the iLO name as the host name, and the sender domain as the domain name. This string can be up to 63 characters.
- **SMTP Port**—The port that the SMTP server will use for unauthenticated SMTP connections. The default value is 25.
- **SMTP Server**—The IP address or DNS name of the SMTP server or the MSA. This server cooperates with the MTA to deliver the email. This string can be up to 63 characters.

Disabling AlertMail

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Configure iLO Settings privilege

Setting AlertMail to Disabled status

1. Navigate to the **Administration**→**Management**→**AlertMail** page.
2. Clear the **Enable iLO AlertMail** check box.
3. To save the changes, click **Apply**.

Remote Syslog

The Remote Syslog feature allows iLO to send event notification messages to Syslog servers. The iLO firmware Remote Syslog includes the IML and iLO Event Log.

Enabling iLO Remote Syslog

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Configure iLO Settings privilege

Setting Remote Syslog to Enabled status

1. Navigate to the **Administration**→**Management**→**Remote Syslog** page.
2. Select the **Enable iLO Remote Syslog** check box.
3. Enter the following information:
 - **Remote Syslog Port**
 - **Remote Syslog Server**

4. Optional: To send a test message to the configured syslog server, click **Send Test Syslog**. This button is available only when iLO Remote Syslog is enabled.
5. To save the changes, click **Apply**.

Remote syslog options

- **Remote Syslog Port**—The port number through which the Syslog server is listening. The default value is 514.
- **Remote Syslog Server**—The IP address, FQDN, IPv6 name, or short name of the server running the Syslog service. This string can be up to 127 characters.
On Linux systems, a tool called syslog logs system events. You can set a syslog server on a remote system that will act as a central logging system for iLO systems. If the iLO Remote Syslog feature is enabled in iLO, it can send its logs to the syslog server.

Disabling iLO Remote Syslog

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Configure iLO Settings privilege

Setting Remote Syslog to Disabled status

1. Navigate to the **Administration**→**Management**→**Remote Syslog** page.
2. Clear the **Enable iLO Remote Syslog** check box.
3. To save the changes, click **Apply**.

10 Managing remote support

HPE embedded remote support

iLO 4 includes the embedded remote support feature, which allows you to register supported servers for HPE remote support. You can also use iLO to monitor service events and remote support data collections.

Connecting a server to Hewlett Packard Enterprise allows it to be remotely supported and to send diagnostic, configuration, telemetry, and contact information to Hewlett Packard Enterprise. No other business information is collected, and the data is managed according to the Hewlett Packard Enterprise privacy statement, which you can review at the following website: <http://www.hpe.com/info/privacy>.

When you use the embedded remote support feature, choose from the following configuration options: [Insight Online direct connect](#) and [Insight Remote Support central connect](#).

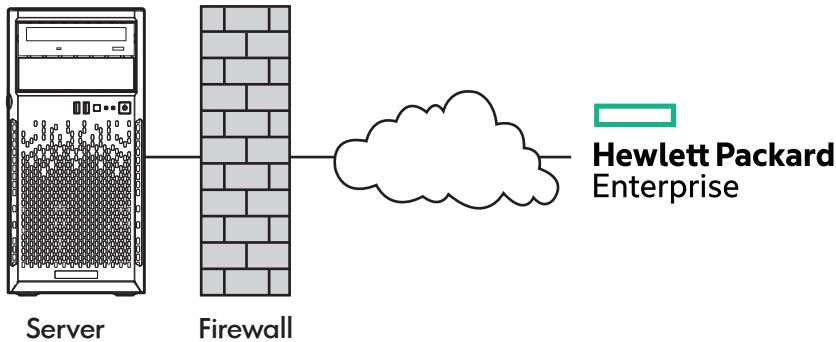
Insight Online direct connect

Register a server directly with Insight Online without the need to set up an Insight Remote Support centralized host server in your local environment. Insight Online will be your primary interface for remote support information.

Insight Online is a Hewlett Packard Enterprise Support Center feature that enables you to view your remotely monitored devices anywhere, anytime. It provides a personalized dashboard for simplified tracking of IT operations and support information, including a mobile dashboard for monitoring when you are on the go.

[Figure 3 \(page 128\)](#) shows the direct connect configuration with a server.

Figure 3 Insight Online direct connect

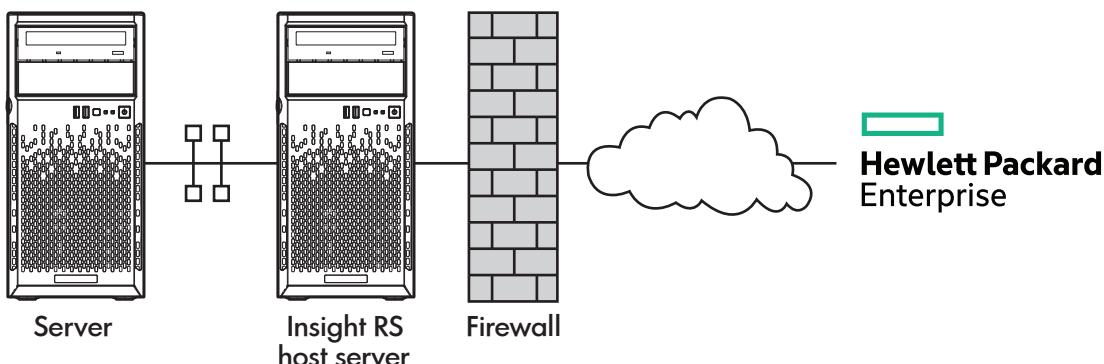


Insight Remote Support central connect

Register a server with Hewlett Packard Enterprise through an Insight Remote Support centralized host server in your local environment. All configuration and service event information is routed through the host server. This information can be viewed by using the local Insight RS Console or the web-based view in Insight Online (if it is enabled in Insight RS).

[Figure 4 \(page 129\)](#) shows the central connect configuration with a server.

Figure 4 Insight Remote Support central connect



Device support

Embedded remote support registration is supported for the following device types:

Insight Online direct connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

Insight Remote Support central connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

If you use HPE OneView to manage your environment, use HPE OneView to register for remote support. For more information, see the HPE OneView user guide.

Data collected by HPE remote support

When a server is registered for remote support, iLO collects Active Health System and server configuration information, and then iLO or the Insight RS host server sends this information to Hewlett Packard Enterprise. Active Health System information is sent every 7 days, and configuration information is sent every 30 days. The following information is included:

- **Registration**—During server registration, iLO collects data to uniquely identify the server hardware. Registration data includes the following:
 - Server model
 - Serial number
 - iLO NIC address
- **Service events**—When service events are recorded, iLO collects data to uniquely identify the relevant hardware component. Service event data includes the following:
 - Server model
 - Serial number
 - Part number of the hardware component
 - Description, location, and other identifying characteristics of the hardware component

- **Configuration**—During data collection, iLO collects data to enable proactive advice and consulting. Configuration data includes the following:
 - Server model
 - Serial number
 - Processor model, speed, and utilization
 - Storage capacity, speed, and utilization
 - Memory capacity, speed, and utilization
 - Firmware/BIOS
 - Installed drivers, services, and applications (if AMS is installed)
- **Active Health System**—During data collection, iLO collects data about the health, configuration, and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis.

More information

[Active Health System](#)
[Remote Support data collection](#)
[Remote support service events](#)

HPE Proactive Care service

HPE Proactive Care service customers must register their servers for remote support to receive the following Proactive Care features: Proactive Scan Report and Firmware and Software Version Report.

- The direct connect option requires the installation of AMS.
- The central connect option requires the installation of AMS or the SNMP/WBEM agents.

For more information, see the following website: <http://www.hpe.com/services/proactivecarecentral>.

Prerequisites for remote support registration

- The server supports embedded remote support registration through iLO. For more information, see [“Device support” \(page 129\)](#).

① IMPORTANT: If you use HPE OneView to manage your environment, use HPE OneView to register for remote support. For more information, see the HPE OneView documentation at <http://www.hpe.com/info/oneview/docs>.

- Your environment meets the requirements for remote support registration. For more information, see the Insight Remote Support and Insight Online setup guide for ProLiant Servers and BladeSystem c-Class Enclosures at the following website: <http://www.hpe.com/info/ilo/docs>.
- A supported version of the iLO firmware is installed.
 To address third-party software vulnerabilities, Hewlett Packard Enterprise recommends using iLO 4.2.03 or later.
- Optional: AMS is installed and the operating system is running on the server that you want to register.
 Hewlett Packard Enterprise recommends installing AMS.

HPE Proactive Care services customers only: AMS installation is required in order to receive the following Proactive Care features: Proactive Scan Report and Firmware and Software Version Report.

AMS is one way in which iLO can obtain the server name. If iLO cannot obtain the server name, the displayed server name in Insight Online and Insight RS is derived from the server serial number.

- If you do not install AMS, do one of the following to ensure that the server name is displayed correctly in Insight Online and Insight RS:

- For Windows systems only, start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.
- Configure the **Server Name** on the **Administration→Access Settings** page in the iLO web interface.

The server name is displayed in Insight Online and Insight RS, and can be viewed by Hewlett Packard Enterprise support and your authorized service provider, reseller/distributor, and installer. To protect your privacy, do not use sensitive information in the server name.

- The ProLiant iLO 3/4 Channel Interface Driver is installed.

This driver is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.

This driver ships standard with SUSE Linux Enterprise Server 11 and 12 and Red Hat Enterprise Linux 6 and 7, and it is automatically loaded.

For more information, see [“iLO drivers and utilities” \(page 32\)](#).

- The iLO time zone is set.

- A DNS server is configured in iLO.

This is required for communication between iLO and Insight Online.

- For Insight Remote Support central connect only: A supported version of the Insight RS software is installed and configured on the Insight RS host server.

For more information, see the following website: <http://www.hpe.com/support/InsightRS-Support-Matrix>.

- For Insight Remote Support central connect only: The RIBCL protocol credentials for the server are configured in the Insight RS Console.

For more information about the RIBCL protocol credentials, see the Insight Remote Support installation and configuration guide.

More information

[AMS and the Insight Management Agents](#)

[Configuring iLO SNTP settings](#)

[Configuring IPv4 settings](#)

[Configuring IPv6 settings](#)

Registering for remote support by using the iLO web interface

HPE remote support provides automatic submission of hardware events to Hewlett Packard Enterprise to prevent downtime and enable faster issue resolution. You can register directly to Hewlett Packard Enterprise or through an Insight RS Hosting Device.

Registering for Insight Online direct connect

When you register for Insight Online direct connect, you must complete steps in both the iLO web interface and the Insight Online portal.

Prerequisites

- Your environment meets the [prerequisites](#) for embedded remote support registration.
- Configure iLO Settings privilege.
- You have an HP Passport account. For more information, see <http://www.hpe.com/info/insightonline>.

Registering for Insight Online direct connect (step 1)

1. Navigate to the **Remote Support→Registration** page.
2. Select **Connect this server directly to HPE**.

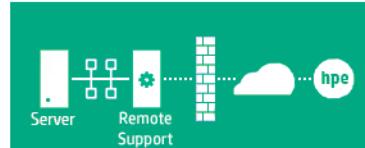
Get Connected to Hewlett Packard Enterprise

A connection to HPE provides you with a differentiated ownership experience for your server. This provides the ability to quickly identify and resolve issues in an automated, seamless and secure way. Read more: [Get Connected](#)

 This server is not registered

Select one of two ways to register:

 Connect this server directly to HPE

 Connect this server through an HPE remote support host server

Step 1 of 2: Register this server directly to HPE

Enter HPE Passport Credentials [Don't have an account?](#)

HPE Passport User ID
HPE Passport Password
Web Proxy Server
Web Proxy Port
Web Proxy Username
Web Proxy Password

I accept the [terms and conditions](#).

Connecting your server to HPE allows it to be remotely supported and to securely send diagnostic, configuration, telemetry and contact information to HPE. No other business information is collected and the data is managed according to the [privacy policy](#).

Register

3. Enter your HP Passport user ID and password.
4. Optional: Enter the following information if the server uses a web proxy server to access the Internet:
 - **Web Proxy Server**—Enter the host name or IP address.
 - **Web Proxy Port**

- **Web Proxy Username**
- **Web Proxy Password**

5. To accept the licensing terms and conditions, select the **I accept the terms and conditions** check box.

You can view these documents at the following website: <http://www.hpe.com/info/SWLicensing>.

6. Click **Register**.

iLO notifies you that Step 1 of the registration process is finished, and prompts you to complete Step 2.

Get Connected to Hewlett Packard Enterprise

⚠ Step 1 of connecting to Hewlett Packard Enterprise has been completed. Proceed to step 2 to complete the registration process.

Step 2 of 2: Complete your HPE Connected Products registration

Please go to www.hpe.com/support/hpesc and log in using your HPE Passport account to complete the registration process. You will be asked to provide your site, contact and partner information so that HPE can deliver service for your server. Allow up to 5 minutes for your registration request to be fully processed before your device will be visible in the HPE Support Center.

Confirm that you have completed the HPE Connected Products registration process.

Apply **Unregister**

Allow up to 5 minutes for your registration request to be fully processed.

Registering for Insight Online direct connect (step 2)

1. Navigate to the Insight Online website at <http://www.hpe.com/info/insightonline>, and then log in with your HP Passport credentials.
2. Follow the onscreen instructions in Insight Online, and provide your site, contact, and partner information so Hewlett Packard Enterprise can deliver service for your server.

To streamline the process when you have multiple servers to register, complete Step 1 for all of the servers, and then complete Step 2 for all of the servers during one Insight Online session.

For detailed instructions, see the Insight Remote Support and Insight Online setup guide for ProLiant servers and BladeSystem c-Class enclosures.

Confirming that registration is complete

1. Navigate to the **Remote Support**→**Registration** page.
2. Select the **Confirm that you have completed the HPE Connected Products registration process** check box, and then click **Apply**.

iLO notifies you that the registration process is finished.

Completing the post-registration steps

1. Optional: Send a test event to confirm the connection between iLO and HPE remote support. For instructions, see “[Sending a test service event](#)” (page 137).
2. Optional: If you want to receive email alerts about system events, configure AlertMail on the **Administration**→**Management**→**AlertMail** page in the iLO web interface. For more information, see “[iLO AlertMail](#)” (page 125).

Other Insight Online direct connect registration methods

You can also register a server for Insight Online direct connect by using the following:

- XML configuration and control scripts. For instructions, see the iLO scripting and CLI guide.
- Intelligent Provisioning. For instructions, see the Intelligent Provisioning documentation at the following website: <http://www.hpe.com/info/intelligentprovisioning/docs/>.

Editing the web proxy settings(Insight Online direct connect only)

If the web proxy settings change after a server is registered for remote support, update the settings to enable the server to continue sending data to Hewlett Packard Enterprise.

1. Navigate to the **Remote Support**→**Registration** page.
2. Update the following settings, as needed:
 - **Web Proxy Server**—Enter the hostname or IP address.
 - **Web Proxy Port**
 - **Web Proxy Username**
 - **Web Proxy Password**
3. Click **Apply**.

Registering for Insight Remote Support central connect

Prerequisites

- Your environment meets the [prerequisites](#) for embedded remote support registration.
- Configure iLO Settings privilege.

Registering for Insight Remote Support central connect

1. Navigate to the **Remote Support**→**Registration** page.
2. Select **Connect this server through an HPE remote support host server**.

Get Connected to Hewlett Packard Enterprise

A connection to HPE provides you with a differentiated ownership experience for your server. This provides the ability to quickly identify and resolve issues in an automated, seamless and secure way. Read more: [Get Connected](#)

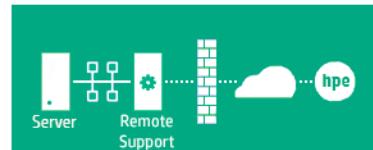


This server is not registered

Select one of two ways to register:



Connect this server directly to HPE



Connect this server through an HPE remote support host server

Connect this server through an HPE remote support host server

HPE remote support host server

Host server hostname or IP address

Port

7906

Connecting your server to HPE allows it to be remotely supported and to securely send diagnostic, configuration, telemetry and contact information to HPE. No other business information is collected and the data is managed according to the [privacy policy](#).

Register

3. Enter the **Host server hostname or IP address** and **Port** number.
The default port is 7906.
4. Click **Register**.
iLO notifies you that the registration process is finished.
5. Optional: Send a test event to confirm the connection between iLO and Insight Remote Support.
For instructions, see [“Sending a test service event” \(page 137\)](#).

Other Insight Remote Support central connect registration methods

You can also register a server for Insight Remote Support central connect by using the following:

- XML configuration and control scripts. For instructions, see the iLO scripting and CLI guide.
- Intelligent Provisioning. For instructions, see the Intelligent Provisioning documentation at the following website: <http://www.hpe.com/info/intelligentprovisioning/docs/>.
- Insight RS Console. For instructions, see the Insight Remote Support monitored devices configuration guide.

Unregistering from Insight Remote Support by using the iLO web interface

The process to unregister from remote support depends on whether you used the direct connect or central connect registration method.

Unregistering from Insight Online direct connect

Prerequisites

Configure iLO Settings privilege.

Unregistering a server from Insight Online direct connect

1. Navigate to the **Remote Support**→**Registration** page.
2. Click **Unregister**.
3. When prompted to confirm the request, click **OK**.
iLO notifies you that the server is no longer registered.

Unregistering from Insight Remote Support central connect

1. Log in to the Insight RS Console.
2. Do one of the following:
 - To stop monitoring a server temporarily, select the server on the **Devices**→**Device Summary** tab in the Insight RS Console, and then select **ACTIONS**→**DISABLE SELECTED**.
Unregistering the server directly from the iLO web interface is the same as temporarily disabling the server in the Insight RS Console.
 - To stop monitoring a server permanently, delete the server from the Insight RS Console.
To delete the server, select it on the **Device Summary** tab, and then select **ACTIONS**→**DELETE SELECTED**.
3. Navigate to the **Remote Support**→**Registration** page in the iLO web interface.
4. Verify that the server is not registered.

Remote support service events

Use the **Remote Support**→**Service Events** page to monitor service events, send test events, and set maintenance mode.

When iLO detects a hardware failure—for example, a problem with a memory DIMM or fan—a service event is generated. When a server is registered for remote support, the service event details are recorded in the **Service Event Log**, and the event is sent directly to Insight Online (direct connect) or to the Insight RS host server (central connect) which forwards it to Hewlett Packard Enterprise. When Hewlett Packard Enterprise receives a service event, a support case is opened (if warranted).

Using maintenance mode

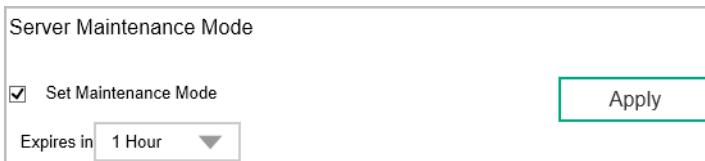
Use maintenance mode when you perform maintenance on a server. In maintenance mode, any events or messages that are sent to Insight RS or Insight Online are flagged to indicate that the event requires no action. This feature helps Hewlett Packard Enterprise to determine whether to open a support case.

Prerequisites

Configure iLO Settings privilege

Setting maintenance mode

1. Navigate to the **Remote Support**→**Service Events** page.
2. Select the **Set Maintenance Mode** check box.
3. Select a time from the **Expires in** menu.



4. Click **Apply**.

iLO notifies you that maintenance mode is set.

Maintenance mode ends automatically when the specified amount of time has passed. iLO notifies you when maintenance mode is cleared.



TIP: To end maintenance mode early, select the **Clear Maintenance Mode** check box, and then click **Apply**.

Sending a test service event

You can send a test event to verify that your remote support configuration is working correctly.

Prerequisites

Configure iLO Settings privilege.

Sending a test event

1. Navigate to the **Remote Support**→**Service Events** page.
2. Click **Send Test Event**.
3. When prompted to confirm the request, click **OK**.

When the transmission is completed, the test event is listed in the Service Event Log, the Insight RS Console (central connect only), and Insight Online.

If the test is successful, the **Submit Status** in the Service Event Log displays the text **No Error**.

The **Time Generated** column in the Service Event Log shows the date and time based on the configured iLO time zone.

Viewing the Service Event Log

Navigate to the **Remote Support**→**Service Events** page.

Service event log details

Service Event Log							
Clear Event Log							
Identifier	Time Generated	Event Id	Perceived Severity	Submit Status	Destination	Event Category	
5295ade2-d47a-e611-962c-10604b9211c2	09/14/16 15:42	1	2	No Error	Insight Online	HPQTEST0001	

The **Service Event Log** displays the following information for each service event:

- **Identifier**—A unique string that identifies the service event.
- **Time Generated**—The time the service event was generated. This column shows the date and time based on the configured iLO time zone.
- **Event ID**—A unique number for the service event type. [Table 4 \(page 138\)](#) lists the possible service events.
- **Perceived Severity**—The severity of the event indication (for example, 5-Major, 7-Fatal).
- **Submit Status**—The status of the event submission. If the status is **No error**, the event was submitted successfully.

- **Destination**—For Insight Remote Support central connect configurations, the host name or IP address and port of the Insight RS host server that received the service event. For Insight Online direct connect configurations, the value **Insight Online** is displayed.
- **Event Category**—The category of the event that matches the Message ID description in the message registry.

Supported service event types

The HPE remote support solution supports the following service event types:

Table 4 Service event types

Event ID	Description
1	Generic Test Service Event
100	Fan Failed Service Event
101	System Battery Failed Service Event
200	Power Supply Failed Service Event
300	Physical Disk Drive Service Event
301	Smart Array Controller Accelerator Battery Failure Event
302	Smart Array Controller Accelerator Board Status Changed Event
303	Smart Array Controller Status Changed Event
304	SAS Physical Drive Status Changed Event
305	ATA Disk Drive Status Changed Event
306	Fibre Channel Host Controller Status Changed Event
400	Memory Module Failed or Predicted to Fail Event
500	Storage System Fan Status Changed Event
501	Storage System Power Supply Status Changed Event

Clearing the Service Event Log

Prerequisites

Configure iLO Settings privilege

Clearing the log

1. Navigate to the **Remote Support**→**Service Events** page.
2. Click **Clear Event Log**.
iLO prompts you to confirm the request.
3. Click **OK**.
iLO notifies you that the service event log has been cleared.

Remote Support data collection

Use the **Remote Support**→**Data Collections** page to view information about the data that is sent to Hewlett Packard Enterprise when a server is registered for remote support. You can also use this page to send data collection information to Hewlett Packard Enterprise manually when a device configuration changes and you do not want to wait for the next scheduled data collection transmission.

Data collection information

Depending on your remote support configuration, iLO or the Insight RS host server sends configuration information to Hewlett Packard Enterprise for analysis and proactive services in accordance with your warranty and service agreements.

- For Insight Online direct connect, this data is transmitted every 30 days. You cannot edit or delete the data collection schedule.
- For Insight Remote Support central connect, the data transmission frequency is configured in the Insight RS Console. For more information, see the Insight RS online help.

Active Health System reporting

Depending on whether you use Insight Online direct connect or Insight Remote Support central connect, iLO or the Insight RS host server sends server health, configuration, and run-time telemetry information to Hewlett Packard Enterprise. This information is used for troubleshooting issues and closed-loop quality analysis.

- For Insight Online direct connect configurations, this data is transmitted every seven days. You cannot edit or delete the Active Health System reporting schedule.
- For Insight Remote Support central connect, this data is transmitted every seven days. You can change the day of the week for Active Health System reporting transmission in the Insight RS Console. For more information, see the Insight RS online help.

Sending data collection information

Prerequisites

Configure iLO Settings privilege.

Sending data collection information

1. Navigate to the **Remote Support**→**Data Collections** page.
2. Click **Send Data Collection**.
3. When prompted to confirm the request, click **OK**.

When the transmission is completed, the **Last Data Collection Transmission** and **Last Data Collection Transmission Status** are updated. The date and time are based on the configured iLO time zone.

Data Collection Information	
iLO sends information about the server configuration to HPE on a periodic basis for analysis and proactive services consistent with your warranty and existing service agreements. This information is transmitted every thirty days.	
Data Collection Frequency (days):	30
Last Data Collection Transmission:	2016-09-14 15:34
Last Data Collection Transmission Status:	No Error
Next Data Collection Scheduled:	2016-10-14 19:02
Send Data Collection	

Viewing data collection status in iLO

Navigate to the **Remote Support**→**Data Collections** page.

Data Collection details

- **Last Data Collection Transmission**—The date and time of the last data collection.
- **Last Data Collection Transmission Status**—The status of the last data transmission.
- **Data Collection Frequency (days)** (Insight Online direct connect only)—The frequency at which data is sent to Hewlett Packard Enterprise.
- **Next Data Collection Scheduled** (Insight Online direct connect only)—The next date and time when data will be sent to Hewlett Packard Enterprise.

Sending Active Health System reporting information

Prerequisites

Configure iLO Settings privilege.

Sending Active Health System Information

1. Navigate to the **Remote Support**→**Data Collections** page.
2. Click **Send Active Health System Report**.
3. When prompted to confirm the request, click **OK**.

The collected data includes Active Health System information from the last seven days.

When the transmission is completed, the **Last Active Health System Reporting Transmission** and **Last Active Health System Reporting Transmission Status** are updated. The date and time are based on the configured iLO time zone.

Active Health System Reporting Information	
iLO provides information on the health, configuration and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis. This information is transmitted every seven days.	
Active Health System Reporting Frequency (days):	7
Last Active Health System Reporting Transmission:	-
Last Active Health System Reporting Transmission Status:	No Error
Next Active Health System Reporting Scheduled:	2016-09-21 19:02
Send Active Health System Report	

You can also download Active Health System information manually and send it to Hewlett Packard Enterprise. For instructions, see [“Active Health System” \(page 189\)](#).

Viewing Active Health System reporting status in iLO

Navigate to the **Remote Support**→**Data Collections** page.

Active Health System reporting details

- **Last Active Health System Reporting Transmission**—The date and time of the last Active Health System report.
- **Last Active Health System Reporting Transmission Status**—The status of the last data transmission.
- **Active Health System Reporting Frequency (days)** (Insight Online direct connect only)—The frequency at which Active Health System data is sent to Hewlett Packard Enterprise.
- **Next Active Health System Reporting Scheduled** (Insight Online direct connect only)—The next date and time when Active Health System data will be sent to Hewlett Packard Enterprise.

11 Managing iLO with the ROM-based utilities

iLO ROM-based utilities

You can use ROM-based utilities to configure iLO. The ROM-based utility embedded in the system ROM of your server depends on your server model.

You can access the ROM-based utilities from the physical system console, or by using an iLO remote console session.

- ProLiant Gen8 servers, except for the DL580 Gen8 server, have the iLO RBSU software embedded in the system ROM.
- ProLiant Gen9 servers, Synergy compute modules, and the DL580 Gen8 server have the UEFI System Utilities software embedded in the system ROM.

Configuring network settings with the ROM-based utilities

Configuring NIC and TCP/IP settings (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **Network**→**NIC and TCP/IP**.
5. From the **Network Configuration** screen, view or update the NIC and TCP/IP settings.
6. To save your changes, press **F10**
7. Select **File**→**Exit**.

More information

[Network Options](#)

Configuring DNS/DHCP settings (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **Network**→**DNS/DHCP**, and press **Enter**.
5. From the **Network Autoconfiguration** screen, view or update the DNS and DHCP settings.
6. To save your changes, press **F10**
7. Select **File**→**Exit**.

More information

[Network Options](#)

Configuring Advanced network settings (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **Network**→**DNS/DHCP**, and press **Enter**.
5. Press **F1**

6. From the **Advanced Autoconfiguration Setup and Status** screen, view or update the advanced network settings.
7. To save your changes, press **F10**.
8. Select **File**→**Exit**.

More information

[Advanced Network Options](#)

Configuring Network Options (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Network Options**, and press **Enter**.
5. Select any of the Network Options and press **Enter**, then select a setting or enter a value for that option and press **Enter** again.
6. Press **F10**.
7. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

More information

[Network Options](#)

Configuring Advanced Network Options (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Advanced Network Options**, and press **Enter**.
5. Select any of the Advanced Network Options and press **Enter**, then select a setting or enter a value for that option and press **Enter** again.
6. Press **F10**.
7. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

More information

[Advanced Network Options](#)

Network Options

- **MAC Address** (read-only)—The MAC address of the selected iLO network interface.
- **Network Interface Adapter**—Specifies the iLO network interface adapter to use.
 - **ON**—Uses the iLO Dedicated Network Port.
 - **Shared Network Port**—Uses the Shared Network Port. This option is only available on supported servers.
 - **OFF**—Disables all network interfaces to iLO.
- **Transceiver Speed Autoselect** (iLO Dedicated Network Port only)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network. This option is only available when **Network Interface Adapter** is set to **ON**.
- **Transceiver Speed Manual Setting** (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface. This option is only available when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
- **Transceiver Duplex Setting** (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface. This option is only available when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
- **VLAN Enable** (Shared Network Port only)—Enables the VLAN feature.

When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.
- **VLAN ID** (Shared Network Port only)—When a VLAN is enabled, specifies a VLAN tag. All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094. This option is only available when **Network Interface Adapter** is set to **Shared Network Port**.
- **DHCP Enable**—Configures iLO to obtain its IP address (and many other settings) from a DHCP server.
- **DNS Name**—Sets the DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`).

This name can only be used if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.
- **IP Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- **Gateway IP Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.

Advanced Network Options

- **Gateway from DHCP**—Specifies whether iLO uses a DHCP server-supplied gateway.
- **Gateway #1, Gateway #2, and Gateway #3**—If **Gateway from DHCP** is disabled, specifies up to three iLO gateway IP addresses.
- **DHCP Routes**—Specifies whether iLO uses the DHCP server-supplied static routes.

- **Route 1, Route 2, and Route 3**—If **DHCP Routes** is disabled, specifies the iLO static route destination, mask, and gateway addresses.
- **DNS from DHCP**—Specifies whether iLO uses the DHCP server-supplied DNS server list.
- **DNS Server 1, DNS Server 2, DNS Server 3**—If **DNS from DHCP** is disabled, specifies the primary, secondary, and tertiary DNS servers.
- **WINS from DHCP**—Specifies whether iLO uses the DHCP server-supplied WINS server list.
- **Register with WINS Server**—Specifies whether iLO registers its name with a WINS server.
- **WINS Server #1 and WINS Server #2**—If **WINS from DHCP** is disabled, specifies the primary and secondary WINS servers.
- **Domain Name**—The iLO domain name. If DHCP is not used, specifies a domain name.

Configuring access settings with the ROM-based utilities

Configuring global settings (iLO RBSU)

1. Optional: If you will access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **Settings**→**Configure**, and press **Enter**.
5. From the **Global iLO 4 Settings** screen, select an option and press the **spacebar** to toggle the setting to **ENABLED** or **DISABLED**.
6. To save the settings, press **F10**.
7. To close iLO RBSU, select **File**→**Exit**.

More information

[Access options](#)

Configuring serial CLI options (iLO RBSU)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **Settings**→**CLI**, and press **Enter**.
5. From the **Configure iLO Command-Line Interface** screen, select an option and press the **spacebar** to toggle through the available settings.
6. To save the changed settings, press **F10**
7. To close iLO RBSU, select **File**→**Exit**.

More information

[Access options](#)

Configuring access settings (iLO 4 Configuration Utility)

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.

4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Setting Options**, and press **Enter**.
5. View or update the access settings.
6. Press **F10**.
7. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

More information

[Access options](#)

Viewing information about iLO by using the iLO 4 Configuration Utility

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen to start the UEFI System Utilities.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**About**, and press **Enter**.
5. View information [about](#) iLO components.
6. Press **Esc** until the main menu is displayed.
7. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
8. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

About

Use this menu to view information about the following iLO components.

- **Firmware Date**—The iLO firmware revision date.
- **Firmware Version**—The iLO firmware version.
- **iLO CPLD Version**—The iLO complex programmable logic device version.
- **Host CPLD Version**—The server complex programmable logic device version.
- **Serial Number**—The iLO serial number.
- **RBSU Date**—The iLO 4 Configuration Utility revision date.
- **PCI BUS**—The PCI bus to which the iLO processor is attached.
- **Device**—The device number assigned to iLO in the PCI bus.

12 Using the iLO web interface

iLO web interface

You can use the iLO web interface to manage iLO. You can also use a Remote Console, XML configuration and control scripts, SMASH CLP, or the iLO RESTful API.

For more information, see the iLO and iLO RESTful API documentation at the following website:
<http://www.hpe.com/info/ilo/docs>.

Browser support

The iLO web interface requires a browser that meets the following requirements:

- **JavaScript**—The iLO web interface uses client-side JavaScript extensively. This setting is not enabled by default in all versions of Internet Explorer. To check or change this setting, see “[Configuring the Internet Explorer JavaScript setting](#)” (page 146).
- **Cookies**—Cookies must be enabled for certain features to function correctly.
- **Pop-up windows**—Pop-up windows must be enabled for certain features to function correctly. Verify that pop-up blockers are disabled.
- **TLS**—To access the iLO web interface, you must enable TLS 1.0 or later in your browser.

For a list of supported browsers, see [Table 5 \(page 146\)](#).

Table 5 Supported browsers

iLO 4 firmware version	Internet Explorer	Firefox	Chrome
1.01	7, 8, 9	3.6, ESR 10	
1.05	7, 8, 9	ESR 10	Latest version
1.10	7, 8, 9	ESR 10	Latest version
1.13	7, 8, 9	ESR 10	Latest version
1.20	7, 8, 9	ESR 10	Latest version
1.30	8, 9, 10	ESR 17	Latest version
1.40	8, 10	ESR 24	Latest version
1.50	8, 11	ESR 24	Latest version
2.00	8, 11	ESR 24	Latest version
2.10	8, 11	ESR 31	Latest version
2.20	8, 11	ESR 31	Latest version
2.30	8, 11	ESR 31	Latest version
2.40	11	Latest version	Latest version
2.50	Latest version	Latest version	Latest version

Configuring the Internet Explorer JavaScript setting

Some versions of Internet Explorer have JavaScript disabled by default.

1. Start Internet Explorer.
2. Select **Tools**→**Internet Options**.
3. Click **Security**.
4. Click **Custom level**.

5. Set the **Scripting→Active scripting** setting to **Enable**.
6. Click **OK**.
7. Refresh your browser window.

Logging in to the iLO web interface

1. Enter `https://<iLO host name or IP address>`.
You must access the iLO web interface through HTTPS (HTTP exchanged over an SSL encrypted session).
2. Do one of the following:
 - On the login page, enter a directory or local user account name and password, and then click **Log In**.
 - Click the **Zero Sign In** button.
If iLO is configured for Kerberos network authentication, the **Zero Sign In** button is displayed below the **Log In** button. Clicking the **Zero Sign In** button logs the user in to iLO without requiring the user to enter a user name and password.

For information about login security and login issues, see “[Login security](#)” (page 70) and “[Login and iLO access issues](#)” (page 322).

After an initial failed login attempt, the iLO firmware imposes a login delay. For more information about the login delay settings, see “[iLO access settings](#)” (page 61).

Cookie sharing between browser instances and iLO

When you browse to iLO and log in, one session cookie is shared with all open browser windows that share the same iLO URL in the browser address bar. As a consequence, all open browser windows share one user session. Logging out in one window ends the user session in all of the open windows. Logging in as a different user in a new window replaces the session in the other windows.

This behavior is typical of browsers. iLO does not support multiple users logged in from two different browser windows in the same browser on the same client.

Shared instances

When the iLO web interface opens another browser window or tab (for example, a help file), this window shares the connection to iLO and the session cookie.

When you are logged in to the iLO web interface, and you open a new browser window manually, a duplicate instance of the original browser window opens. If the domain name in the address bar matches the original browser session, the new instance shares a session cookie with the original browser window.

Cookie order

During login, the login page builds a browser session cookie that links the window to the appropriate session in the iLO firmware. The firmware tracks browser logins as separate sessions listed in the **Active Sessions** section of the **iLO Overview** page.

For example, when User1 logs in, the web server builds the initial frames view, with User1 listed in the top pane, menu items in the left pane, and page data in the lower right pane. When User1 clicks from link to link, only the menu items and page data are updated.

While User1 is logged in, if User2 opens a browser window on the same client and logs in, the second login overwrites the cookie generated in the User1 session. Assuming that User2 is a different user account, a different current frame is built, and a new session is granted. The second session appears in the **Active Sessions** section of the **iLO Overview** page as User2.

The second login has effectively orphaned the first session by overriding the cookie generated during the User1 login. This behavior is the same as closing the User1 browser without clicking the **Sign Out** button. The User1 orphaned session is reclaimed when the session timeout expires.

Because the current user frame is not refreshed unless the browser is forced to refresh the entire page, User1 can continue navigating by using the browser window. However, the browser is now operating by using the User2 session cookie settings, even though it might not be readily apparent.

If User1 continues to navigate in this mode (User1 and User2 sharing a process because User2 logged in and reset the session cookie), the following might occur:

- User1 session behaves consistently with the privileges assigned to User2.
- User1 activity keeps User2 session alive, but User1 session can time out unexpectedly.
- Logging out of either window causes both sessions to end. The next activity in the other window can redirect the user to the login page as if a session timeout or premature timeout occurred.
- Clicking **Sign Out** from the second session (User2) results in the following warning message:
Logging out: unknown page to display before redirecting the user to the login page.
- If User2 logs out and then logs back in as User3, User1 assumes the User3 session.
- If User1 is at login, and User2 is logged in, User1 can alter the URL to redirect to the index page. It appears as if User1 has accessed iLO without logging in.

These behaviors continue as long as the duplicate windows are open. All activities are attributed to the same user, using the last session cookie set.

Displaying the current session cookie

After logging in, you can force the browser to display the current session cookie by entering the following in the URL navigation bar:

```
javascript:alert(document.cookie)
```

The first field visible is the session ID. If the session ID is the same among the different browser windows, these windows are sharing iLO session.

You can force the browser to refresh and reveal your true identity by pressing **F5**, selecting **View→Refresh**, or clicking the **Refresh** button.

Best practices for preventing cookie-related issues

- Start a new browser for each login by double-clicking the browser icon or shortcut.
- To close an iLO session before you close the browser window, click the **Sign Out** button.

Using the iLO controls

When you log in to the iLO web interface, the controls at the bottom of the browser window are available from any iLO page.

- **POWER**—Use this menu to access the Virtual Power features.
- **UID**—Use this button to turn the UID LED on and off.
- **Language**—Use this menu to select a language or to navigate to the **Access Settings - Language** page, where you can install a language pack and configure other language-related settings. This option is available only if a language pack is installed.
- **Health icon**—Use this icon to view the overall health status for the server fans, temperature sensors, and other monitored subsystems. To view the status of the monitored components,

click the icon. For all components except AMS, select a component to view more information about the component status.

Starting a remote management tool from the login page

1. Navigate to the iLO login page.

When iLO is under the control of a remote management tool, the iLO web interface displays a message similar to the following:

This system is being managed by <remote management tool name>. Changes made locally in iLO will be out of sync with the centralized settings, and could affect the behavior of the remote management system.

2. The name of the remote management tool is a link. To start the remote management tool, click the link.

Language pack support

If a language pack is installed in iLO, a language menu is available on the login screen for you to select the language for the iLO session. This selection is saved in a browser cookie for future use.

13 Viewing iLO overview and system information

Viewing iLO overview information

Navigate to the **Information**→**Overview** page.

The **iLO Overview** page displays high-level details about the server and the iLO subsystem, as well as links to commonly used features.

System information



- **Server Name**—The server name defined by the host operating system. To navigate to the **Access Settings** page, click the **Server Name** link
- **Product Name**—The product with which this iLO processor is integrated.
- **UUID**—The universally unique identifier that software uses to identify this host. This value is assigned when the system is manufactured.
- **UUID (Logical)**—The system UUID that is presented to host applications. This value is displayed only when set by other software, such as HPE Virtual Connect Enterprise Manager. This value might affect operating system and application licensing. The **UUID (Logical)** value is set as part of the logical server profile that is assigned to the system. If the logical server profile is removed, the system **UUID** value reverts from the **UUID (Logical)** value to the **UUID** value. If no **UUID (Logical)** value is set, this item is not displayed.
- **Server Serial Number**—The server serial number, which is assigned when the system is manufactured. You can change this value by using the system RBSU or the UEFI System Utilities during POST.
- **Serial Number (Logical)**—The system serial number that is presented to host applications. This value is displayed only when set by other software, such as HPE Virtual Connect Enterprise Manager. This value might affect operating system and application licensing. The **Serial Number (Logical)** value is set as part of the logical server profile that is assigned to the system. If the logical server profile is removed, the serial number value reverts from the **Serial Number (Logical)** value to the **Server Serial Number** value. If no **Serial Number (Logical)** value is set, this item is not displayed.
- **Chassis Serial Number**—The serial number of the chassis that contains the server node. This information is displayed for servers with chassis firmware version 6.0 or later.

- **Product ID**—This value distinguishes between different systems with similar serial numbers. The product ID is assigned when the system is manufactured. You can change this value by using the system RBSU or the UEFI System Utilities during POST.
- **System ROM**—The version of the active system ROM.
- **System ROM Date**—The date of the active system ROM.
- **Backup System ROM**—The version of the backup system ROM. If a system ROM update fails or is rolled back, the backup system ROM is used. This value is displayed only if the system supports a backup system ROM.
- **Integrated Remote Console**—Provides links to start the .NET IRC or Java IRC for remote, out-of-band communication with the server console. When you use the Java IRC:
 - For environments with Windows or Linux and the Oracle JRE—Use the **Java Web Start** link.
 - For environments with Linux and the OpenJDK JRE—Use the **Java Applet** link.
- **License Type**—The level of licensed iLO firmware functionality.
- **iLO Firmware Version**—The version and date of the installed iLO firmware. To navigate to the **Firmware Update** page, click the **iLO Firmware Version** link.
- **IP Address**—The network IP address of the iLO subsystem.
- **Link-Local IPv6 Address**—The SLAAC link-local address of the iLO subsystem. To navigate to the **Network Summary** page, click the **Link-Local IPv6 Address** link. This value is displayed only for iLO Dedicated Network Port configurations.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. By default, the hostname is **iLO**, followed by the system serial number and the current domain name. This value is used for the network name and must be unique.

System status details

Status	
System Health	OK
Server Power	ON
UID Indicator	UID OFF
TPM Status	Not Present
SD-Card Status	Not Present
iLO Date/Time	Thu Sep 15 15:50:10 2016

- **System Health**—The server health indicator. This value summarizes the condition of the monitored subsystems, including overall status and redundancy (ability to handle a failure). Lack of redundancy in any subsystem at startup will not degrade the system health status. To navigate to the **Health Summary** page, click the **System Health** link.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.

You can change the UID LED state to **UID ON** or **UID OFF** by using the UID buttons on the server chassis or the UID control at the bottom of the iLO web interface window.

When the UID LED is blinking, the **UID Indicator** displays the status **UID BLINK**. When the UID LED stops blinking, the status reverts to the previous value (**UID ON** or **UID OFF**). If a

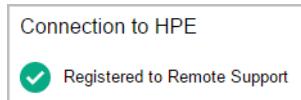
new state is selected while the UID LED is blinking, that state takes effect when the UID LED stops blinking.

⚠ **CAUTION:** The UID LED blinks automatically to indicate that a critical operation is underway on the host, such as Remote Console access or a firmware update. Do not remove power from a server when the UID LED is blinking.

- **TPM Status or TM Status**—The status of the TPM or TM socket or module.
- **Module Type**—The TPM or TM type and specification version. The possible values are **TPM 1.2**, **TPM 2.0**, **TM 1.0**, **Not Specified**, and **Not Supported**. This value is displayed when a TPM or TM is present on a server.
- **SD-Card Status**—The status of the internal SD card. If present, the number of blocks in the SD card is displayed.
- **iLO Date/Time**—The internal clock of the iLO subsystem.

HPE remote support status

The **Connection to HPE** section shows the remote support registration status for supported servers.



The possible status values follow:

- **Registered to Remote Support**—The server is registered.
- **Registration incomplete**—The server is registered for Insight Online direct connect remote support, but step 2 of the registration process is incomplete.
- **Not registered**—The server is not registered.
- **Unable to retrieve the HPE Remote Support information**—The registration status could not be determined.
- **Remote Support Registration Error**—A remote support connection error occurred.

Active sessions list

The **iLO Overview** page displays the following information about all users logged in to iLO.

Active Sessions		
User	IP Address	Source
Local User:		HTTPS

- Login name
- IP address
- Source (for example, HTTPS, Remote Console, or SSH)

Viewing system information with iLO

The **iLO System Information** page displays the health of the monitored subsystems and devices.

The information that you can view depends on whether you are using Agentless Management or SNMP Pass-thru, and whether AMS is installed. For more information, see “[iLO SNMP management](#)” (page 112).

The **System Information** page includes the following embedded health tabs:

- [Summary](#)
- [Fans](#)
- [Temperatures](#)
- [Power](#)
- [Processors](#)
- [Memory](#)
- [Network](#)
- [Device Inventory](#)
- [Storage](#)
- [Firmware](#)
- [Software](#)

Viewing health summary information

Navigate to the **Information**→**System Information** page, and then click the **Summary** tab.

The **Health Summary** page displays the status of monitored subsystems and devices. Depending on the server configuration, the information on this page varies.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Subsystems and Devices	
Subsystems and Devices	Status
Agentless Management Service	 OK
BIOS/Hardware Health	 OK
Fans	 OK
Memory	 OK
Network	 OK
Power Supplies	 OK
Processors	 OK
Storage	 OK
Temperatures	 OK

Redundancy status

Redundancy status is displayed for the following:

- **Fan Redundancy**
- **Power Status**

Subsystem and device status

Summarized status information is displayed for the following:

- **BIOS/Hardware Health**
- **Fans**
- **Memory**
- **Network**

- **Power Supplies** (nonblade servers only)
- **Processors**
- **Storage**
- **Temperatures**
- **Smart Storage Battery Status** (supported servers only)
- **Agentless Management Service**

Subsystem and device status values

The **Health Summary** page uses the following status values:

-  **Redundant**—There is a backup component for the device or subsystem.
-  **OK**—The device or subsystem is working correctly.
-  **Not Redundant**—There is no backup component for the device or subsystem.
-  **Not Available**—The component is not available or not installed.
-  **Degraded**—The device or subsystem is operating at a reduced capacity.

Previous versions of iLO used a status of **Mismatched** to indicate the presence of mismatched power supplies. iLO 4 displays the power supply status as **Degraded** when mismatched power supplies are installed.

If you power on a server with nonredundant fans or power supplies, the system health status is listed as **OK**. However, if a redundant fan or power supply fails while the system is powered on, the system health status is listed as **Degraded** until you replace the fan or power supply.

-  **Failed Redundant**—The device or subsystem is in a nonoperational state.
-  **Failed**—One or more components of the device or subsystem are nonoperational.
-  **Other**—For more information, navigate to the **System Information** page of the component that is reporting this status.
-  **Link Down**—The network link is down.
-  **Unknown**—The iLO firmware has not received data about the device status. If iLO was reset when the server was powered off, some subsystems display the status **Unknown** because the status cannot be updated when the server is powered off.
-  **Not Installed**—The subsystem or device is not installed.

Viewing fan information

1. Navigate to the **Information**→**System Information** page, and then click the **Fans** tab.
2. Optional: On servers that support fan redundancy, empty fan bays are hidden. To view the empty fan bays, click **show empty bays**. When empty fan bays are displayed, click **hide empty bays** to hide them.

The information displayed on the **Fan Information** page varies depending on the server configuration.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Fan details

Fans				
Fan	Location	▲ Status	Speed	
Fan 1	System	OK	6%	

The following details are displayed for each fan:

- **Fan**—The fan name.
- **Location**—For nonblade servers, the location in the server chassis is listed. For server blades, the virtual fan is listed with the location **Virtual**.
- **Status**—The fan health status.
For more information, see [“Subsystem and device status values” \(page 154\)](#).
- **Speed**—The fan speed (percent).

Fans

The iLO firmware, in conjunction with the hardware, controls the operation and speed of the fans. Fans provide essential cooling of components to ensure reliability and continued operation. The fans react to the temperatures monitored throughout the system to provide sufficient cooling with minimal noise.

Monitoring the fan subsystem includes the sufficient, redundant, and nonredundant fan configurations. If one or more fans fail, the server still provides sufficient cooling to continue operation.

Fan operation policies might differ from server to server based on fan configuration and cooling demands. Fan control monitors the internal temperature of the system, increasing the fan speed to provide more cooling, and decreasing the fan speed when cooling is sufficient. If a fan failure occurs, fan operation policies might increase the speed of the other fans, record the event in the IML, or turn on LED indicators.

In nonredundant configurations, or redundant configurations where multiple fan failures occur, the system might be incapable of providing sufficient cooling to protect the server from damage and to ensure data integrity. In this case, in addition to the cooling policies, the system might start a graceful shutdown of the operating system and server.

Server blades use the enclosure fans to provide cooling because they do not have internal fans. The enclosure fans are called *virtual fans* on the **Fans** tab. The **Virtual** fan reading represents the cooling amount that a server blade is requesting from the enclosure. The server blade calculates the amount of required cooling by examining various temperature sensors and calculating an appropriate fan speed. The enclosure uses information from all of the installed server and nonserver blades to adjust the fans to provide the appropriate enclosure cooling.

Temperature information

The **Temperature Information** page includes a temperature graph and a table that displays the location, status, temperature, and threshold settings of temperature sensors in the server chassis.

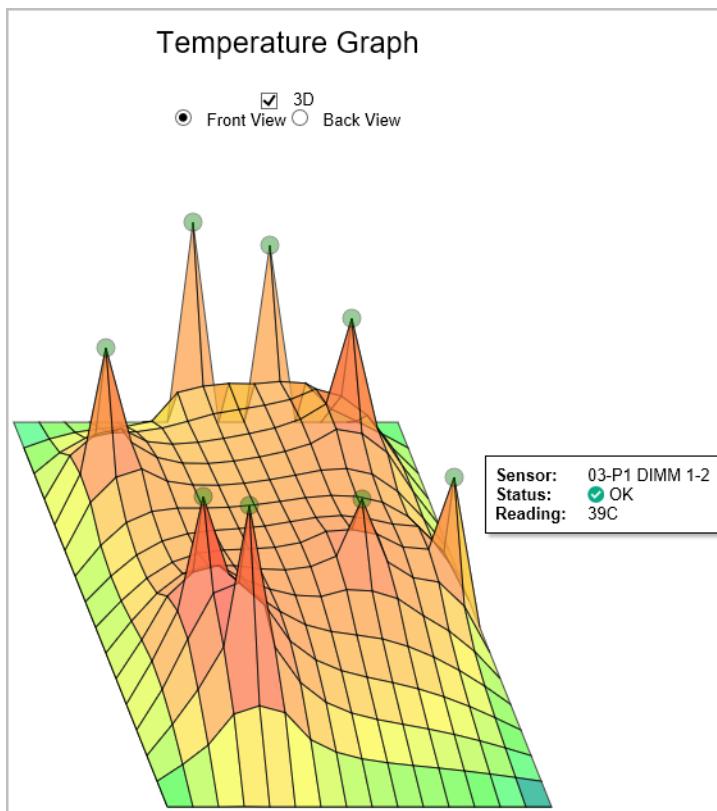
If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Viewing the temperature graph

1. Navigate to the **Information**→**System Information** page, and then click the **Temperatures** tab.

2. Optional: Customize the graph display.
 - Select the **3D** check box to display a three-dimensional graph.
 - Clear the **3D** check box to display a two-dimensional graph.
 - Select **Front View** or **Back View** to display the sensors located at the front or back of the server.
3. Optional: Move the mouse over a circle on the graph to view individual sensor details. The sensor ID, status, and temperature reading are displayed.

Temperature graph details



When you view the temperature graph, the circles on the graph correspond to the sensors listed in the **Sensor Data** table.

The color on the graph is a gradient that ranges from green to red. Green represents a temperature of 0°C and red represents the critical threshold. As the temperature of a sensor increases, the graph color changes from green to amber, and then to red if the temperature approaches the critical threshold.

Viewing temperature sensor data

1. Navigate to the **Information**→**System Information** page, and then click the **Temperatures** tab.
2. Optional: When temperatures are displayed in Celsius, click the **Show values in Fahrenheit** button to change the display to Fahrenheit. When temperatures are displayed in Fahrenheit, click the **Show values in Celsius** button to change the display to Celsius.
3. Optional: By default, sensors that are not installed are hidden. To view the missing sensors, click **show missing sensors**. When missing sensors are displayed, click **hide missing sensors** to hide them.

Temperature sensor details

Sensor Data (show missing sensors)						
Show values in Fahrenheit						
Sensor	Location	X	Y	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	3	0	OK	-1C	Caution: 42C; Critical: 46C
02-CPU	CPU	10	6	OK	40C	Caution: 70C; Critical: N/A
03-P1 DIMM 1-2	Memory	14	7	OK	39C	Caution: 87C; Critical: N/A
05-Chipset	System	4	2	OK	65C	Caution: 105C; Critical: N/A
06-Chipset Zone	System	3	4	OK	54C	Caution: 68C; Critical: 73C
07-VR P1 Zone	System	9	12	OK	0C	Caution: 88C; Critical: 93C
09-iLO Zone	System	7	15	OK	52C	Caution: 72C; Critical: 77C
11-PCI 1 Zone	I/O Board	2	11	OK	46C	Caution: 64C; Critical: 69C
12-Sys Exhaust	Chassis	10	15	OK	46C	Caution: 68C; Critical: 73C
13-LOM	System	12	12	OK	47C	Caution: 100C; Critical: N/A

- **Sensor**—The ID of the temperature sensor, which also gives an indication of the sensor location.
- **Location**—The area where the temperature is being measured.

In this column, **Memory** refers to the following:

- Temperature sensors located on physical memory DIMMs.
- Temperature sensors located close to the memory DIMMs, but not located on the DIMMs. These sensors are located further down the airflow cooling path, near the DIMMs, to provide additional temperature information.

The ID of the temperature sensor in the **Sensor** column helps to pinpoint the location, providing detailed information about the DIMM or memory area.

- **X**—The x-coordinate of the temperature sensor.
- **Y**—The y-coordinate of the temperature sensor.
- **Status**—The temperature status.
- **Reading**—The temperature recorded by the temperature sensor. If a temperature sensor is not installed, the **Reading** column shows the value **N/A**.
- **Thresholds**—The temperature thresholds for the warning for overheating conditions. The two threshold values are **Caution** and **Critical**. If a temperature sensor is not installed, the **Thresholds** column shows the value **N/A**.

Temperature monitoring

The following temperature thresholds are monitored:

- **Caution**—The server is designed to maintain a temperature below the caution threshold. If the temperature exceeds the caution threshold, the fan speeds are increased to maximum. If the temperature exceeds the caution threshold for 60 seconds, a graceful server shutdown is attempted.
- **Critical**—If temperatures are uncontrollable or rise quickly, the critical temperature threshold prevents system failure by physically shutting down the server before the high temperature causes an electronic component failure.

Monitoring policies differ depending on the server requirements. Policies usually include increasing fan speeds to maximum cooling, logging temperature events in the IML, providing a visual indication of events by using LED indicators, and starting a graceful shutdown of the operating system to avoid data corruption.

Additional policies are implemented after an excessive temperature condition is corrected, including returning the fan speed to normal, recording the event in the IML, turning off the LED indicators, and canceling shutdowns in progress (if applicable).

Viewing power information

Navigate to the **Information**→**System Information** page, and then click the **Power** tab.

The information displayed on the **Power Information** page varies depending on the server type.

- **Nonblade servers (DL, ML)**—The page displays the following sections: **Power Supply Summary**, **Power Supplies**, **HPE Power Discovery Services** (if available), and **Smart Storage Battery** (supported servers only).
- **Nonblade servers (SL, XL)**—The page displays the following section: **Power Supply Summary**.
More power information is displayed on the **Chassis Information** page. For more information, see “[Viewing chassis information](#)” (page 259).
- **Server blades and Synergy compute modules**—The page displays the following sections: **Power Readings**, **Power Microcontroller**, and **Smart Storage Battery** (supported servers only).

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Power Supply Summary details

Power Supply Summary	
Present Power Reading	N/A
Power Management Controller Firmware Version	N/A
Power Status	<input checked="" type="checkbox"/> OK
HPE Power Discovery Services Status	N/A
High Efficiency Mode	N/A

Present Power Reading

When HPE Common Slot Power Supplies are present, the most recent power reading from the server is displayed. Other power supplies do not provide this data.

Although this value is typically equal to the sum of all active power supply outputs, there might be some small variance as a result of reading the individual power supplies. This value is a guideline value and is not as accurate as the values presented on the **Power Management** pages. For more information, see “[Viewing server power usage](#)” (page 249).

Power Management Controller Firmware Version

The firmware version of the power management controller. The server must be powered on for the iLO firmware to determine this value. This feature is not available on all servers.

Power Status

The overall status of the power supplied to the server.

- If the server power supplies are connected to a nonintelligent power source, this section displays the status of the internal server power supplies.
- If the server power supplies are connected to Power Discovery Services through an iPDU, this section displays the status of the power supplied to the internal server power supplies.

Possible **Power Status** values follow:

- **Redundant**—Indicates that the power supplies are in a redundant state. If Power Discovery Services is integrated into the infrastructure, this value indicates whether the externally supplied power to the internal power supplies is redundant.
- **Not Redundant**—Indicates that at least one of the power supplies or iPDU (if Power Discovery Services is used) is not supplying power to the server. The most common reason for this status is a loss of input power to the power supply. Another reason for this status is a configuration with multiple power supplies connected to the same iPDU. In this case, the individual power supply status is **Good, In Use**, but the **Power Status** value is **Not Redundant** because the loss of input power to the iPDU would lead to a total loss of power to the server.
- **OK**—A Common Slot Power Supply is not installed. The installed power supply is working correctly.
- **N/A**—Only one power supply is installed. Redundancy is not applicable in this configuration.

HPE Power Discovery Services Status

The possible values follow:

- **Redundant**—The server is configured for a redundant iPDU configuration.
- **Not Redundant**—There are not sufficient iPDU to support redundancy, or the server power supplies are connected to the same iPDU.
- **N/A**—No iPDU were discovered.

When the iLO processor or the server is reset, the iPDU discovery process might take a few minutes to complete.

High Efficiency Mode

The redundant power supply mode that will be used when redundant power supplies are configured.

The possible values follow:

- **N/A**—Not applicable.
- **Balanced Mode**—Delivers power equally across all installed power supplies.
- **High Efficiency Mode (Auto)**—Delivers full power to one of the power supplies, and places the other power supplies on standby at a lower power-usage level. A semirandom distribution is achieved because the **Auto** option chooses between the odd or even power supply based on the server serial number.
- **High Efficiency Mode (Even Supply Standby)**—Delivers full power to the odd-numbered power supplies, and places the even-numbered power supplies on standby at a lower power-usage level.
- **High Efficiency Mode (Odd Supply Standby)**—Delivers full power to the even-numbered power supplies, and places the odd-numbered power supplies on standby at a lower power-usage level.
- **Not Supported**—The installed power supplies do not support High Efficiency Mode.

More information

[Power monitoring](#)

[High Efficiency Mode](#)

Power Supplies list

Power Supplies										
Bay	Present	Status	PDS	Hotplug	Model	Spare	Serial Number	Capacity	Firmware	
1	✓ OK	✓ Good, In Use	No	No	N/A	N/A	N/A	N/A Watts	N/A	

Some power supplies do not provide information for all of the values in this list. If a power supply does not provide information for a value, **N/A** is displayed.

Bay

The power supply bay number.

Present

Indicates whether a power supply is installed. The possible values are **OK** and **Not Installed**.

Status

The power supply status. The displayed value includes a status icon (**OK**, **Degraded**, **Failed**, or **Other**), and text that provides more information. The possible values follow:

- **Unknown**
- **Good, In Use**
- **Good, Standby**
- **General Failure**
- **Over Voltage Failure**
- **Over Current Failure**
- **Over Temperature Failure**
- **Input Voltage Lost**
- **Fan Failure**
- **High Input A/C Warning**
- **Low Input A/C Warning**
- **High Output Warning**
- **Low Output Warning**
- **Inlet Temperature Warning**
- **Internal Temperature Warning**
- **High Vaux Warning**
- **Low Vaux Warning**
- **Mismatched Power Supplies**

PDS

Whether the installed power supply is enabled for Power Discovery Services.

Hotplug

Whether the power supply bay supports swapping the power supply when the server is powered on. If the value is **Yes**, and the power supplies are redundant, the power supply can be removed or replaced when the server is powered on.

Flex Slot Battery Backup Unit

The following information is displayed for supported servers with an installed Flex Slot Battery Backup Unit:

- **Charge**—The current battery charge (percent).
- **Days Active**—The number of calendar days that the battery has been installed in a powered server.
- **Battery Health**—The battery health status (0 to 100 percent).

Power capping and power metering are not supported on servers with an installed Flex Slot Battery Backup Unit.

For more information, see the Flex Slot Battery Backup Unit installation instructions.

Model

The power supply model number.

Spare

The spare power supply part number.

Serial Number

The power supply serial number.

Capacity

The power supply capacity (watts).

Firmware

The installed power supply firmware version.

HPE Power Discovery Services iPDU Summary

This section is displayed if the server power supplies are connected to an iPDU.

After iLO is reset, or when an iPDU is attached, it takes approximately 2 minutes for the iLO web interface to display iPDU summary data. This delay is due to the iPDU discovery process.

Bay

The power supply bay number.

Status

The overall communication-link status and rack input power redundancy, as determined by the iPDU. Possible values follow:

- **iPDU Redundant**—This **Good** status indicates that the server is connected to at least two different iPDUUs.
- **iPDU Not Redundant**—This **Caution** status indicates that the server is not connected to at least two different iPDUUs. This status is displayed when one of the following conditions occurs:
 - An iPDU link is not established for all power supplies.
 - Two or more power supplies are connected to the same iPDU.The iPDU MAC address and serial number are identical for power supplies whose input power comes from the same iPDU. If one power supply is waiting for a connection to be established, the iPDU is listed as **Not Redundant**.
- **Waiting for connection**—This **Informational** status indicates one or more of the following conditions:
 - The wrong power cord was used to connect the power supply to the iPDU.
 - The iPDU and the iLO processor are in the process of connecting. This process can take up to 2 minutes after the iLO processor or the iPDU is reset.
 - The iPDU module does not have a network (or IP) address.

Part Number

The iPDU part number.

Serial

The iPDU serial number.

MAC Address

The MAC address of the iPDU network port. This value helps you to identify each connected iPDU because each iPDU has a unique MAC address.

iPDU Link

The iPDU HTTP address (if available). To open the Intelligent Modular PDU web interface, click the link in this column.

More information

[Power monitoring](#)

Power Readings

Present Power Reading—The most recent power reading from the server.

Although this value is typically equal to the sum of all active power supply outputs, there might be some small variance as a result of reading the individual power supplies. This value is a guideline value and is not as accurate as the values presented on the **Power Management** pages. For more information, see [“Viewing server power usage” \(page 249\)](#).

Power Microcontroller

Firmware Version—The firmware version of the power microcontroller.

The server must be powered on for the iLO firmware to determine the power microcontroller firmware version.

Smart Storage Battery details

The following details are displayed on servers that support the Smart Storage Battery.

- **Index**—The battery index number.
- **Present**—Whether a battery is installed. The possible values are **OK** and **Not Installed**.
- **Status**—The battery status. The possible values are **OK**, **Degraded**, **Failed**, or **Other**.
- **Model**—The battery model number.
- **Spare**—The part number of the spare battery.
- **Serial**—The battery serial number.
- **Capacity**—The battery capacity.
- **Firmware**—The installed battery firmware version.

Power monitoring

iLO monitors the power supplies in the server to ensure the longest available uptime of the server and operating system. Brownouts and other electrical conditions might affect power supplies, or AC cords might be unplugged accidentally. These conditions result in a loss of redundancy if redundant power supplies are configured, or result in a loss of operation if redundant power supplies are not used. If a power supply hardware failure is detected or the AC power cord is disconnected, events are recorded in the IML and LED indicators are used.

The iLO processor is an essential component of the Power Discovery Services infrastructure. The iLO processor communicates with the Intelligent Power Distribution Unit attached to each Platinum Plus power supply to determine rack and data center power redundancy. When the iLO processor is part of the Power Discovery Services infrastructure, it intelligently reports external server input power redundancy status and individual (internal) power supply status.

For more information, see the following website: <http://www.hpe.com/info/rackandpower>.

High Efficiency Mode

High Efficiency Mode improves the power efficiency of the server by placing the secondary power supplies in standby mode. When the secondary power supplies are in standby mode, primary power provides all DC power to the system. The power supplies are more efficient (more DC output watts for each watt of AC input) at higher output levels, and the overall power efficiency improves.

High Efficiency Mode does not affect power redundancy. If the primary power supplies fail, the secondary power supplies immediately begin supplying DC power to the system, preventing any downtime. You can configure redundant power supply modes only through the system RBSU or the UEFI System Utilities. You cannot modify these settings through the iLO firmware.

If High Efficiency Mode is configured to use an unsupported mode, you might experience decreased power supply efficiency.

For more information, see the system RBSU user guide or the UEFI System Utilities user guide.

Viewing processor information

Navigate to the **Information**→**System Information** page, and then click the **Processors** tab.

The **Processor Information** page displays the available processor slots, the type of processor installed in each slot, and a summary of the processor subsystem.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Processor details

Processor 1	
Processor Name	Intel(R) Core(TM) i3-3220T CPU @ 2.80GHz
Processor Status	OK
Processor Speed	2800 MHz
Execution Technology	2/2 cores, 4 threads
Memory Technology	64-bit Capable
Internal L1 cache	64 KB
Internal L2 cache	512 KB
Internal L3 cache	3072 KB

The following information is displayed for each processor:

- **Processor Name**—The name of the processor.
- **Processor Status**—The health status of the processor.
- **Processor Speed**—The speed of the processor.
- **Execution Technology**—Information about the processor cores and threads.
- **Memory Technology**—The processor memory capabilities.
- **Internal L1 cache**—The L1 cache size.
- **Internal L2 cache**—The L2 cache size.
- **Internal L3 cache**—The L3 cache size.

Viewing memory information

1. Navigate to the **Information**→**System Information** page, and then click the **Memory** tab.
2. Optional: By default, empty memory sockets are hidden in the **Memory Details** table. To view the empty memory sockets, click **show empty sockets**. When empty memory sockets are displayed, click **hide empty sockets** to hide them.

The **Memory Information** page displays a summary of the system memory. When server power is off, AMP data is unavailable, and only memory modules present at POST are displayed.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

Advanced Memory Protection details

Advanced Memory Protection (AMP)	
AMP Status	Supported AMP Modes
AMP Mode Status	Advanced ECC
Advanced ECC	
Configured AMP Mode	
Advanced ECC	

AMP Mode Status

The status of the AMP subsystem.

- **Other/Unknown**—The system does not support AMP, or the management software cannot determine the status.
- **Not Protected**—The system supports AMP, but the feature is disabled.
- **Protected**—The system supports AMP. The feature is enabled but not engaged.
- **Degraded**—The system was protected, but AMP is engaged. Therefore, AMP is no longer available.
- **DIMM ECC** (Error Correcting Code)—The system is protected by DIMM ECC only.
- **Mirroring**—The system is protected by AMP in the mirrored mode. No DIMM faults have been detected.
- **Degraded Mirroring**—The system is protected by AMP in the mirrored mode. One or more DIMM faults have been detected.
- **On-line Spare**—The system is protected by AMP in the hot spare mode. No DIMM faults have been detected.
- **Degraded On-line Spare**—The system is protected by AMP in the hot spare mode. One or more DIMM faults have been detected.
- **RAID-XOR**—The system is protected by AMP in the XOR memory mode. No DIMM faults have been detected.
- **Degraded RAID-XOR**—The system is protected by AMP in the XOR memory mode. One or more DIMM faults have been detected.
- **Advanced ECC**—The system is protected by AMP in the Advanced ECC mode.
- **Degraded Advanced ECC**—The system is protected by AMP in the Advanced ECC mode. One or more DIMM faults have been detected.
- **LockStep**—The system is protected by AMP in the LockStep mode.
- **Degraded LockStep**—The system is protected by AMP in the LockStep mode. One or more DIMM faults have been detected.

Configured AMP Mode

The active AMP mode. The following modes are supported:

- **None/Unknown**—The management software cannot determine the AMP fault tolerance, or the system is not configured for AMP.
- **On-line Spare**—A single spare bank of memory is set aside at boot time. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
- **Mirroring**—The system is configured for mirrored memory protection. All memory banks are duplicated in mirrored memory, as opposed to only one for online spare memory. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
- **RAID-XOR**—The system is configured for AMP with the XOR engine.
- **Advanced ECC**—The system is configured for AMP with the Advanced ECC engine.
- **LockStep**—The system is configured for AMP with the LockStep engine.
- **Online Spare (Rank Sparing)**—The system is configured for Online Spare Rank AMP.
- **Online Spare (Channel Sparing)**—The system is configured for Online Spare Channel AMP.

- **Intersocket Mirroring**—The system is configured for mirrored intersocket AMP between the memory of two processors or boards.
- **Intrasocket Mirroring**—The system is configured for mirrored intrasocket AMP between the memory of a single processor or board.

Supported AMP Modes

The following modes are supported:

- **RAID-XOR**—The system can be configured for AMP using the XOR engine.
- **Dual Board Mirroring**—The system can be configured for mirrored advanced memory protection in a dual memory board configuration. The mirrored memory can be swapped with memory on the same memory board or with memory on the second memory board.
- **Single Board Mirroring**—The system can be configured for mirrored advanced memory protection in a single memory board.
- **Advanced ECC**—The system can be configured for Advanced ECC.
- **Mirroring**—The system can be configured for mirrored AMP.
- **On-line Spare**—The system can be configured for online spare AMP.
- **LockStep**—The system can be configured for LockStep AMP.
- **Online Spare (Rank Sparing)**—The system can be configured for Online Spare Rank AMP.
- **Online Spare (Channel Sparing)**—The system can be configured for Online Spare Channel AMP.
- **Intersocket Mirroring**—The system can be configured for mirrored intersocket AMP between the memory of two processors or boards.
- **Intrasocket Mirroring**—The system can be configured for mirrored intrasocket AMP between the memory of a single processor or board.
- **None**—The system cannot be configured for AMP.

Memory Summary

Memory Summary				
Location	Number of Sockets	Total Memory	Operating Frequency	Operating Voltage
Processor 1	2	4 GB	1333 MHz	1.5 V

The **Memory Summary** section shows a summary of the memory that was installed and operational at POST.

Location

The slot or processor on which the memory board, cartridge, or riser is installed. Possible values follow:

- **System Board**—There is no separate memory board slot. All DIMMs are installed on the motherboard.
- **Board <Number>**—There is a memory board slot available. All DIMMs are installed on the memory board.
- **Processor <Number>**—The processor on which the memory DIMMs are installed.
- **Riser <Number>**—The riser on which the memory DIMMs are installed.

Number of Sockets

The number of present memory module sockets.

Total Memory

The capacity of the memory, including memory recognized by the operating system and memory used for spare, mirrored, or XOR configurations.

Operating Frequency

The frequency at which the memory operates.

Operating Voltage

The voltage at which the memory operates.

Memory Details

Memory Details (show empty sockets)										
Memory Location	Socket	Status	HPE Memory	Part Number	Type	Size	Maximum Frequency	Minimum Voltage	Ranks	Technology
Processor 1	1	Good, In Use	No	N/A	DIMM DDR3	2048 MB	1333 MHz	1.5 V	1	UDIMM
Processor 1	2	Good, In Use	No	N/A	DIMM DDR3	2048 MB	1333 MHz	1.5 V	1	UDIMM

The **Memory Details** section shows the memory modules on the host that were installed and operational at POST. Unpopulated module positions are also listed. Various resilient memory configurations can change the actual memory inventory from what was sampled at POST. In systems that have a high number of memory modules, all module positions might not be listed.

Memory Location

The slot or processor on which the memory module is installed.

Socket

The memory module socket number.

Status

The memory module status and whether the module is in use.

HPE Memory

Indicates whether the memory module is HPE SmartMemory or HPE Standard Memory.

If no memory module is installed, the value **N/A** is displayed. If the value **No** is displayed, the listed module is not an HPE Memory module. Third-party memory modules will function, but they do not have a warranty, and they might not perform as well as an HPE Memory module.

For more information, see <http://www.hpe.com/info/memory>.

Part Number

The memory module part number.

This value is displayed only for HPE Memory modules.

Type

The type of memory installed. Possible values follow:

- **Other**—Memory type cannot be determined.
- **Board**—Memory module is permanently mounted (not modular) on a system board or memory expansion board.

- **CPQ single width module**
- **CPQ double width module**
- **SIMM**
- **PCMCIA**
- **Compaq-specific**
- **DIMM**
- **Small outline DIMM**
- **RIMM**
- **SRIMM**
- **FB-DIMM**
- **DIMM DDR**
- **DIMM DDR2**
- **DIMM DDR3**
- **DIMM DDR4** (supported servers only)
- **FB-DIMM DDR2**
- **FB-DIMM DDR3**
- **N/A**—Memory module is not present.

Size

The size of the memory module, in MB.

Maximum Frequency

The maximum frequency at which the memory module can operate.

Minimum Voltage

The minimum voltage at which the memory module can operate.

Ranks

The number of ranks in the memory module.

Technology

The memory module technology. Possible values follow:

- **Unknown**—Memory technology cannot be determined.
- **N/A**—Memory module is not present.
- **Fast Page**
- **EDO**
- **Burst EDO**
- **Synchronous**
- **RDRAM**
- **RDIMM**
- **UDIMM**

- **LRDIMM**
- **NVDIMM**
- **R-NVDIMM**

Viewing network information

1. Navigate to the **Information**→**System Information** page, and then click the **Network** tab.
2. Optional: To expand or collapse the information on this page, click **Expand All** or **Collapse All**, respectively.

If the server is powered off, the health status information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view a full set of data on this page, ensure that AMS is installed and running. The server IP address, add in network adapters, and the server NIC status are displayed only if AMS is installed and running on the server.

The information on this page is updated when you log in to iLO. To refresh the data, log out of iLO, and then log back in.

Physical Network Adapters

Physical Network Adapters

▼ Adapter 1 - iLO

Description	Shared Network Port
Location	Embedded
Status	OK

MAC Address	IPv4 Address	IPv6 Address	Port	Status
38:63:bb:2d:09:b8	Unknown	Unknown	dedicated	Disabled
38:63:bb:2d:09:b9	16.85.178.140	unknown	shared	OK

▼ Adapter 2 - HP Ethernet 1Gb 4-port 331i Adapter

Location	Embedded
Firmware	1.46.0
Status	OK

Network Ports

Port	MAC Address	IPv4 Address	IPv6 Address	Status	Team/Bridge
1	38:63:bb:33:93:88	16.110.181.208	fe80::4dd0:7a95:7bba:a685%12	OK	N/A
2	38:63:bb:33:93:89	N/A	N/A	Unknown	N/A
3	38:63:bb:33:93:8a	16.85.179.62	fd0e:2d:ba9:221a:98e:8940:e44d:a0e	OK	NIC TEAM 1
4	38:63:bb:33:93:8b	16.85.179.62	fd0e:2d:ba9:221a:98e:8940:e44d:a0e	OK	NIC TEAM 1

► Adapter 3 - HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter

► Adapter 4 - HPE Ethernet 25Gb 2-port 640SFP28 Adapter

Integrated and add-in NICs and Fibre Channel adapters

This section displays the following information about the integrated and add-in NICs and Fibre Channel adapters in the server:

- **Adapter number**—The adapter number, for example, **Adapter 1** or **Adapter 2**.
- **Device Type**—The device type is one of the following:
 - **iLO**—This device type is assigned to the iLO Dedicated Network Port or Shared Network Port.
 - **<NIC type>**—This device type indicates NIC or LAN adapter components embedded in the server or added after manufacturing. Because system NICs are directly available

to the server host operating system, the iLO firmware cannot obtain current IP addresses (or other configuration settings) for these devices.

- **Description**—A description of the physical network adapter, for example, Dedicated Network Port or Shared Network Port. This value is displayed for iLO adapters only.
- **Location**—The location of the adapter on the system board.
- **Firmware**—The version of the installed adapter firmware, if applicable. This value is displayed for system NICs (embedded and stand-up) only.
- **Status**—The NIC status.
 - On Windows servers:
 - If the NIC has never been plugged in to a network, iLO displays the status **Unknown**.
 - If the NIC has been plugged in to a network, and is now unplugged, iLO displays the status **Link Down**.
 - On Linux servers:
 - If NetworkManager is used to manage the NIC, the default status is **Up** and the link status is displayed in iLO.
 - If Linux legacy utilities are used to manage the NIC, iLO displays the link status only if the NIC is configured by an administrator. If the NIC is not configured, iLO displays the status **Unknown**.
 - On VMware servers:
 - If iLO cannot communicate with the NIC port, it displays the status **Unknown**.
 - If the NIC driver reports the status `link_down`, iLO displays the status **Down**.
 - If the NIC driver reports the status `link_up`, iLO displays the status **Up**.
- **Port**—The configured network port. This value is displayed for system NICs (embedded and stand-up) only.
- **MAC Address**—The port MAC address.
- **IPv4 Address**—For iLO adapters, the iLO IPv4 address. For system NICs (embedded and stand-up), the server IP address (if available).
- **IPv6 Address**—For iLO adapters, the iLO IPv6 address. For system NICs (embedded and stand-up), the server IP address (if available).
- **Status**—The port status.
- **Team/Bridge**—If a port is configured for NIC teaming, the name of the configured link between the physical ports that form a logical network adapter. This value is displayed for system NICs (embedded and stand-up) only.

Fibre Channel host bus adapters or converged network adapters

The following information is displayed for Fibre Channel host bus adapters or converged network adapters:

- **Physical Port**—The physical network port number.
- **WWNN**—The port world wide node name.
- **WWPN**—The world wide port name.
- **Status**—The port status.

Boot progress and boot targets

The following information about the boot progress and boot targets is displayed when DCI connectivity is available:

- **Port**—The configured virtual port number.
- **Boot Progress**—The current boot status.
- **Boot Targets**
 - **WWPN**—The world wide port name.
 - **LUN ID**—The logical unit number ID.

Logical Network Adapters

The screenshot shows a list of logical network adapters. Adapter 1 - NIC TEAM 1 is expanded, displaying its MAC Address (38:63:bb:33:93:8a), IP Address (16.85.179.62), and Status (OK). Below this is a table showing the members of the team:

Members	MAC Address	Status
1	38:63:bb:33:93:8b	OK
2	38:63:bb:33:93:8a	OK

Adapter 2 - NIC TEAM 2 - 10G is collapsed, indicated by a right-pointing arrow.

This section displays the following information about network adapters that use NIC teaming to combine two or more ports into a single logical network connection:

- **Adapter name**—The name of the configured link between the physical ports that form the logical network adapter.
- **MAC Address**—The logical network adapter MAC address.
- **IP Address**—The logical network adapter IP address.
- **Status**—The logical network adapter status.

The following information is displayed for the ports that form each logical network adapter:

- **Members**—A sequential number assigned to each port that forms the logical network adapter.
- **MAC Address**—The MAC address of the physical adapter port.
- **Status**—The status of the physical adapter port.

Viewing the device inventory

Navigate to the **Information**→**System Information** page, and then click the **Device Inventory** tab.

The **Device Inventory** page displays information about devices installed on the system board. Some examples of the devices listed on this page include installed adapters, PCI devices, SATA controllers, and Smart Storage batteries.

If the server is powered off, the health status information on this page is current as of the last power on. Health information is updated only when the server is powered on and POST is complete.

The following information is displayed only if AMS is installed and running on the server: Firmware version and status of add-in network adapters, network-attached storage details, and Smart Storage Battery status.

If the iLO firmware cannot retrieve the network adapter product name or part number directly from the device, it attempts to collect that information from AMS.

Device Inventory details

Device Inventory							
This table displays the server primary device information such as embedded storage and network controllers. For embedded and third party devices, not all the fields (such as Product Part Number or Serial Number) may be populated. The embedded devices are part of the system board Field Replaceable Unit (FRU).							
Location	Product Name	Product Part Number	Assembly Number	Serial Number	Product Version	Firmware Version	Status
Embedded	HP Ethernet 1Gb 2-port 332i Adapter	615732-B21	N/A	N/A	N/A	1.30.0	ⓘ Unknown
Embedded	Standard IDE Controller	N/A	N/A	N/A	N/A		ⓘ OK
PCI-E Slot 1	Empty	N/A	N/A	N/A	N/A		ⓘ Not installed

- **Location**—The device install location.
- **Product Name**—The device product name.
- **Product Part Number**—The device part number.

This column displays the value **Various** when the actual part number of the listed device depends on internally installed graphics devices that differ by server model.

- **Assembly Number**—The device part number (Hewlett Packard Enterprise devices) or the EEPROM Board Info data (third-party devices).
- **Serial Number**—The device serial number.
- **Product Version**—The device product version.
- **Firmware Version**—The installed device firmware version.
- **Status**—The device status.

Device status values

The **Device Inventory** page uses the following status values:

- ⓘ **OK**—The device is working correctly.
- ⓘ **Other**—The device status could not be determined.
- ⓘ **No Supporting CPU**—The CPU that supports the device slot is not installed.
- ⚠ **Not Installed**—A device is not installed.
- ⚠ **Link Down**—The network link is down.
- ⚠ **Failed**—One or more components of the device are nonoperational.
- ⚠ **Degraded**—The device is operating at a reduced capacity.
- ⓘ **Unknown**—The iLO firmware has not received data about the device status.

Viewing PCI slot details

1. Navigate to the **Information**→**System Information** page, and then click the **Device Inventory** tab.

2. Move the cursor over the **Location** column for a listed PCI slot.

PCI-E Slot 1		
Type:	PCI Express Gen 2 x16	
Bus Width:	16x	
Length:	Long Length	
Characteristics 1: Provides 3.3 volts		
Bus	Device	Function
0x7	0x0	0x0

PCI slot tool tip details

- **Type**—The PCI slot type.
- **Bus Width**—The PCI slot bus width.
- **Length**—The PCI slot length.
- **Characteristics 1**—Information about the PCI slot, for example, voltage and other support information.
- **Characteristics 2**—Information about the PCI slot, for example, voltage and other support information.

Viewing storage information

1. Navigate to the **Information**→**System Information** page, and then click the **Storage** tab.
2. Optional: To expand or collapse the data, click **Expand All** or **Collapse All**, respectively.
3. Smart Array controllers only: For the controller you want to view, select one of the following options:
 - **Logical View**—View configured logical drives and associated physical drives. This view does not show physical drives that are not configured as part of an array, or spare drives.
 - **Physical View**—View physical drives. This view does not show logical drives.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view a full set of data on this page, ensure that AMS is installed and running. SAS/SATA controller information is displayed only if AMS is installed and running on the server.

The information displayed on this page depends on your storage configuration. Some storage configurations will not display information for every category.

Fibre Channel adapters are not listed on this page. To view information about Fibre Channel adapters, see the **Information**→**System Information**→**Network** page.

Supported storage components

The **Storage Information** page displays information about the following storage components:

- Smart Array controllers, drive enclosures, the attached logical drives, and the physical drives that constitute the logical drives.
- Hewlett Packard Enterprise and third-party storage controllers that manage direct-attached storage, and the attached physical drives.

iLO 4 2.10 and later supports the following products:

- HPE ML/DL Server M.2 SSD Enablement Kit
- HPE 12G SAS Expander
- HPE Dual 8GB MicroSD EM USB Kit

iLO 4 2.30 and later supports the following product:

- NVMe drives

Smart Array controllers are listed first on the page, followed by other Hewlett Packard Enterprise and third-party storage controllers.

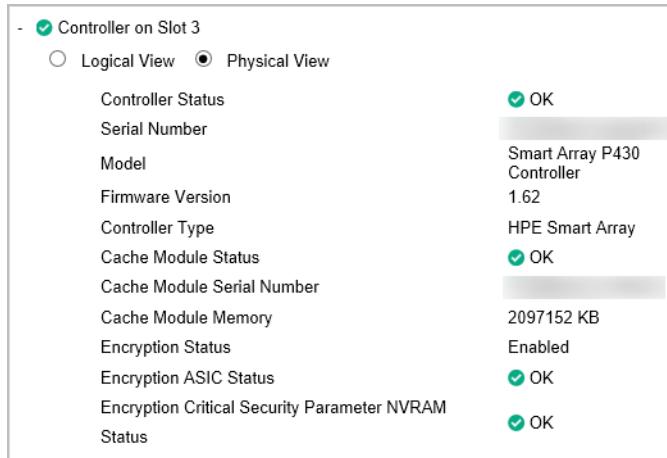
Smart Array details

iLO displays information about the following:

- [Controllers](#)
- [Drive enclosures](#)
- [Logical drives](#)
- [Physical drives](#)

iLO can monitor 71 physical drives on a controller, 256 physical drives total, and 256 logical drives total.

Controllers



The screenshot shows the 'Physical View' of a Smart Array controller on Slot 3. The controller is an HPE Smart Array P430. The status is 'OK'. The table lists the following information:

Setting	Status
Controller Status	OK
Serial Number	
Model	Smart Array P430 Controller
Firmware Version	1.62
Controller Type	HPE Smart Array
Cache Module Status	OK
Cache Module Serial Number	
Cache Module Memory	2097152 KB
Encryption Status	Enabled
Encryption ASIC Status	OK
Encryption Critical Security Parameter NVRAM Status	OK

This section provides the following details for each Smart Array controller.

- Controller location—Slot number or system board
- Top-level controller status—The top-level controller status (displayed on the left of the controller location) is a combination of the controller hardware status and the status of cache modules, enclosures, and physical, logical, and spare drives associated with the controller. If the controller hardware status is **OK**, and any associated hardware has a failure, the

top-level controller status changes to **Major Warning** or **Degraded**, depending on the failure type. If the controller hardware has a **Failed** status, the top-level controller status is **Failed**.

- **Controller Status**—Controller hardware status (**OK** or **Failed**)
- **Serial Number**
- **Model**
- **Firmware Version**
- **Controller Type**
- **Cache Module Status**
- **Cache Module Serial Number**
- **Cache Module Memory**
- **Encryption Status**—Indicates whether encryption is enabled in the controller.
The following values are possible:
 - **Enabled**
 - **Not Enabled**
 - **Enabled—Local Mode**—This value is displayed when you do not use a remote key management server.
- **Encryption ASIC Status**—Indicates whether the ASIC encryption self tests for the controller passed or failed. A failed status indicates that the controller is not encrypted.
- **Encryption Critical Security Parameter NVRAM Status**—Indicates whether the controller successfully detected the critical security parameter NVRAM. A failed status means that the controller is not encrypted.

The encryption settings for a Smart Array controller can be configured by using the Smart Storage Administrator software.

Drive Enclosures

- <input checked="" type="checkbox"/> Drive Enclosure Port 1I Box 1
Status <input checked="" type="checkbox"/> OK
Drive Bays 4

This section provides the following information about the drive enclosures attached to a Smart Array controller.

- Enclosure port and box numbers
- **Status**
- **Drive Bays**—The number of drive bays
- **Serial Number**
- **Model**
- **Firmware Version**

Some enclosures do not have all of the listed properties, and some storage configurations do not have drive enclosures.

Logical Drives

-	 Logical Drive 01
Status	 OK
Capacity	136 GiB
Fault Tolerance	RAID 5
Logical Drive Type	Data LUN
Encryption Status	Encrypted

When the **Logical View** option is selected, the following information is listed for the logical drives attached to a Smart Array controller.

- Logical drive number
- **Status**
- **Capacity**
- **Fault Tolerance**
- **Logical Drive Type**
- **Encryption Status**

Logical drives must be configured through the Smart Storage Administrator software before they can be displayed on this page.

Physical Drives

-	 Physical Drive in Port 1I Box 1 Bay 2
Status	 OK
Serial Number	
Model	DH072BB978
Media Type	HDD
Capacity	72 GB
Location	Port 1I Box 1 Bay 2
Firmware Version	HPDC
Drive Configuration	Configured
Encryption Status	Encrypted

The information listed in this section depends on whether the **Logical View** or **Physical View** option is selected. In the **Logical View**, physical drives that are configured as part of an array are listed. In the **Physical View**, all physical drives are listed.

When a physical drive has a **Failed** status, this status does not affect the overall storage health status. Only logical drives affect the storage health status.

The following information is listed for the physical drives attached to a Smart Array controller:

- Physical drive port, box, and bay numbers
- **Status**
- **Serial Number**
- **Model**
- **Media Type**
- **Capacity**
- **Location**
- **Firmware Version**

- **Drive Configuration**
- **Encryption Status**

Direct-attached storage details

iLO displays information about the following:

- **Controllers**
- **Physical drives**

Controllers

- <input checked="" type="checkbox"/> Controller on System Board
Controller Status <input checked="" type="checkbox"/> OK
Serial Number N/A
Model Standard IDE Controller
Firmware Version N/A
Controller Type SAS/SATA

This section provides the following information about the Hewlett Packard Enterprise and third-party storage controllers that manage direct-attached storage.

- **Controller location**
- **Top-level controller status**—The top-level controller status (displayed on the left of the controller location) is a combination of the controller hardware status and the status of the enclosures, physical drives, and spare drives associated with the controller. If the controller hardware status is **OK**, and any associated hardware has a failure, the top-level controller status changes to **Major Warning** or **Degraded**, depending on the failure type. If the controller hardware has a **Failed** status, the top-level controller status is **Failed**.
- **Controller Status**—Controller hardware status (**OK** or **Failed**)
- **Serial Number**
- **Model**
- **Firmware Version**
- **Controller Type**

Physical Drives

- <input checked="" type="checkbox"/> Physical Drive in SATA Device 0
Status <input checked="" type="checkbox"/> OK
Serial Number L50QQ1FH
Model Maxtor 6L250S0
Media Type Not available
Capacity 232 GiB
Location SATA Device 0
Firmware Version BACE1G10
Drive Configuration Not available
Encryption Status Not Encrypted

This section provides information about physical drives attached to Hewlett Packard Enterprise and third-party storage controllers.

When a physical drive has a **Failed** status, this status does not affect the overall storage health status. Only logical drives affect the storage health status.

- Physical drive location
- **Status**
- **Serial Number**
- **Model**
- **Media Type**
- **Capacity**
- **Location**
- **Firmware Version**
- **Drive Configuration**
- **Encryption Status**

Viewing firmware information

Navigate to the **Information**→**System Information** page, and then click the **Firmware** tab.

The **Firmware Information** page displays firmware information for various server components.

If the server is powered off, the information on this page is current as of the last power off.

Firmware information is updated only when the server is powered on and POST is complete.

Firmware types

The firmware types listed on the **Firmware Information** page vary based on the server model and configuration.

For most servers, the system ROM and iLO firmware are listed. Other possible firmware options include the following:

- Power Management Controller
- Server Platform Services Firmware
- Smart Array
- Intelligent Platform Abstraction Data (supported servers only)
- Smart Storage Battery (supported servers only)
- TPM or TM firmware
- SAS Programmable Logic Device
- System Programmable Logic Device
- Intelligent Provisioning
- Networking adapters
- NVMe Backplane Firmware

Firmware information for hard drives is not listed on this page. To view hard drive firmware details, navigate to the **Information**→**System Information** page, and then click the **Storage** tab.

Firmware details

Firmware Version Info		
Firmware Name	Firmware Version	Location
HP Ethernet 1Gb 2-port 332i Adapter	1.30.0	Embedded
iLO	2.50 Sep 15 2016	System Board
Intelligent Platform Abstraction Data	0.00	System Board
Intelligent Provisioning	1.61.10	System Board
Redundant System ROM	J06 06/06/2014	System Board
Server Platform Services (SPS) Firmware	2.2.0.31.2	System Board
System Programmable Logic Device	Version 0x06	System Board
System ROM	J06 06/06/2014	System Board
System ROM Bootblock	02/04/2012	System Board

The **Firmware Information** page displays the following information for each listed firmware type:

- **Firmware Name**—The name of the firmware.
- **Firmware Version**—The version of the firmware.
- **Location**—The location of the component that uses the listed firmware.

Viewing software information

1. Navigate to the **Information**→**System Information** page, and then click the **Software** tab.
2. Select one of the following:
 - **HPE Software**—Lists all of the Hewlett Packard Enterprise software on the managed server. This page displays Hewlett Packard Enterprise and Hewlett Packard Enterprise-recommended third-party software that was added manually or by using the SPP.
 - **Running Software**—Lists all of the software that is running or available to run on the managed server.
 - **Installed Software**—Lists all of the software installed on the managed server.
3. Optional: To update the software information data, click **Refresh**.

The information on this page is cached in the browser, and iLO displays the date and time of the last update. If 5 minutes or more have passed since the page was updated, click **Refresh** to update the page with the latest information.

To display a complete set of data on this page, AMS must be installed.

More information

[iLO SNMP management](#)

HPE Software List details

<input checked="" type="radio"/> HPE Software	<input type="radio"/> Running Software	<input type="radio"/> Installed Software	Refresh
Last updated: Tue Sep 27 13:15:07 2016			
Name	Description	Version	
b57nd60a.sys	broadcom netxtreme gigabit ethernet ndis6.x unified driver.	16.6.0.4	
BXVBDA.SYS	broadcom netxtreme ii gige vbd	7.4.14.0	
evbda.sys	broadcom netxtreme ii 10 gige vbd	7.4.33.1	
hpqams.exe	hpe proliant agentless management service	10.40.0.0	
hpqilo3chif.sys	hp proliant ilo 3/4 channel interface driver	3.10.0.0	
hpqilo3core.sys	hp proliant ilo 3/4 management controller core driver	3.9.0.0	
lsi_sas2.sys	lsi sas gen2 driver (storport)	2.0.60.82	
mlx4_bus.sys	mlx4 bus driver	4.4.13905.0	
ProLiantMonitor.exe	hp proliant monitor service	3.15.1.0	

- **Name**—The name of the software.
- **Description**—A description of the software.
- **Version**—The software version.

The versions of the firmware components displayed on this page indicate the firmware versions available in the firmware flash components that are saved on the local operating system (for example, the `hp-firmware-ilo4` RPM on Linux systems). The displayed version might not match the firmware running on the server.

Running Software details

<input type="radio"/> HPE Software	<input checked="" type="radio"/> Running Software	<input type="radio"/> Installed Software	Refresh
Last updated: Tue Sep 27 13:15:07 2016			
Name	Type	File Path	
csrss.exe	OS Software	N/A	
csrss.exe	OS Software	N/A	
dwm.exe	Application	C:\Windows\System32	
HpAmsStor.exe	Application	C:\Program Files\Hewlett-Packard\AMS\service	
hpqams.exe	Application	C:\Program Files\Hewlett-Packard\AMS\service	
LogonUI.exe	Application	C:\Windows\System32	
lsass.exe	Application	C:\Windows\System32	
ProLiantMonitor.exe	Application	C:\Program Files\Hewlett-Packard\iLO 3\service	
services.exe	OS Software	N/A	
smss.exe	OS Software	N/A	
spoolsv.exe	Application	C:\Windows\System32	
svchost.exe	Application	C:\Windows\System32	

- **Name**—The name of the software.
- **Type**—The software type. The following values are valid: **Application** and **OS Software**.
- **File path**—The file path of the software.

Installed Software details

<input type="radio"/> HPE Software	<input type="radio"/> Running Software	<input checked="" type="radio"/> Installed Software	Refresh															
Last updated: Tue Sep 27 13:15:07 2016																		
<table><thead><tr><th>Name</th></tr></thead><tbody><tr><td>3ware</td></tr><tr><td>1394 OHCI Compliant Host Controller</td></tr><tr><td>ACPI Power Meter Driver</td></tr><tr><td>ACPI Processor Aggregator Driver</td></tr><tr><td>ACPI Wake Alarm Driver</td></tr><tr><td>Adaptec SAS/SATA-II RAID Storport's Miniport Driver</td></tr><tr><td>ADP80XX</td></tr><tr><td>AMD K8 Processor Driver</td></tr><tr><td>AMD Processor Driver</td></tr><tr><td>amdsata</td></tr><tr><td>amdsbs</td></tr><tr><td>amdxata</td></tr><tr><td>Ancillary Function Driver for Winsock</td></tr><tr><td>ARM ID Driver</td></tr></tbody></table>				Name	3ware	1394 OHCI Compliant Host Controller	ACPI Power Meter Driver	ACPI Processor Aggregator Driver	ACPI Wake Alarm Driver	Adaptec SAS/SATA-II RAID Storport's Miniport Driver	ADP80XX	AMD K8 Processor Driver	AMD Processor Driver	amdsata	amdsbs	amdxata	Ancillary Function Driver for Winsock	ARM ID Driver
Name																		
3ware																		
1394 OHCI Compliant Host Controller																		
ACPI Power Meter Driver																		
ACPI Processor Aggregator Driver																		
ACPI Wake Alarm Driver																		
Adaptec SAS/SATA-II RAID Storport's Miniport Driver																		
ADP80XX																		
AMD K8 Processor Driver																		
AMD Processor Driver																		
amdsata																		
amdsbs																		
amdxata																		
Ancillary Function Driver for Winsock																		
ARM ID Driver																		

The **Installed Software** list displays the name of each installed software program.

14 Using the iLO logs

iLO Event Log

The event log provides a record of significant events recorded by iLO.

Logged events include major server events such as a server power outage or a server reset, and iLO events such as unauthorized login attempts. Other logged events include successful or unsuccessful browser and Remote Console logins, virtual power and power-cycle events, clearing the log, and some configuration changes, such as creating or deleting a user and registering for remote support.

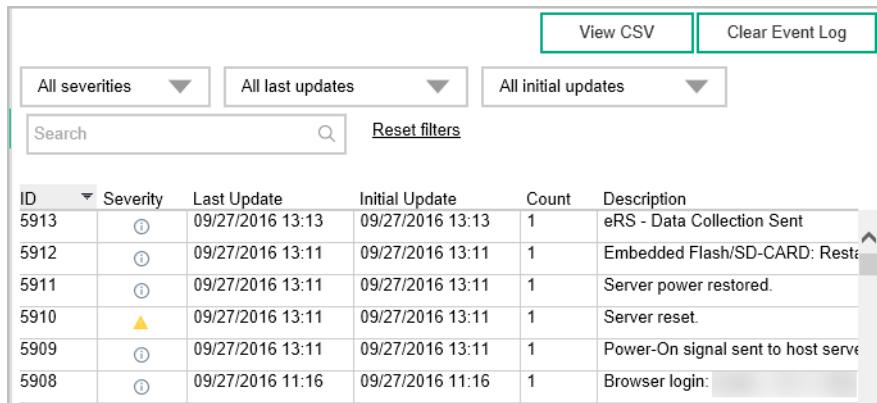
iLO provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. The **Authentication Failure Logging** setting allows you to configure logging criteria for failed authentications. The event log captures the client name for each logged entry to improve auditing capabilities in DHCP environments, and records the account name, computer name, and IP address. For information about configuring Authentication Failure Logging, see [“iLO access settings” \(page 61\)](#).

For a list of the errors that might appear in the event log, see the error messages guide for your server.

Viewing the event log

1. Navigate to the **Information**→**iLO Event Log** page.
2. Optional: Use the event log filters to customize the log view.

Event log details



ID	Severity	Last Update	Initial Update	Count	Description
5913	ⓘ	09/27/2016 13:13	09/27/2016 13:13	1	eRS - Data Collection Sent
5912	ⓘ	09/27/2016 13:11	09/27/2016 13:11	1	Embedded Flash/SD-CARD: Restored
5911	ⓘ	09/27/2016 13:11	09/27/2016 13:11	1	Server power restored.
5910	⚠	09/27/2016 13:11	09/27/2016 13:11	1	Server reset.
5909	ⓘ	09/27/2016 13:11	09/27/2016 13:11	1	Power-On signal sent to host server
5908	ⓘ	09/27/2016 11:16	09/27/2016 11:16	1	Browser login:

- **ID**—The event ID number. Events are numbered in the order in which they are generated. By default, the event log is sorted by the ID, with the most recent event at the top.
- **Severity**—The importance of the detected event.
- **Last Update**—The date and time when the latest event of this type occurred. This value is based on the date and time stored by the iLO firmware.
If the iLO firmware did not recognize the date and time when an event was updated, [NOT SET] is displayed.
- **Initial Update**—The date and time when the first event of this type occurred. This value is based on the date and time stored by the iLO firmware.
If the iLO firmware did not recognize the date and time when the event was first created, [NOT SET] is displayed.

- **Count**—The number of times this event has occurred (if supported).
In general, important events generate an event log entry each time they occur. They are not consolidated into one event log entry.
When less important events are repeated, they are consolidated into one event log entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.
- **Description**—The description identifies the component and detailed characteristics of the recorded event.
If the iLO firmware is rolled back to an earlier version, the description UNKNOWN EVENT TYPE might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the event log.

More information

[Event log icons](#)

[Configuring iLO SNTP settings](#)

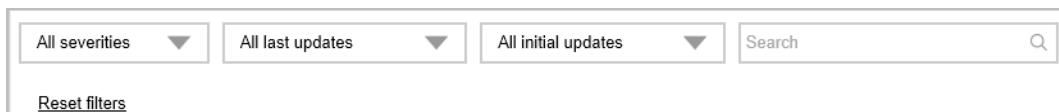
Event log icons

iLO uses the following icons to indicate event severity:

-  **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.
-  **Caution**—The event is significant but does not indicate performance degradation.
-  **Informational**—The event provides background information.
-  **Unknown**—The event severity could not be determined.

Customizing the event log view

You can customize the event log view by using the controls at the top of the page.



- To filter by severity, select a severity level from the **Severity** menu.
- To filter by the **Last Update** date, select a value in the **Last Update** menu.
If you select the **Specific date range** option, select a date range in the **Last Update Range** dialog box, and then click **Apply**.
- To filter by the **Initial Update** date, select a value in the **Initial Update** menu.
If you select the **Specific date range** option, select a date range in the **Initial Update Range** dialog box, and then click **Apply**.
- To search for events based on dates, event IDs, or description text, enter text in the **Search** box, and then press **Enter**.
- Click **Reset filters** to set the filters back to the default values.
- Click a column heading to sort the event log table by that column.
- When sorting the event log table by column, click the triangle next to the column heading to change the display to ascending or descending order.

Saving the event log to a CSV file

Use a supported browser to export the event log to a CSV file.

For Internet Explorer users only: This feature is supported with Internet Explorer 11 and later.

1. Navigate to the **Information**→**iLO Event Log** page.
2. Click **View CSV**.
3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.
4. Click **Close** to close the window.

Clearing the event log

Users with the Configure iLO Settings privilege can clear the event log of all previously logged information.

1. Navigate to the **Information**→**iLO Event Log** page.
2. Click **Clear Event Log**.
3. When prompted to confirm the request, click **OK**.

The following event is recorded:

Event log cleared by <user name>.

Integrated Management Log

The IML provides a record of historical events that have occurred on the server. Events are generated by the system ROM and by services such as the iLO health driver. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes.

Entries in the IML can help you diagnose issues or identify potential issues. Preventative action might help to avoid disruption of service.

iLO manages the IML, which you can access through a supported browser, even when the server is off. The ability to view the log when the server is off can be helpful when troubleshooting remote host server issues.

Examples of the types of information recorded in the IML follow:

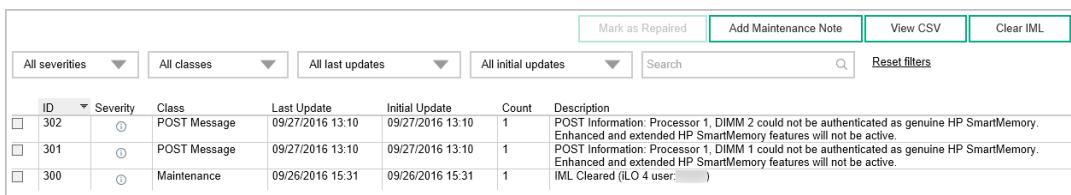
- Fan inserted
- Fan removed
- Fan failure
- Fan degraded
- Fan repaired
- Fan redundancy lost
- Fans redundant
- Power supply inserted
- Power supply removed
- Power supply failure
- Power supplies redundancy lost
- Power supplies redundant
- Temperature over threshold
- Temperature normal

- Automatic shutdown started
- Automatic shutdown canceled
- Drive failure

Viewing the IML

1. Navigate to the **Information→Integrated Management Log** page.
2. Optional: Use the IML filters to customize the log view.

IML details



							Mark as Repaired	Add Maintenance Note	View CSV	Clear IML
All severities		All classes		All last updates		All initial updates		<input type="text" value="Search"/> 	Reset filters	
ID	Severity	Class	Last Update	Initial Update	Count	Description				
302		POST Message	09/27/2016 13:10	09/27/2016 13:10	1	POST Information: Processor 1, DIMM 2 could not be authenticated as genuine HP SmartMemory. Enhanced and extended HP SmartMemory features will not be active.				
301		POST Message	09/27/2016 13:10	09/27/2016 13:10	1	POST Information: Processor 1, DIMM 1 could not be authenticated as genuine HP SmartMemory. Enhanced and extended HP SmartMemory features will not be active.				
300		Maintenance	09/26/2016 15:31	09/26/2016 15:31	1	IML Cleared (iLO 4 user.)				

- The first column on the left side of the web interface displays a check box next to each event with Critical or Caution status. Use this check box to select an event to mark as repaired. For information about marking events as repaired, see [“Marking an IML entry as repaired” \(page 186\)](#).
- **ID**—The event ID number. Events are numbered in the order in which they are generated. By default, the IML is sorted by the ID, with the most recent event at the top. A factory reset will reset the counter.
- **Severity**—The importance of the detected event.
- **Class**—Identifies the type of event that occurred, for example, network, maintenance, or system revision.
- **Last Update**—The date and time when the latest event of this type occurred. This value is based on the date and time stored by the iLO firmware.
If iLO did not recognize the date and time when an event was updated, [NOT SET] is displayed.
- **Initial Update**—The date and time when the first event of this type occurred. This value is based on the date and time stored by the iLO firmware.
If iLO did not recognize the date and time when the event was first created, [NOT SET] is displayed.
- **Count**—The number of times this event has occurred (if supported).
In general, important events generate an IML entry each time they occur. They are not consolidated into one event log entry.
When less important events are repeated, they are consolidated into one IML entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.
- **Description**—The description identifies the component and detailed characteristics of the recorded event.
If the iLO firmware is rolled back, the description UNKNOWN EVENT TYPE might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the log.

To access troubleshooting information for selected events, click the link in the **Description** column.

More information

[Configuring iLO SNTP settings](#)

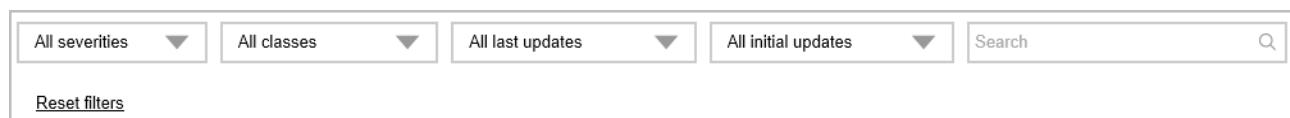
IML icons

iLO uses the following icons to indicate IML event severity:

- **Critical**—The event indicates a service loss or an imminent service loss. Immediate attention is needed.
- **Caution**—The event is significant but does not indicate performance degradation.
- **Informational**—The event provides background information.
- **Repaired**—An event has undergone corrective action.
- **Unknown**—The event severity could not be determined.

Customizing the IML view

You can customize the IML view by using the controls at the top of the page.



- To filter by severity, select a severity level from the **Severity** menu.
- To filter by class, select a class from the **Class** menu.
- To filter by the **Last Update** date, select a value in the **Last Update** menu.
If you select the **Specific date range** option, select a date range in the **Last Update Range** dialog box, and then click **Apply**.
- To filter by the **Initial Update** date, select a value in the **Initial Update** menu.
If you select the **Specific date range** option, select a date range in the **Initial Update Range** dialog box, and then click **Apply**.
- To search for events based on dates, event IDs, or description text, enter text in the **Search** box, and then press **Enter**.
- Click **Reset filters** to set the filters back to the default values.
- Click a column heading to sort the IML table by that column.
- When sorting the IML table by column, click the triangle next to the column heading to change the display to ascending or descending order.

Marking an IML entry as repaired

Use this feature to change the status of an IML entry from **Critical** or **Caution** to **Repaired**.

Prerequisites

You must have the Configure iLO Settings privilege to perform this procedure.

Changing an IML entry to repaired status

When a **Critical** or **Caution** event is reported in the IML:

1. Investigate and repair the issue.
2. Navigate to the **Information**→**Integrated Management Log** page.
3. Select the log entry.

To select an IML entry, click the check box next to the entry in the first column of the IML table. If a check box is not displayed next to an IML entry, that entry cannot be marked as repaired.

ID	Severity	Class	Last Update	Initial Update	Count	Description
141	critical	Network	12/02/2014 11:17	12/02/2014 11:17	1	Network Adapter Link Down (Slot 0, Port 2)

4. Click **Mark as Repaired**.

The iLO web interface refreshes, and the selected log entry status changes to **Repaired**.

Adding a maintenance note to the IML

Use the maintenance note feature to create a log entry that logs information about maintenance activities such as component upgrades, system backups, periodic system maintenance, or software installations.

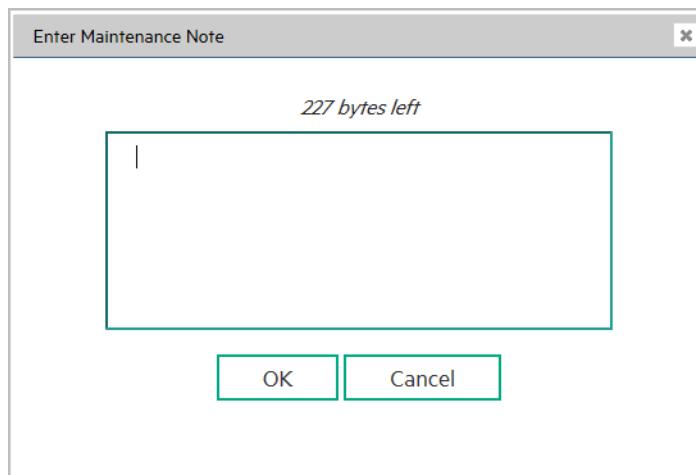
Prerequisites

Configure iLO Settings privilege

Adding a maintenance note

1. Navigate to the **Information**→**Integrated Management Log** page.
2. Click **Add Maintenance Note**.

The **Enter Maintenance Note** window opens.



3. Enter the text that you want to add as a log entry, and then click **OK**.

You can enter up to 227 bytes of text. You cannot submit a maintenance note without entering some text.

An **Informational** log entry with the class **Maintenance** is added to the IML.

Saving the IML to a CSV file

Use a supported browser to export the IML to a CSV file.

For Internet Explorer users only: This feature is supported with Internet Explorer 11 and later.

1. Navigate to the **Information**→**Integrated Management Log** page.
2. Click **View CSV**.

3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.
4. Click **Close** to close the window.

Clearing the IML

Users with the Configure iLO Settings privilege can clear the IML of all previously logged information.

1. Navigate to the **Information**→**Integrated Management Log** page.
2. Click **Clear IML**.
3. When prompted to confirm the request, click **OK**.

The following event is recorded:

IML Cleared (iLO 4 user:<user name>)

You can also clear the IML from the server HPE System Management Homepage.

IML troubleshooting links

Troubleshooting information is available for selected IML events. Supported events are displayed as links in the **Description** column on the **Integrated Management Log** page.

15 Using the Active Health System

Active Health System

The Active Health System monitors and records changes in the server hardware and system configuration.

The Active Health System provides:

- Continuous health monitoring of over 1600 system parameters
- Logging of all configuration changes
- Consolidated health and service alerts with precise time stamps
- Agentless monitoring that does not affect application performance

Active Health System data collection

The Active Health System does not collect information about your operations, finances, customers, employees, or partners.

Examples of information that is collected:

- Server model and serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS and driver versions and settings

The Active Health System does not parse or change operating system data from third-party error event log activities (for example, content created or passed through the operating system).

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data.

When the Active Health System Log is full, new data overwrites the oldest data in the log.

It takes less than 5 minutes to download the Active Health System Log and send it to a Hewlett Packard Enterprise support professional to help you resolve an issue.

When you download and send Active Health System data to Hewlett Packard Enterprise, you agree to have Hewlett Packard Enterprise use the data for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the privacy statement, available at <http://www.hpe.com/info/privacy>.

The Active Health System Log is not supported on servers that do not have a NAND.

Active Health System Log download methods

You can use the following methods to download the Active Health System Log:

- **iLO web interface**—For instructions, see “[Downloading the Active Health System Log for a date range](#)” (page 190) and “[Downloading the entire Active Health System Log](#)” (page 190).
- **Intelligent Provisioning**—For instructions, see the Intelligent Provisioning user guide.
- **Active Health System download CLI**—For instructions, see the server troubleshooting guide.
- **curl**—For instructions, see “[Extracting the Active Health System Log by using curl](#)” (page 191).

Downloading the Active Health System Log for a date range

1. Navigate to the **Information→Active Health System Log** page.
The Active Health System Log is inaccessible when it is being used by Intelligent Provisioning or the Active Health System download CLI tool.
2. Enter the range of days to include in the log. The default value is seven days.
 - a. Click the **From** box.
A calendar is displayed.
 - b. Select the range start date on the calendar.
 - c. Click the **To** box.
A calendar is displayed.
 - d. Select the range end date on the calendar.
3. Optional: Enter the following information to include in the downloaded file:
 - Support case number
 - Contact name
 - Phone number
 - E-mail address
 - Company name

The contact information you provide will be treated in accordance with the Hewlett Packard Enterprise privacy statement. This information is not written to the log data stored on the server.
4. Click **Download**.
5. Save the file.
6. If you have an open support case, you can email the log file to hpsupport_global@hpe.com.
 - Use the following convention for the email subject: CASE: <case number>.
 - Files that are larger than 15 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.

Downloading the entire Active Health System Log

It might take a long time to download the entire Active Health System Log. If you must upload the Active Health System Log for a technical issue, Hewlett Packard Enterprise recommends downloading the log for the specific range of dates in which the problem occurred.

1. Navigate to the **Information→Active Health System Log** page.
The Active Health System Log is inaccessible when it is being used by Intelligent Provisioning or the Active Health System download CLI tool.
2. Click **Show Advanced Settings**.
3. Optional: Enter the following information to include in the downloaded file:
 - Support case number
 - Contact name
 - Phone number
 - E-mail address
 - Company name

The contact information that you provide will be treated in accordance with the Hewlett Packard Enterprise privacy statement. This information is not written to the log data stored on the server.

4. Click **Download Entire Log**.
5. Save the file.
6. If you have an open support case, you can email the log file to hpsupport_global@hpe.com.
 - Use the following convention for the email subject: CASE: <case number>.
 - Files that are larger than 15 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.

Extracting the Active Health System Log by using curl

iLO 4 1.30 and later supports extracting the Active Health System log with the `curl` command-line tool.

1. Install `curl`.
You can download `curl` from the following website: <http://curl.haxx.se/>.
2. Open a command window.
3. Enter one of the following commands:
 - To download the Active Health System log for a range of dates, enter the following command:
`curl "https://<iLO IP address>/ahsdata/ahs.ahs?from=<yyyy-mm-dd>&to=<yyyy-mm-dd>" -k -v -u <username>:<password> -o <filename>.ahs`
 - To download the entire Active Health System log, enter the following command:
`curl "https://<iLO IP address>/ahsdata/ahs.ahs?downloadAll=1" -k -v -u <username>:<password> -o <filename>.ahs`
4. Close the command window.

curl command usage with iLO 4

When you use `curl` to extract the Active Health System log, the command components include the following:

- `<iLO IP address>` is the iLO IP address.
- `from=<yyyy-mm-dd>&to=<yyyy-mm-dd>` represents the start and end date of the range of dates to include in the log. Enter dates in the format `year-month-day`, for example, `2016-07-29` for July 29, 2016.
- `downloadAll=1` indicates that you want to download the entire log.
- `-k` specifies that HTTPS warnings will be ignored.
- `-v` specifies verbose output.
- `-u <username>:<password>` specifies your iLO user account credentials.
- `-o <filename>.ahs` specifies the output file name and path.

Clearing the Active Health System Log

If the log file is corrupted, or if you want to clear and restart logging, use the following procedure to clear the Active Health System Log.

Prerequisites

Configure iLO Settings privilege

Clearing the log

1. Navigate to the **Information**→**Active Health System Log** page.

The Active Health System Log is inaccessible when it is being used by Intelligent Provisioning or the Active Health System download CLI tool.

2. Click **Show Advanced Settings**.

3. Scroll to the **Clear Log** section, and then click the **Clear** button.

4. When prompted to confirm the request, click **OK**.

iLO notifies you that the log is being cleared.

5. Reset iLO.

Resetting iLO after clearing the Active Health System Log is required because some Active Health System data is recorded to the log only during iLO startup. Performing this step ensures that a complete set of data is available in the log.

6. Reboot the server.

Rebooting the server after clearing the Active Health System Log is required because some information, such as the operating system name and version, is logged at server startup. Performing this step ensures that a complete set of data is available in the log.

More information

[iLO diagnostics](#)

16 Using the iLO diagnostics, reboot, and reset features

iLO diagnostics

The **Diagnostics** page displays the iLO self-test results and allows you to reset iLO, generate an NMI to the system, or configure redundant ROM.

Viewing iLO self-test results

The **iLO Self-Test Results** section displays the results of internal iLO diagnostic tests, including the test name, status, and notes.

Navigate to the **Information**→**Diagnostics** page.

Self-test details

iLO Self-Test Results		
Self-Test	Status	Notes
CPLD - PAL0	ⓘ	ProLiant MicroServer Gen8 System Programmable Logic Device version 0x06
BMC USB Interface	✓	
NVRAM data	✓	
Embedded Flash/SD-CARD	✓	Controller firmware revision 2.10.00
EEPROM	✓	
Host ROM	✓	
Supported host	✓	

- The test status is listed in the **Status** column. To view a tooltip description, move the cursor over a status icon.
- If a status has not been reported for a test, the test is not listed.
- The tests that are run are system-dependent. Not all tests are run on all systems. To see the tests that are performed on your system, view the list on the **Diagnostics** page.
- A test might include additional information in the **Notes** column. This column displays the versions of other system programmable logic, such as the System Board PAL or the Power Management Controller.
- The following information is displayed in the **Embedded Flash/SD-CARD** test results:
 - Firmware revision
 - SD-CARD size
 - SD-CARD slot
 - SD-CARD write counterThe write counter counts data in 512-byte blocks. If the write counter is at zero, no write counter text is displayed.
Write counter information is displayed only when a recognized supported SD-Card is installed with a retail version of the iLO firmware.

Resetting the iLO processor through the web interface

If iLO is slow to respond, you might need to reset the iLO processor.

Using the **Reset** option does not make any configuration changes, but ends all active connections to the iLO firmware. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reset iLO until the process is finished.

Prerequisites

Configure iLO Settings privilege

Resetting iLO

1. Navigate to the **Information→Diagnostics** page.
2. Click **Reset**.
3. When prompted to confirm the request, click **OK**.

iLO resets and closes your browser connection.

For other reset methods, see “[Rebooting \(Resetting\) iLO](#)” (page 195).

Generating an NMI

The **Generate NMI to System** feature enables you to stop the operating system for debugging.

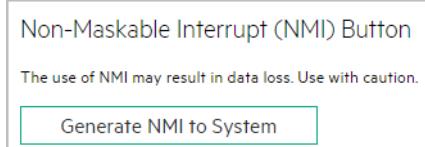
⚠ **CAUTION:** Generating an NMI as a diagnostic and debugging tool is used primarily when the operating system is no longer available. NMI is not used during normal operation of the server. Generating an NMI does not gracefully shut down the operating system, but causes the operating system to crash, resulting in lost service and data. Use the **Generate NMI to System** button only in extreme cases in which the OS is not functioning correctly and an experienced support organization has recommended an NMI.

Prerequisites

You must have the Virtual Power and Reset privilege to perform this procedure.

Generating an NMI

1. Navigate to the **Information→Diagnostics** page.
2. Click **Generate NMI to System**.



3. When iLO warns you that generating an NMI to the system might cause data loss, click **OK** to confirm, or click **Cancel**.

If you clicked **OK**, iLO confirms that the NMI was sent.

Configuring redundant ROM

Prerequisites

- The server supports redundant ROM.
- Virtual Power and Reset privilege

Updating the ROM settings

1. Navigate to the **Information→Diagnostics** page.

The screenshot shows the 'Information→Diagnostics' page with the 'ROM' section selected. It displays two tables: 'Active ROM' and 'Backup ROM', and a 'Swap ROM' button.

Active ROM	
System ROM	J06 06/06/2014
System ROM Date	06/06/2014

Backup ROM	
Backup ROM	J06 06/06/2014
Bootblock Date	02/04/2012

Swap ROM

The Active ROM table shows the version and date of the active system ROM.

The Backup ROM table shows the version of the backup ROM and the release date of the backup ROM bootblock (ProLiant Gen8 servers only). The backup ROM is typically the previously installed version.

2. To swap the active ROM and the backup ROM, click **Swap ROM**.
3. When prompted to confirm the request, click **OK**.

The change will take effect after the next system reboot.

Rebooting (Resetting) iLO

In some cases, it might be necessary to reboot iLO; for example, if iLO is not responding to the browser.

① **IMPORTANT:** The iLO web interface and the ROM-based setup utilities sometimes uses the term iLO reset to mean an iLO reboot.

Rebooting iLO does not make any configuration changes, but it ends all active connections to iLO.

To reboot iLO, use one of the following methods:

- Click **Reset** on the **Information→Diagnostics** page in the iLO web interface.
- Use the CLI or HPONCFG. For instructions, see the iLO scripting and CLI guide.
- The Insight Management Agents 5.40 and later can reset iLO. Select the **Reset iLO** option on the **Management Agent** page in the iLO section.
- Click **Apply** on the **Network→iLO Dedicated Network Port or Shared Network Port→General** page. This action forces the iLO management processor to reset. If the **Apply** button is not available, change a setting, change it back, and then click **Apply** to reset iLO without changing the configuration.
- Use the iLO 4 Configuration Utility. The iLO 4 Configuration Utility is available only on servers that support UEFI.
- Use the UID button on supported ProLiant Gen9 servers.
- Use the iLO RESTful API and the RESTful Interface Tool. For more information, see <http://www.hpe.com/info/restfulapi>.
- Use IPMI. For more information, see the iLO IPMI user guide.

If none of these methods are available or working as expected, you must power down the server and disconnect the power supplies completely.

More information

[iLO diagnostics](#)

[Resetting iLO \(iLO 4 Configuration Utility\)](#)

[Rebooting iLO with the server UID button](#)

Resetting iLO (iLO 4 Configuration Utility)

Prerequisite

Configure iLO Settings privilege

To reset iLO:

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Reset iLO**.
The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.
5. Select **YES**, and press **Enter**.
6. When prompted to confirm the reset, press **Enter**.
iLO resets and all active connections are ended. If you are managing iLO remotely, the remote console session is automatically ended.
When you reset iLO, the iLO 4 Configuration Utility is not available again until the next reboot.
7. Resume the boot process:
 - a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.
The UEFI System Utilities are still open from the previous session.
 - b. Press **Esc** until the main menu is displayed.
 - c. Select **Exit and Resume Boot** in the main menu, and press **Enter**.
 - d. When prompted to confirm the request, press **Enter** to exit the utility and resume the normal boot process.

Rebooting iLO with the server UID button

The UID button on ProLiant Gen9 servers (if present) can be used to initiate a manual reboot of iLO.

For more information about the UID button, see the user guide for your server at the following website: <http://www.hpe.com/support/proliantgen9/docs>.

Performing a graceful iLO reboot with the server UID button

When you initiate a graceful iLO reboot, the iLO firmware initiates the iLO reboot.

Initiating a graceful iLO reboot does not make any configuration changes, but ends all active connections to iLO. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reboot iLO until the process is finished.

To initiate a graceful iLO reboot, press and hold the UID button for 5 to 9 seconds.

The UID button/LED flashes blue 4 Hz/cycle per second to indicate that a graceful iLO reboot is in progress.

Performing a hardware iLO reboot with the server UID button

When you initiate a hardware iLO reboot, the server hardware initiates the iLO reboot.

To initiate a hardware iLO reboot, press and hold the UID button for 10 seconds or longer.

The UID button/LED flashes blue 8 Hz/cycle per second to indicate that an iLO hardware reboot is in progress.

⚠ **CAUTION:** Initiating a hardware iLO reboot does not make any configuration changes, but ends all active connections to iLO. If a firmware flash is in progress, it is interrupted, which might cause data corruption on the flash device. If data corruption occurs on the flash device, use the recovery method described in “[iLO network Failed Flash Recovery](#)” (page 355). Data loss or NVRAM corruption might occur during a hardware iLO reboot. Do not initiate a hardware reboot if other troubleshooting options are available.

Reset iLO to the factory default settings

In some cases, you might need to reset iLO to the factory default settings. For example, you must reset iLO to the default settings when you disable FIPS mode. You can use the iLO RBSU or the UEFI system utilities to perform this task.

⚠ **CAUTION:** This operation clears all user and license data.

If a server has an installed iLO Advanced license when you perform this procedure, the iLO Advanced icon might be selected when the server boot process finishes. The icon will be set correctly after POST completes, or after the server is shut down, powered off, and then powered on again.

Resetting iLO to the factory default settings (iLO RBSU)

⚠ **CAUTION:** This operation clears all user and license data.

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F8** in the server POST screen.
The iLO RBSU starts.
4. Select **File→Set Defaults**.
5. When prompted to confirm the request, press **F10** to continue.
iLO RBSU notifies you that iLO will be reset to the factory defaults, and will reboot. The iLO RBSU utility will close.
6. Press **Enter**.
iLO resets and the server boot process finishes.
7. Optional: Use the default iLO account information to log in to iLO after the reset.

More information

[iLO default credentials](#)

Resetting iLO to the factory default settings (iLO 4 Configuration Utility)

⚠ **CAUTION:** This operation clears all user and license data.

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.

3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Set to factory defaults**, and press **Enter**.
The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.
5. Select **YES**, and press **Enter**.
6. When prompted to confirm the request, press **Enter**.
iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended. You cannot access the iLO 4 Configuration Utility again until after the next system reboot.
7. Resume the boot process:
 - a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.
The iLO 4 Configuration Utility screen is still open from the previous session.
 - b. Press **Esc** until the main menu is displayed.
 - c. Select **Exit and Resume Boot** in the main menu, and press **Enter**.
 - d. When prompted to confirm the request, press **Enter** to exit the screen and resume the boot process.
8. Optional: Use the default iLO account information to log in to iLO after the reset.

More information

[iLO default credentials](#)

17 Using iLO Federation

iLO Federation features

iLO Federation enables you to manage multiple servers from one system using the iLO web interface.

When configured for iLO Federation, iLO uses multicast discovery and peer-to-peer communication to enable communication between the systems in an iLO Federation group.

When an iLO Federation page loads, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all data for the selected iLO Federation group is retrieved.

iLO 4 firmware version 1.40 and later supports the following features:

- Group health status—View server health and model information.
- Group Virtual Media—Connect scripted media for access by the servers in an iLO Federation group.
- Group power control—Manage the power status of the servers in an iLO Federation group.
- Group power capping—Set dynamic power caps for the servers in an iLO Federation group.
- Group firmware update—Update the firmware of the servers in an iLO Federation group.

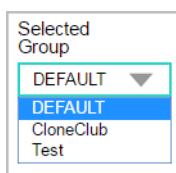
iLO 4 firmware version 2.00 and later supports the following features:

- Group license installation—Enter a license key to activate iLO licensed features on the servers in an iLO Federation group.
- Group configuration—Add iLO Federation group memberships for multiple iLO systems.

Any user can view information on iLO Federation pages, but a license is required for using the following features: Group Virtual Media, Group power control, Group power capping, Group configuration, and Group firmware update. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Selected Group list

All of the iLO Federation pages under **iLO Federation** in the navigation tree have a **Selected Group** list.



When you select a group from the **Selected Group** list:

- The servers affected by a change on the **Group Virtual Media**, **Group Power**, **Group Firmware Update**, **Group Licensing**, and **Group Configuration** pages are listed in the **Affected Systems** table.
- The information displayed on iLO Federation pages applies to all of the servers in the selected group.
- The changes you make on iLO Federation pages apply to all of the servers in the selected group.
- The selected group is saved in a cookie and remains persistent, even when you log out of iLO.

After you select a group, you can filter the servers in the list to view server information or perform actions on a subset of the servers in the group.

Selected Group list filters

When you filter the list of servers:

- The information displayed on iLO Federation pages applies to all of the servers in the selected group that meet the filter criteria.
- The changes you make on iLO Federation pages apply to all of the servers in the selected group that meet the filter criteria.
- The filter settings are saved in a cookie and remain persistent, even when you log out of iLO.

Selected Group list filter criteria

You can use the following criteria to filter the servers in a group:

- **Health status**—Click a health status link to select servers with a specific health status.
- **Model**—Click a server model number link to select servers matching the selected model.
- **Server name**—Click a server name to filter by an individual server.
- **Firmware Information**—Click a firmware version or flash status to select servers matching the selected firmware version or status.
- **TPM or TM Option ROM Measuring**—Click an Option ROM Measuring status to include or exclude servers matching the selected Option ROM Measuring status.
- **License usage**—If an error message related to a license key is displayed, click the license key to select servers that use that license key.
- **License type**—Click a license type to select servers with the selected license type installed.
- **License status**—Click a license status to select servers with an installed license matching the selected status.

Exporting iLO Federation information to a CSV file

All of the pages in the **iLO Federation** navigation tree menu, except for the **Group Power Settings** page, allow you to export information to a CSV file.

For Internet Explorer users only: This feature is supported with Internet Explorer 11 and later.

1. Navigate to a page in the **iLO Federation** menu that supports the file export feature.
2. Click **View CSV**.
3. In the **CSV Output** window, click **Save**, and then follow the browser prompts to save or open the file.

When you export the list, the CSV file contains only the servers displayed on the iLO Federation page.

If multiple pages of servers are included in the list, the CSV file will contain only the servers that are currently displayed on the iLO web interface page.

If a query error occurred, the systems that did not respond to the query are excluded from the iLO web interface page and the CSV file.

iLO Federation information export options

You can export the following information from the **iLO Federation** pages:

- Systems with critical or degraded status—Export this list from the **Multi-System View** page.
- iLO peers list—Export this list from the **Multi-System Map** page.
- Affected systems list—Export the list of systems affected by an iLO Federation action on the following pages:
 - **Group Virtual Media**
 - **Group Power**
 - **Group Firmware Update**
 - **Group Licensing**
 - **Group Configuration**

The export feature is not supported on the **Group Power Settings** page.

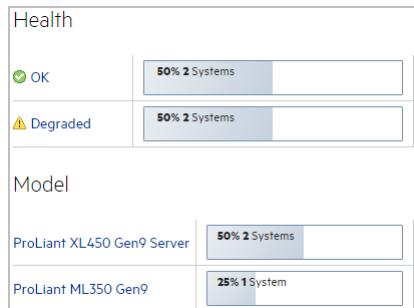
iLO Federation Multi-System view

The **Multi-System View** page provides a summary of the server models, server health, and critical and degraded systems in an iLO Federation group.

Viewing server health and model information

1. Navigate to the **iLO Federation**→**Multi-System View** page.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of servers, click a health status, server model, or server name link.

Server health and model details



- **Health**—The number of servers in each listed health status. The percentage of the total number of servers in each listed health status is also displayed.
- **Model**—The list of servers, grouped by model number. The percentage of the total number of servers for each model number is also displayed.
- **Critical and Degraded Systems**—The list of servers in the critical or degraded state.

More information

[Viewing health summary information](#)

Viewing servers with critical and degraded status

1. Navigate to the **iLO Federation**→**Multi-System View** page.
2. Select a group from the **Selected Group** menu.

3. Optional: To filter the list of servers, click a health status, server model, or server name link.
4. Click **Next** or **Previous** (if available) to view more servers in the **Critical and Degraded Systems** list.

Critical and degraded server status details

Critical and Degraded Systems						
Server Name	System Health	Server Power	UID Indicator	System ROM	iLO Hostname	IP Address
Host is unnamed	⚠ Degraded	● ON	● UID OFF	P89 v2.20 (12/17/2015) 12/17/2015		
	⚠ Degraded	● ON	● UID OFF	P92 v2.20 (12/08/2015) 12/08/2015		

- **Server Name**—The server name defined by the host operating system.
- **System Health**—The server health status.
- **Server Power**—The server power status (**ON** or **OFF**).
- **UID Indicator**—The state of the server UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **System ROM**—The installed System ROM version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

More information

[Exporting iLO Federation information to a CSV file](#)

Viewing the iLO Federation Multi-System Map

The **Multi-System Map** page displays information about the peers of the local iLO system. The local iLO system identifies its peers through multicast discovery.

When an iLO Federation page loads, a data request is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all of the data for the selected group is retrieved.

1. Navigate to the **iLO Federation**→**Multi-System Map** page.
2. Select a group from the **Selected Group** menu.

iLO peer details

iLO Peers					View CSV
#	iLO UUID	Last Seen	Last Error	URL	IP
124		3:57:16 PM	No Error	http://	
126		3:52:03 PM	No Error	http://	

- **#**—The peer number.
- **iLO UUID**—The iLO system UPnP UUID.
- **Last Seen**—The time stamp of the last communication from the server.
- **Last Error**—A description of the most recent communication error between the listed peer and the local iLO system.

- **URL**—The URL for starting the iLO web interface for the listed peer.
- **IP**—The peer IP address.

More information

[Exporting iLO Federation information to a CSV file](#)

iLO Federation Group Virtual Media

Group Virtual Media enables you to connect scripted media for access by the servers in an iLO Federation group.

- Scripted media only supports 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO). The image must be on a web server on the same network as the grouped iLO systems.
- Only one of each type of media can be connected to a group at the same time.
- You can view, connect, eject, or boot from scripted media. When you use scripted media, you save a floppy disk or CD/DVD-ROM disk image to a web server and connect to the disk image by using a URL. iLO accepts URLs in HTTP or HTTPS format. iLO does not support FTP.

Using the iLO Virtual Floppy to boot a remote host server is supported only on ProLiant Gen8 servers. It is not supported on ProLiant Gen9 servers or Synergy compute modules.

- Before you use the Virtual Media feature, review the Virtual Media operating system considerations.

Connecting scripted media for groups

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Connecting scripted media

1. Navigate to the **iLO Federation**→**Group Virtual Media** page.
2. Select a group from the **Selected Group** menu.

The scripted media you connect will be available to all of the systems in the selected group.

3. Enter the URL for the scripted media disk image in the **Scripted Media URL** box in the **Connect Virtual Floppy** section (IMG files) or the **Connect CD/DVD-ROM** section (ISO files).

Connect CD/DVD-ROM to 4 Systems	
Media Inserted	None
Scripted Media URL	<input type="text" value="http://"/>
Boot on Next Reset	<input type="checkbox"/>
Insert Media	

4. Select the **Boot on Next Reset** check box if you want the servers in the group to boot to this disk image only on the next server reboot.

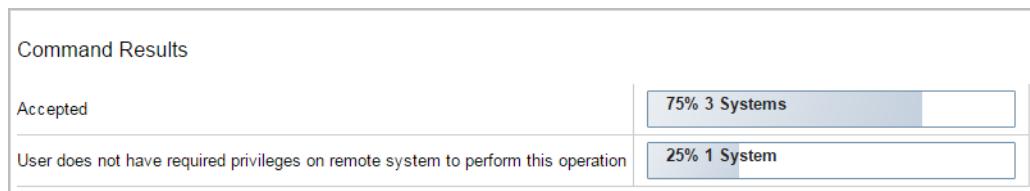
The disk image will be ejected automatically on the second server reboot so that the servers do not boot to it twice.

If this check box is not selected, the disk image will remain connected until it is ejected manually, and the servers will boot to it on all subsequent server resets, if the system boot options are configured accordingly.

If a server in the group is in POST when you use the **Boot on Next Reset** check box, an error occurs because you cannot modify the server boot order during POST. Wait for POST to finish, and then try again.

5. Click **Insert Media**.

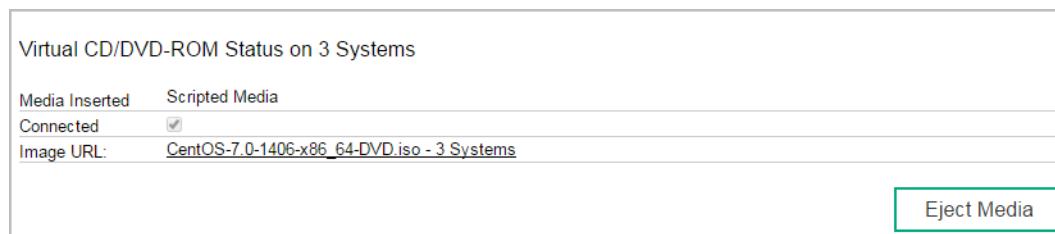
iLO displays the command results.



Viewing scripted media status for groups

Navigate to the **iLO Federation**→**Group Virtual Media** page.

Scripted media details



When scripted media is connected to the systems in an iLO Federation group, the following details are listed in the **Virtual Floppy Status** section and **Virtual CD/DVD-ROM Status** section:

- **Media Inserted**—The Virtual Media type that is connected. **Scripted Media** is displayed when scripted media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.
- **Image URL**—The URL that points to the connected scripted media.

The **Virtual Floppy Status** and **Virtual CD/DVD-ROM Status** sections are displayed only when media is connected.

Ejecting a scripted media device

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Ejecting a scripted media device

1. Navigate to the **iLO Federation**→**Group Virtual Media** page.

2. Select a group from the **Selected Group** menu.
The scripted media device that you eject will be disconnected from all of the systems in the selected group.
3. Click **Eject Media** in the **Virtual Floppy Status** section or the **Virtual CD/DVD-ROM Status** section.

Servers affected by a Group Virtual Media action

The **Affected Systems** section provides the following details about the servers affected when you initiate a Group Virtual Media action:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More information

[Exporting iLO Federation information to a CSV file](#)

iLO Federation Group Power

The Group Power feature enables you to manage the power of multiple servers from a system running the iLO web interface. Use this feature to do the following:

- Power off, reset, or power-cycle a group of servers that are in the **ON** or **Reset** state.
- Power on a group of servers that are in the **OFF** state.
- View the list of servers that will be affected when you click a button in the **Virtual Power Button** section of the **Group Power** page.

Changing the power state for a group of servers

The **Virtual Power Button** section on the **Group Power** page summarizes the current power state of the servers in a group. The summary information includes the total number of servers that are in the **ON**, **OFF**, or **Reset** state. The **System Power** summary indicates the state of the server power when the page is first opened. Use the browser refresh feature to update the **System Power** information.

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Each member of the selected iLO Federation group has granted the Virtual Power and Reset privilege to the group.

Changing the power state for a group

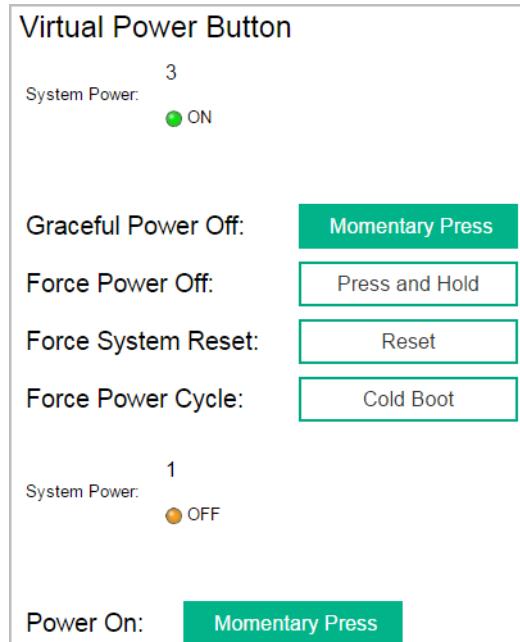
1. Navigate to the **iLO Federation**→**Group Power** page.

2. Select a group from the **Selected Group** menu.
iLO displays the grouped servers by power state with a counter that shows the total number of servers in each state.
3. To change the power state of a group of servers, do one of the following:
 - For servers that are in the **ON** or **Reset** state, click one of the following buttons:
 - Momentary Press**
 - Press and Hold**
 - Reset**
 - Cold Boot**
 - For servers that are in the **OFF** state, click the **Momentary Press** button.
The **Press and Hold**, **Reset**, and **Cold Boot** options are not available for servers that are in the **OFF** state.
4. When prompted to confirm the request, click **OK**.
iLO displays a progress bar while the grouped servers respond to the Virtual Power Button action. The progress bar indicates the number of servers that successfully processed the command.
The **Command Results** section displays the command status and results, including error messages related to the power state change.

More information

[Power-on protection](#)

Virtual Power Button options



- **Momentary Press**—The same as pressing the physical power button.
Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. Hewlett Packard Enterprise recommends using

system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power Button.

- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.
The servers in the selected group are powered off as a result of this operation. Using this option might circumvent a graceful operating system shutdown.
This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently, depending on a short press or long press.
- **Reset**—Forces the servers in the selected group to warm-boot: CPUs and I/O resources are reset. Using this option circumvents a graceful operating system shutdown.
- **Cold Boot**—Immediately removes power from the servers in the selected group. Processors, memory, and I/O resources lose main power. The servers will restart after approximately 6 seconds. Using this option circumvents a graceful operating system shutdown.

Servers affected by the Virtual Power Button

The **Affected Systems** list provides the following details about the servers affected when you initiate a Virtual Power Button action:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More information

[Exporting iLO Federation information to a CSV file](#)

Configuring group power capping

Prerequisites

- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.

Configuring a power cap

1. Navigate to the **iLO Federation**→**Group Power Settings** page.
2. Select a group from the **Selected Group** menu.
Changes you make on this page affect all of the systems in the selected group.
3. Select the **Enable power capping** check box.
4. Enter the **Power Cap Value** in watts, BTU/hr, or as a percentage.

The percentage is the difference between the maximum and minimum power values. The power cap value cannot be set below the server minimum power value.

When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.

5. Click **Apply**.

Power capping considerations

The Group Power Settings feature enables you to set dynamic power caps for multiple servers from a system running the iLO web interface.

- When a group power cap is set, the grouped servers share power to stay below the power cap. More power is allocated to busy servers and less power is allocated to servers that are idle.
- The power caps that you set for a group operate concurrently with the power caps that you can set on the **Power Settings** page for an individual server.
- If a power cap configured at the enclosure or individual server level or by another iLO Federation group affects a server, other group power caps might allocate less power to that server.
- When a power cap is set, the average power reading of the grouped servers must be at or below the power cap value.
- During POST, the ROM runs two power tests that determine the peak and minimum observed power values.

Consider the values in the **Automatic Group Power Capping Settings** table when determining your power capping configuration.

- **Maximum Available Power**—The total power supply capacity for all servers in a group. This value is the **Maximum Power Cap** threshold. The servers in a group must not exceed this value.
- **Peak Observed Power**—The maximum observed power for all servers in a group. This value is the **Minimum High-Performance Cap** threshold, and it represents the maximum power that the servers in a group use in their current configuration. A power cap set to this value does not affect server performance.
- **Minimum Observed Power**—The minimum observed power for all servers in a group. This value is the **Minimum Power Cap** threshold, and it represents the minimum power that the servers in a group use. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- Power capping is not supported on servers with an installed Flex Slot Battery Backup Unit.
- Power capping is not supported on Synergy compute modules.
- You cannot use the iLO web interface to configure group power capping settings for SL servers and some XL servers. Use one of the following tools to configure the power capping settings for these servers:
 - HPE ProLiant Power Interface Control Utility
 - HPE Advanced Power Manager

To verify the power management features your XL server supports, see the server Quickspecs at <http://www.hpe.com/info/qsl/>.

Viewing group power capping information

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Viewing group power capping information

1. Navigate to the **iLO Federation**→**Group Power Settings** page.
2. Select a group from the **Selected Group** menu.
3. Optional: When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.

Power capping details

The screenshot shows the 'Group Power Settings' interface. At the top, it says '2 Systems Selected' and 'Selected Group: automation'. The main section is titled 'HPE Automatic Group Power Capping Settings'. It displays the following data:

Measured Power Values	BTU/hr	Percent (%)	Power Cap Thresholds
Maximum Available Power	6142 BTU/hr	100%	Maximum Power Cap
Peak Observed Power	2678 BTU/hr	43%	Minimum High-Performance Cap
Minimum Observed Power	764 BTU/hr	12%	Minimum Power Cap

Below this, a table shows the 'Power Cap Value' as 2487 BTU/hr, 41%, and a percentage sign. There is a checkbox for 'Enable power capping' which is checked, and buttons for 'Show values in Watts' and 'Apply'.

The 'Current State' section shows 'Present Power Reading' as 290 BTU/hr and 'Present Power Cap' as 2487 BTU/hr.

The 'Group Power Allocations for this system' section shows 'Present Power Cap: DEFAULT' as 0 BTU/hr and 'Present Power Cap: automation' as 0 BTU/hr.

- **HPE Automatic Group Power Capping Settings**—This section shows the following details:
 - **Measured Power Values**—The maximum available power, peak observed power, and minimum observed power.
 - **Power Cap Value**—The power cap value, if one is configured.
- **Current State**—This section includes the following details:
 - **Present Power Reading**—The current power reading for the selected group.
 - **Present Power Cap**—The total amount of power allocated to the selected group. This value is 0 if a power cap is not configured.
- **Group Power Allocations for this system**—The group power caps that affect the local iLO system, and the amount of power allocated to the local iLO system by each group power cap. If a power cap is not configured, the allocated power value is 0.

iLO Federation Group Firmware Update

The Group Firmware Update feature enables you to view firmware information and update the firmware of multiple servers from a system running the iLO web interface. The following firmware types are supported with iLO Federation:

- iLO firmware
- System ROM (BIOS)
- Chassis firmware (Power Management)
- Power Management Controller
- System Programmable Logic Device (CPLD)
- NVMe Backplane Firmware

Obtaining the iLO firmware image file

The BIN file from the iLO Online ROM Flash Component is required for updating the iLO firmware on the **Group Firmware Update** page.

1. Navigate to the Hewlett Packard Enterprise Support Center: <http://www.hpe.com/support/hpesc>.
2. To locate and download the iLO Online ROM Flash Component file, follow the onscreen instructions.
To extract the BIN file, download a Windows or Linux component.
3. Extract the BIN file.
 - For Windows components: Double-click the downloaded file, and then click the **Extract** button. Select a location for the extracted files, and then click **OK**.
 - For Linux components: Depending on the file format, enter one of the following commands:
 - `#sh ./CP00XXXX.scexe -unpack=/tmp/`
 - `#rpm2cpio hp-firmware-ilo4-2.xx-1x1.i386.rpm | cpio -id`

The name of the iLO firmware image file is similar to `ilo4_<yyy>.bin`, where `<yyy>` represents the firmware version.

The URL to enter for the iLO firmware image file is similar to
`http://<server.example.com>/<subdir>/ilo4_240.bin`.

Obtaining supported server firmware image files

1. Navigate to the Hewlett Packard Enterprise Support Center: <http://www.hpe.com/support/hpesc>.
2. To locate and download an Online ROM Flash Component file, follow the onscreen instructions.
3. Double-click the downloaded file, and then click the **Extract** button.
4. Select a location for the extracted files, and then click **OK**.

Server firmware file type details

- When you update the system ROM, you must use a signed image or the signed ROMPAQ image:
 - **Signed image example:**
http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash
 - **Signed ROMPAQ image example:**
<http://<server.example.com>/<wwwroot>/CPQPJ0612.A48>
- The Power Management Controller, chassis firmware, and NVMe backplane files use the file extension `.hex`. For example, the file name might be similar to `ABCD5S95.hex`.
- The System Programmable Logic Device (CPLD) firmware file uses the file extension `.vme`.

Updating the firmware for multiple servers

Prerequisites

- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Updating firmware

1. Download the supported firmware from the Hewlett Packard Enterprise Support Center: <http://www.hpe.com/support/hpesc>.
2. Save the firmware file to a web server.
3. Navigate to the **iLO Federation**→**Group Firmware Update** page.
4. Select a group from the **Selected Group** menu.
All of the systems in the selected group will be affected when you initiate a firmware update on this page.
5. Optional: To filter the list of affected systems, click a firmware version, flash status, or TPM or TM Option ROM Measuring status link.

△ **CAUTION:** If you attempt to perform a system ROM or option ROM update on a server with Option ROM Measuring enabled, iLO prompts you to cancel the update, verify that you have a recovery key, and suspend BitLocker before the update. Failure to follow these instructions might result in losing access to your data.

6. In the **Firmware Update** section, enter the URL to the firmware file on your web server, and then click the **Update Firmware** button.

Each selected system downloads the firmware image and attempts to flash it.

The **Flash Status** section is updated and iLO notifies you that the update is in progress. When the update is complete, the **Firmware Information** section is updated.

If a firmware image is not valid for a system or has a bad/missing signature, iLO rejects the image and the **Flash Status** section shows an error for the affected system.

Some firmware update types might require a system reset, iLO reset, or a server reboot for the new firmware to take effect.

More information

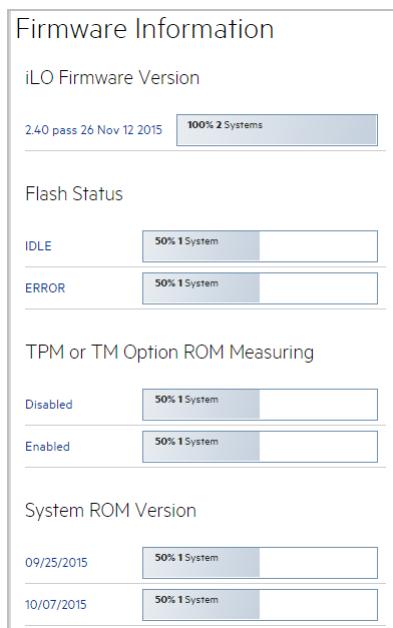
[Obtaining the iLO firmware image file](#)

Obtaining supported server firmware image files

Viewing firmware information

1. Navigate to the **iLO Federation**→**Group Firmware Update** page.
2. Select a group from the **Selected Group** menu.

Firmware details



The **Firmware Information** section displays the following information:

- The number of servers with each supported firmware version. The percentage of the total number of servers with the listed firmware version is also displayed.
- The flash status for the grouped servers. The percentage of the total number of servers with the listed flash status is also displayed.
- The TPM or TM Option ROM Measuring status for the grouped servers. The percentage of the total number of servers with the listed Option ROM Measuring status is also displayed.

Servers affected by a Group Firmware Update

The **Affected Systems** list provides the following details about the servers affected by a firmware update:

- **Server Name**—The server name defined by the host operating system.
- **System ROM**—The installed System ROM (BIOS).
- **iLO Firmware Version**—The installed iLO firmware version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More information

[Exporting iLO Federation information to a CSV file](#)

Using iLO Federation group licensing

The **Group Licensing** page displays the license status for members of a selected iLO Federation group. Use this page to enter an optional key to activate iLO licensed features.

Viewing license information

1. Navigate to the **iLO Federation**→**Group Licensing** page.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of servers, click a license type or status link in the **License Information** section.

iLO Federation group license details



- **Type**—The number of servers with each listed license type. The percentage of the total number of servers with each listed license type is also displayed.
- **Status**—The number of servers with each listed license status. The percentage of the total number of servers with each license status is also displayed. The possible status values follow:
 - **Evaluation**—A valid evaluation license is installed.
 - **Expired**—An expired evaluation license is installed.
 - **Perpetual**—A valid iLO license is installed. This license does not have an expiration date.
 - **Unlicensed**—The factory default (iLO Standard) features are enabled.

Installing license keys (iLO Federation group)

Prerequisites

- Configure iLO Settings privilege
- Each member of the iLO Federation group has granted the Configure iLO Settings privilege to the group.
- The license key is authorized for the number of selected servers.
- The server you want to license is a ProLiant server. For Synergy compute modules, an iLO Advanced license is automatically included, and the **Enter License Activation Key** section is not displayed on the iLO **Licensing** page.

Installing a license key

1. Navigate to the **iLO Federation**→**Group Licensing** page.

2. Optional: To filter the list of affected systems, click a license type or status link. If you install a license key on a server that already has a key installed, the new key replaces the installed key. If you do not want to replace existing licenses, click **Unlicensed** in the **License Information Status** table to install licenses only on servers that are unlicensed.
3. Enter the license key in the **Activation Key** box.
To move the cursor between the segments in the **Activation Key** box, press the **Tab** key or click inside a segment of the box. The cursor advances automatically when you enter data into the segments of the **Activation Key** box.
4. Click **Install**.
The EULA confirmation dialog box opens. The EULA details are available in the License Pack option kit.
5. Click **OK**.
The **License Information** section is updated to show the new license details for the selected group.

Servers affected by a license installation

The **Affected Systems** section provides the following details about the servers that will be affected when you install a license key:

- **Server Name**—The server name defined by the host operating system.
- **License**—The installed license type.
- **iLO Firmware Version**—The installed iLO firmware version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. To open the iLO web interface for the server, click the link in the **iLO Hostname** column.
- **IP Address**—The network IP address of the iLO subsystem. To open the iLO web interface for the server, click the link in the **IP Address** column.

Click **Next** or **Previous** (if available) to view more servers in the list.

More information

[Exporting iLO Federation information to a CSV file](#)

Using the iLO Federation Group Configuration feature

For information about using the features on the **iLO Federation→Group Configuration** page, see [“Adding iLO Federation group memberships \(multiple iLO systems\)” \(page 56\)](#).

18 Using the iLO Remote Consoles

Using the Integrated Remote Console

The iLO Integrated Remote Console is a graphical remote console that can be used to control the display, keyboard, and mouse of the host server. The Integrated Remote Console provides access to the remote file system and network drives.

With Integrated Remote Console access, you can observe POST boot messages as the remote host server restarts, and initiate ROM-based setup activities to configure the remote host server hardware. When you install operating systems remotely, the Integrated Remote Console (if licensed) enables you to view and control the host server monitor throughout the installation process.

Integrated Remote Console access options

- **.NET IRC**—Provides access to the system KVM, allowing control of Virtual Power and Virtual Media from a single console through a supported browser on a Windows client. In addition to the standard features, the .NET IRC supports Console Capture, Shared Console, Virtual Folder, and Scripted Media.
- **Java Web Start and Java Applet**—Provide access to the system KVM, allowing control of Virtual Power and Virtual Media. In addition to the standard features, the Java IRC includes the iLO disk image tool and Scripted Media.
- **Standalone IRC (HPLOCONS)**—Provides full iLO Integrated Remote Console functionality directly from your Windows desktop, without going through the iLO web interface. HPLOCONS has the same functionality and requirements as the .NET IRC application that is launched from the iLO web interface. Download HPLOCONS from the following website: <http://www.hpe.com/support/ilo4>.
- **iLO Mobile Application for iOS and Android devices**—Provides Integrated Remote Console access from your supported mobile phone or tablet. For more information, see <http://www.hpe.com/info/ilo/mobileapp>.

Integrated Remote Console usage information and tips

- Users with the Remote Console privilege can use the .NET IRC and the Java IRC.
- On WS and blade servers, the Integrated Remote Console is always enabled. On nonblade servers, a license must be installed to use the Integrated Remote Console after the OS is started. To determine whether a license is installed, select **Administration**→**Licensing**. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- Previous versions of iLO 4 exclusively used a Java applet for the Java IRC. With iLO 4 2.40 and later, the Java IRC can also be launched as a Java Web Start application.
- When you use Windows or Linux with the Oracle Java Runtime Environment, the Java IRC is a Java Web Start application that is launched from the iLO web interface and runs in a separate window outside of the web browser. At launch, a blank secondary window opens. Do not close this window after the Java IRC loads.
- When you use Linux with the OpenJDK Java Runtime Environment, the Java IRC is a Java applet that is launched from the iLO web interface and runs in a separate window.
- Java IRC with OpenJDK only: When you refresh or close the iLO web interface window, the Remote Console connection is closed. When the Remote Console connection is closed, you lose access to Virtual Media devices that were connected through the Java IRC, except for devices that were connected by using scripted media.
- The Integrated Remote Console is suitable for high-latency (modem) connections.

- Do not run the Integrated Remote Console from the host operating system on the server that contains the iLO processor.
- Hewlett Packard Enterprise recommends that users who log in to a server through the Integrated Remote Console logout before closing the console.
- Pop-up blockers prevent the .NET IRC or Java IRC applet from running, so you must disable them before starting an Integrated Remote Console session. In some cases, you can bypass the pop-up blocker by **Ctrl+clicking** the remote console launch button. This limitation does not apply to the Java IRC Web Start application.
- Google Chrome version 42 and later does not support the Java plug-in. The following alternatives are available:
 - Windows users: Use the Java IRC Java Web Start application.
 - Linux users with Oracle JRE: Use the Java IRC Java Web Start application.
 - Linux users with OpenJDK JRE: Use the Java IRC applet.
- The UID LED blinks when an Integrated Remote Console session is active.
- When you finish using the Integrated Remote Console, close the window or click the browser **Close** button (X) to exit.
- The **Idle Connection Timeout** specifies how long a user can be inactive before an Integrated Remote Console session ends automatically. This value does not affect Integrated Remote Console sessions when a virtual media device is connected.
For more information about the **Idle Connection Timeout**, see “[iLO access settings](#)” (page 61).
- When the mouse is positioned over the Integrated Remote Console window, the console captures all keystrokes, regardless of whether the console window has focus.

.NET IRC requirements

Microsoft .NET Framework

The .NET IRC requires one of the following versions of the .NET Framework:

- .NET Framework 3.5 Full (SP1 recommended)
- .NET Framework 4.0 Full
- .NET Framework 4.5
- .NET Framework 4.6

For Windows 7, 8, 8.1, and 10, a supported version of the .NET Framework is included in the OS. The .NET Framework is also available at the Microsoft Download Center: <http://www.microsoft.com/download>.

The .NET Framework versions 3.5 and 4.0 have two deployment options: Full and Client Profile. The Client Profile is a subset of the Full framework. The .NET IRC is supported with the Full framework only; the Client Profile is not supported. Versions 4.5 and later of the .NET Framework do not have the Client Profile option.

For Internet Explorer users only: The **iLO Integrated Remote Console** page indicates whether a supported version of the .NET Framework is installed. This information is not displayed if Internet Explorer is configured to hide the user agent string.

The Microsoft Edge browser does not display information about the installed .NET Framework version.

Microsoft ClickOnce

The .NET IRC is launched using Microsoft ClickOnce, which is part of the .NET Framework. ClickOnce requires that any application installed from an SSL connection must be from a trusted source. If a browser is not configured to trust an iLO system, and the **IRC requires a trusted certificate in iLO setting** is set to **Enabled**, ClickOnce displays the following error message:

Cannot Start Application - Application download did not succeed...

For more information, see [“Configuring the Integrated Remote Console Trust setting \(.NET IRC\)” \(page 94\)](#).

- Mozilla Firefox requires an add-on to launch .NET applications. You can launch the .NET IRC from a supported version of Firefox by using a ClickOnce add-on such as the Microsoft .NET Framework Assistant. You can download the .NET Framework Assistant from <http://addons.mozilla.org/>.
- Previous versions of Google Chrome could run the .NET IRC with an NPAPI plug-in that supported ClickOnce. Google Chrome 42 and later does not support NPAPI-based plug-ins. As a workaround, use one of the following:
 - The .NET IRC with a different browser.
 - The standalone .NET IRC.
 - The Java IRC.
 - The iLO mobile app.

Starting the Integrated Remote Console

Starting the .NET IRC

1. Navigate to the **Remote Console**→**Remote Console** page.
2. Verify that your system meets the requirements for using the .NET IRC.
For more information, see [“.NET IRC requirements” \(page 216\)](#).
3. Click the **Launch** button.

Starting the Java IRC (Oracle JRE)

Use this procedure to start the Java IRC in environments with Windows or Linux and the Oracle JRE.

1. Navigate to the **Remote Console**→**Remote Console** page.
2. Verify that your system meets the requirements for using the Java IRC.
For more information, see [“Integrated Remote Console usage information and tips”](#)
3. Click the **Web Start** button.
 - Internet Explorer: The browser prompts you to open the Java IRC JNLP file.
 - Firefox: The browser prompts you to save the Java IRC JNLP file.
 - Chrome: The browser downloads the Java IRC JNLP file.
4. Open the JNLP file.
 - Internet Explorer: Click the open prompt.
 - Firefox: Save and open the downloaded JNLP file.
 - Chrome: Open the downloaded JNLP file.

5. If you are prompted to confirm that you want to run the application, click **Run**.
If you do not click **Run**, the Java IRC will not start.
6. If a **Security Warning** dialog box is displayed, click **Continue**.
If you do not click **Continue**, the Java IRC will not start.

Starting the Java IRC (OpenJDK JRE)

Use this procedure to start the Java IRC in environments with Linux and the OpenJDK JRE.

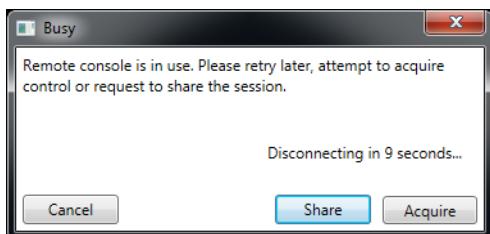
1. Navigate to the **Remote Console**→**Remote Console** page.
2. Verify that your system meets the requirements for using the Java IRC.
For more information, see “[Integrated Remote Console usage information and tips](#)”
3. Click the **Applet** button.
4. If a **Security Warning** dialog box is displayed, click **Yes** to continue.
If you do not click **Yes**, the Java IRC will not start.

Acquiring the Remote Console

If another user is working in the Remote Console, you can acquire it from that user.

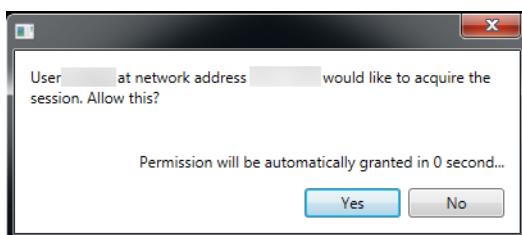
1. Navigate to the **Remote Console**→**Remote Console** page.
2. Click the button for the Remote Console you want to use.

The system notifies you that another user is working in the Remote Console.



3. Click the **Acquire** button.

The other user is prompted to approve or deny permission to acquire the Remote Console.



If there is no response in 10 seconds, permission is granted.

Using the Remote Console power switch

To use the power switch, select one of the following options from the Remote Console **Power Switch** menu:

- **Momentary Press**—The same as pressing the physical power button. If a server is powered off, a momentary press will turn on the server power.
Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. Hewlett Packard Enterprise recommends using

system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.

- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.
The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.
This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.
- **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.
- **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.

NOTE: The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.

More information

[Power-on protection](#)

Using iLO Virtual Media from the Remote Console

For instructions on using the Virtual Media feature from the Remote Console, see “[Remote Console Virtual Media](#)” (page 236).

Shared Remote Console (.NET IRC only)

Shared Remote Console allows the connection of multiple sessions on the same server. This feature can be used for activities such as training and troubleshooting.

The first user to initiate a Remote Console session connects to the server normally and is designated as the session leader. Any subsequent user who requests Remote Console access initiates an access request for a satellite client connection. A dialog box for each access request opens on the session leader desktop, identifying the requester user name and DNS name (if available) or IP address. The session leader can grant or deny access. If there is no response, permission is denied automatically.

Shared Remote Console does not support passing the session leader designation to another user, or reconnecting a user after a failure. Restart the Remote Console session to allow user access after a failure.

During a Shared Remote Console session, the session leader has access to all Remote Console features, whereas all other users can access only the keyboard and mouse. Satellite clients cannot control Virtual Power or Virtual Media.

iLO encrypts Shared Remote Console sessions by authenticating the client first, and then the session leader determines whether to allow new connections.

Joining a Shared Remote Console session

Prerequisites

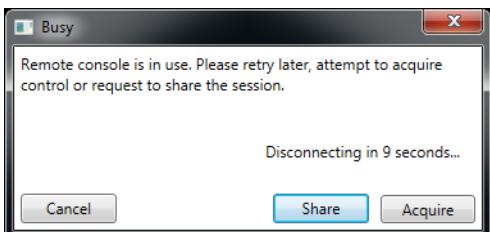
An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Joining a remote console session

1. Navigate to the **Remote Console**→**Remote Console** page.

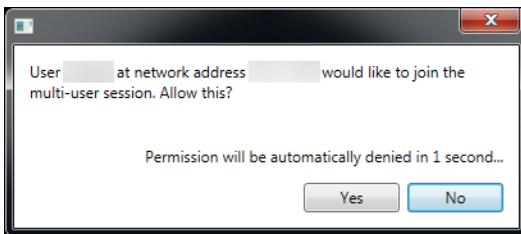
2. Click **Launch**.

A message notifies you that the .NET IRC is already in use.



3. Click **Share**.

The session leader receives your request to join the .NET IRC session.



If the session leader clicks **Yes**, you are granted access to the .NET IRC session with access to the keyboard and mouse.

Console Capture (.NET IRC only)

Console Capture allows you to record and play back video streams of events such as startup, ASR events, and sensed operating system faults. iLO automatically captures the Server Startup and Server Prefailure sequences. You can manually start and stop the recording of console video.

When you are using Console Capture, note the following:

- Console Capture is supported with the .NET IRC; it is not supported with the Java IRC.
- Console Capture is available only through the .NET IRC. It cannot be accessed through XML scripting or the CLP.
- The Server Startup and Server Prefailure sequences are not captured automatically during firmware updates or while the Remote Console is in use.
- Server Startup and Server Prefailure sequences are saved automatically in iLO memory. They will be lost during firmware updates, iLO reset, and power loss. You can save the captured video to your local drive by using the .NET IRC.
- The Server Startup file starts capturing when server startup is detected, and stops when it runs out of space. This file is overwritten each time the server starts.
- The Server Prefailure file starts capturing when the Server Startup file is full, and stops when iLO detects an ASR event. The Server Prefailure file is locked when iLO detects an ASR event. The file is unlocked and can be overwritten after it is downloaded through the .NET IRC.
- The Console Capture control buttons are on the bottom of the .NET IRC session window. The following playback controls are available:
 -  **Skip to Start**—Restarts playback from the beginning of the file.
 -  **Pause**—Pauses the playback.

-  **Play**—Starts playback if the currently selected file is not playing or is paused.
-  **Record**—Records your .NET IRC session.
-  **Progress Bar**—Shows the progress of the video session.

Viewing Server Startup and Server Prefailure sequences

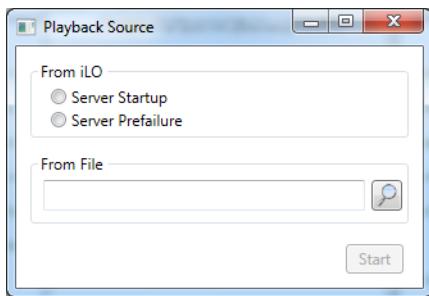
Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Viewing a startup or prefailure sequence

1. Start the .NET IRC.
2. Press the **Play** button.

The **Playback Source** dialog box opens.



3. Select **Server Startup** or **Server Prefailure**.
4. Click **Start**.

Saving Server Startup and Server Prefailure video files

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Saving a captured video file

1. Start the .NET IRC
2. Press the **Play** button.
3. Select **Server Startup** or **Server Prefailure**.
4. Click **Start**.
5. Press the **Play** button again to stop playback.

Capturing video files

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Capturing a video file

To capture video files of sequences other than Server Startup and Server Prefailure:

1. Start the .NET IRC.
2. Click the **Record** button.

3. The **Save Video** dialog box opens.
4. Enter a file name and save location, and then click **Save**.
5. When you are finished recording, press the **Record** button again to stop recording.

Viewing saved video files

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Viewing a saved video file

1. Start the .NET IRC.
2. Press the **Play** button.

The **Playback Source** dialog box opens.

3. Click the magnifying glass icon next to the **From File** box.
4. Navigate to a video file, and then click **Open**.

Video files captured in the Remote Console use the iLO file type.

5. Click **Start**.

Remote Console hot keys

The **Program Remote Console Hot Keys** page allows you to define up to six hot keys to use during Remote Console sessions. Each hot key represents a combination of up to five keys that are sent to the host server when the hot key is pressed. Hot keys are active during Remote Console sessions that use the .NET IRC, Java IRC, and the text-based Remote Console.

If a hot key is not set—for example, **Ctrl+V** is set to **NONE, NONE, NONE, NONE, NONE**—this hot key is disabled. The server operating system will interpret **Ctrl+V** as it usually does (paste, in this example). If you set **Ctrl+V** to use another combination of keys, the server operating system will use the key combination set in iLO (losing the paste functionality).

Example 1: If you want to send **Alt+F4** to the remote server, but pressing that key combination closes your browser, you can configure the hot key **Ctrl+X** to send the **Alt+F4** key combination to the remote server. After you configure the hot key, press **Ctrl+X** in the Remote Console window when you want to send **Alt+F4** to the remote server.

Example 2: If you want to create a hot key to send the international **AltGR** key to the remote server, use **R_ALT** in the key list.

Creating hot keys

Prerequisites

Configure iLO Settings privilege

Creating a hot key

1. Navigate to the **Remote Console→Hot Keys** page.
2. For each hot key that you want to create, select the key combination to send to the remote server.

To configure hot keys to generate key sequences from international keyboards, select the key on a U.S. keyboard that is in the same position as the desired key on the international keyboard. [Table 6 \(page 223\)](#) lists the keys you can use when you configure hot keys.

3. Click **Save Hot Keys**.

iLO confirms that the hot key settings were updated successfully.

Keys for configuring Remote Console hot keys

Table 6 Keys for configuring hot keys

ESC	SCRL LCK	1	g
L_ALT	SYS RQ	2	h
R_ALT	F1	3	i
L_SHIFT	F2	4	j
R_SHIFT	F3	5	k
L_CTRL	F4	6	l
R_CTRL	F5	7	m
L_GUI	F6	8	n
R_GUI	F7	9	o
INS	F8	;	p
DEL	F9	=	q
HOME	F10	[r
END	F11	\	s
PG UP	F12]	t
PG DN	SPACE	'	u
ENTER	'	a	v
TAB	,	b	w
BREAK	-	c	x
BACKSPACE	.	d	y
NUM PLUS	/	e	z
NUM MINUS	0	f	

Resetting hot keys

Prerequisites

Configure iLO Settings privilege

Clearing all hot key assignments

Resetting the hot keys clears all current hot key assignments.

1. Navigate to the **Remote Console**→**Hot Keys** page.
2. Click **Reset Hot Keys**.
iLO prompts you to confirm the request.
3. Click **OK**.
iLO notifies you that the hot keys were reset.

Viewing configured remote console hot keys (Java IRC only)

1. Start the Java IRC.
2. Select **Keyboard**→**View Hot Keys**.

Using a text-based Remote Console

iLO supports a true text-based Remote Console. Video information is obtained from the server, and the contents of the video memory are sent to the iLO management processor, compressed, encrypted, and forwarded to the management client application. iLO uses a screen-frame buffer that sends the characters (including screen positioning information) to text-based client applications. This method ensures compatibility with standard text-based clients, good performance, and simplicity. However, you cannot display non-ASCII or graphical information, and screen positioning information (displayed characters) might be sent out of order.

iLO uses the video adapter DVO port to access video memory directly. This method increases iLO performance significantly. However, the digital video stream does not contain useful text data, and text-based client applications such as SSH cannot render this data.

There are two text-based console options, as described in the following sections:

- [“Using the iLO Virtual Serial Port” \(page 224\)](#)
- [“Text-based Remote Console \(Textcons\)” \(page 228\)](#)

Using the iLO Virtual Serial Port

You can access a text-based console from iLO using a standard license and the iLO Virtual Serial Port.

The iLO Virtual Serial Port is one type of iLO text-based remote console. The iLO Virtual Serial Port gives you a bidirectional data flow with a server serial port. Using the remote console, you can operate as if a physical serial connection exists on the remote server serial port.

The iLO Virtual Serial Port is displayed as a text-based console, but the information is rendered through graphical video data. iLO displays this information through an SSH client when the server is in a pre-operating-system state, enabling a nonlicensed iLO system to observe and interact with the server during POST.

By using the iLO Virtual Serial Port, the remote user can perform operations such as the following:

- Interact with the server POST sequence and the operating system boot sequence.

① **IMPORTANT:** To start iLO RBSU during a Virtual Serial Port session, enter the key combination **ESC+8**.

To start the UEFI System Utilities during a Virtual Serial Port session, enter the key combination **ESC+9**.

- Establish a login session with the operating system, interact with the operating system; and execute and interact with applications on the operating system.
- For an iLO system running Linux in a graphical format, you can configure `getty()` on the server serial port, and then use the iLO Virtual Serial Port to view a login session to the Linux OS. For more information, see [“Configuring the iLO Virtual Serial Port for Linux” \(page 226\)](#).
- Use the EMS Console through the iLO Virtual Serial Port. EMS is useful for debugging Windows boot issues and kernel-level issues. For more information, see [“Windows EMS Console with iLO Virtual Serial Port” \(page 227\)](#).

Configuring the iLO Virtual Serial Port in the host system RBSU

The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

This procedure is for systems that support the legacy system RBSU. For systems that support the UEFI System Utilities, see [“Configuring the iLO Virtual Serial Port in the UEFI System Utilities” \(page 225\)](#).

1. Optional: If you access the server remotely, start an iLO remote console session.

2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The system RBSU starts.
4. Set the Virtual Serial Port COM port.
 - a. Select **System Options**, and then press **Enter**.
 - b. Select **Serial Port Options**, and then press **Enter**.
 - c. Select **Virtual Serial Port**, and then press **Enter**.
 - d. Select the COM port you want to use, and then press **Enter**.
 - e. Press **ESC** twice to return to the main menu.
5. Set the BIOS serial console port COM port.
 - a. Select **BIOS Serial Console & EMS**, and then press **Enter**.
 - b. Select **BIOS Serial Console Port**, and then press **Enter**.
 - c. Select the COM port that matches the value selected in [step 4](#), and then press **Enter**.
6. Set the **BIOS Serial Console Baud Rate**.
 - a. Select **BIOS Serial Console Baud Rate**, and then press **Enter**.
 - b. Select **115200**, and then press **Enter**.

NOTE: The iLO Virtual Serial Port does not use a physical UART, so the **BIOS Serial Console Baud Rate** value has no effect on the speed the iLO Virtual Serial Port uses to send and receive data.

7. Set the EMS Console COM port.

EMS is for Windows only.

- a. Select **EMS Console**, and then press **Enter**.
- b. Select the COM port that matches the value selected in [step 4](#), and then press **Enter**.

8. Exit the system RBSU.

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

This procedure is for systems that support the UEFI System Utilities. For systems that support the legacy system RBSU, see [“Configuring the iLO Virtual Serial Port in the host system RBSU” \(page 224\)](#).

1. Access the UEFI system utilities.
 - a. Optional: If you access the server remotely, start an iLO remote console session.
 - b. Restart or power on the server.
 - c. Press **F9** in the server POST screen.
The UEFI System Utilities start.
2. Set the Virtual Serial Port COM port.
 - a. From the **System Configuration** screen, use the up or down arrow keys and the **Enter** key to navigate to the **BIOS/Platform configuration (RBSU)→System Options→Serial Port Options** screen.
 - b. Select **Virtual Serial Port**, and then press **Enter**.
 - c. Select the COM port you want to use, and then press **Enter**.
 - d. Press **ESC** twice to return to the main menu.
3. Set the BIOS serial console port COM port.
 - a. Select **BIOS Serial Console and EMS**, and then press **Enter**.
 - b. Select **BIOS Serial Console Port**, and then press **Enter**.

- c. Select the Virtual Serial Port, and then press **Enter**.
- d. Press **ESC**.

The main menu is displayed.

4. Set the **BIOS Serial Console Baud Rate**.

- a. Select **BIOS Serial Console Baud Rate**, and then press **Enter**.
- b. Select **115200**, and then press **Enter**.

NOTE: The iLO Virtual Serial Port does not use a physical UART, so the **BIOS Serial Console Baud Rate** value has no effect on the speed the iLO Virtual Serial Port uses to send and receive data.

- c. Press **ESC**.

The main menu is displayed.

5. Set the EMS Console COM port.

EMS is for Windows only.

- a. Select **EMS Console**, and then press **Enter**.
- b. Select the COM port that matches the value selected in [step 2](#), and then press **Enter**.
- c. Press **F10** to save the changes.

6. Resume the boot process.

- a. Press **Esc** until the main menu is displayed.

- b. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.

- c. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

Configuring the iLO Virtual Serial Port for Linux

You can manage Linux servers remotely using console redirection. To configure Linux to use console redirection, you must configure the Linux boot loader (GRUB). The boot-loader application loads from the bootable device when the server system ROM finishes POST. Define the serial interface (ttyS0) as the default interface so that if no input arrives from the local keyboard within 10 seconds (the default timeout value), the system will redirect output to the serial interface (iLO Virtual Serial Port).

NOTE: ttyS0 and unit 0 are for com1 and ttyS1 and unit 1 are for com2.

The following configuration example uses Red Hat Enterprise Linux 6 and com1:

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
title Red Hat Linux (2. 6.18-164.e15)
root (hd0,2)
9
kernel /vmlinuz-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS0,115200
initrd /initrd-2.6.18-164.e15.img
```

If com2 was selected, the configuration example would be as follows:

```
serial -unit=1 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
title Red Hat Linux (2. 6.18-164.e15)
root (hd0,2)
9
kernel /vmlinuz-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS1,115200
initrd /initrd-2.6.18-164.e15.img
```

After Linux is fully booted, a login console can be redirected to the serial port.

- If configured, the `/dev/ttys0` and `/dev/ttys1` devices enable you to obtain serial TTY sessions through the iLO Virtual Serial Port. To begin a shell session on a configured serial port, add the following line to the `/etc/inittab` file to start the login process automatically during system boot.
The following example initiates the login console on `/dev/ttys0`:
`S0:2345:respawn:/sbin/agetty 115200 ttys0 vt100`
The following example initiates the login console on `dev/ttys1`:
`S1:2345:respawn:/sbin/agetty 115200 ttys1 vt100`
- Use SSH to connect to iLO, and then use the iLO CLP command `start /system1/oemhp_vsp1` to view a login session to the Linux operating system.

Windows EMS Console with iLO Virtual Serial Port

iLO enables you to use the Windows EMS Console over the network through a web browser. EMS enables you to perform emergency management services when video, device drivers, or other OS features prevent normal operation and normal corrective actions from being performed.

When using the Windows EMS Console with iLO:

- You must configure the Windows EMS console in the OS before you can use the iLO Virtual Serial Port. For information about how to enable the EMS console, see your OS documentation. If the EMS console is not enabled in the OS, iLO displays an error message when you try to access the iLO Virtual Serial Port.
- The Windows EMS serial port must be enabled through the host system RBSU or the UEFI System Utilities. The configuration options allow you to enable or disable the EMS port, and select the COM port. iLO automatically detects whether the EMS port is enabled or disabled, and detects the selection of the COM port.
- You can use the Windows EMS Console and the iLO Remote Console at the same time.
- To display the `SAC>` prompt, you might have to press **Enter** after connecting through the iLO Virtual Serial Port.

More information

[Configuring the iLO Virtual Serial Port in the host system RBSU](#)

[Configuring the iLO Virtual Serial Port in the UEFI System Utilities](#)

Configuring Windows for use with the iLO Virtual Serial Port

1. Open a command window.
2. Enter the following command to edit the boot configuration data:
`bcdedit /ems on`
3. Enter the following command to configure the EMSPORT and EMSBAUDRATE values:
`bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200`

NOTE: EMSPORT:1 is COM1, and EMSPORT:2 is COM2.

Enter `bcdedit /?` for syntax help.

4. Reboot the operating system.

Starting an iLO Virtual Serial Port session

1. Verify that the iLO Virtual Serial Port settings are configured in the iLO RBSU or UEFI System Utilities.
For more information, see “[Configuring the iLO Virtual Serial Port in the host system RBSU](#)” (page 224) or “[Configuring the iLO Virtual Serial Port in the UEFI System Utilities](#)” (page 225).
2. Verify that the Windows or Linux operating system is configured for use with the iLO Virtual Serial Port.
For more information, see “[Windows EMS Console with iLO Virtual Serial Port](#)” (page 227) or “[Configuring the iLO Virtual Serial Port for Linux](#)” (page 226).
3. Start an SSH session.
For example, you could enter `ssh Administrator@<iLO IP address>` or connect through port 22 with `putty.exe`.
4. When prompted, enter your iLO account credentials.
5. At the `</>hpilo->` prompt, enter `vsp`, and press **Enter**.
6. For Windows systems only: At the `<SAC>` prompt, enter `cmd` to create a command prompt channel.
7. For Windows systems only: Enter `ch - si <#>` to switch to the channel specified by the channel number.
8. When prompted, enter the OS login credentials.

Viewing the iLO Virtual Serial Port log

If the iLO Virtual Serial Port log is enabled, you can view iLO Virtual Serial Port activity by using the `vsp log` command.

Virtual Serial Port activity is logged to a 150-page circular buffer in the iLO memory, and can be viewed using the CLI command `vsp log`. The Virtual Serial Port buffer size is 128 KB.

1. Verify that an iLO Advanced or iLO Scale-Out license is installed.
2. Enable **Secure Shell (SSH) Access** and **Virtual Serial Port Log** on the **Access Settings** page.
For instructions, see “[iLO access settings](#)” (page 61).
3. Connect to the CLI through SSH.
4. Use the `vsp` command to view iLO Virtual Serial Port activity.
5. Enter `ESC (` to exit.
6. Enter `vsp log` to view the iLO Virtual Serial Port log.

Text-based Remote Console (Textcons)

You can access the Text-based Remote Console (Textcons) using a licensed iLO system and SSH. When you use SSH, the data stream, including authentication credentials, is protected by the encryption method that the SSH client and iLO use.

This feature is supported only on servers that are configured to use the Legacy BIOS boot mode. It is not supported on servers that are configured to use UEFI mode. For more information, see “[Virtual Media Boot Order](#)” (page 241).

For more information about iLO licensing, see the following website: <http://www.hpe.com/info/ilo/licensing>.

When you use Textcons, the presentation of colors, characters, and screen controls depends on the client you are using, which can be any standard SSH client compatible with iLO. Features and support include the following:

- Display of text-mode screens that are 80x25 (standard color configurations), including:
 - System boot process (POST)
 - Standard option ROMs
 - Text boot loaders (boot loaders without a frame buffer)
 - Linux operating system in VGA 80x25 mode
 - DOS
 - Other text-based operating systems
- International language keyboards (if the server and client systems have a similar configuration)
- Line-drawing characters when the correct font and code page are selected in the client application

Customizing the Text-based Remote Console

You can use the `textcons` command options and arguments to customize the Text-based Remote Console display. In general, you do not need to change these options.

- **To control the sampling rate:**

Use the `textcons speed` option to indicate, in ms, the time between each sampling period. A sampling period is when the iLO firmware examines screen changes and updates the Text-based Remote Console. Adjusting the speed can alleviate unnecessary traffic on long or slow network links, reduce bandwidth use, and reduce iLO CPU time. Hewlett Packard Enterprise recommends that you specify a value between 1 and 5,000 (1 ms to 5 seconds). For example:

```
textcons speed 500
```

- **To control smoothing:**

iLO attempts to transmit data only when it changes and becomes stable on the screen. If a line of the text screen is changing faster than iLO can sample the change, the line is not transmitted until it becomes stable.

When a Text-based Remote Console session is active, the data is displayed rapidly and is indecipherable. If iLO transmits this indecipherable data across the network, it consumes bandwidth. The default behavior is smoothing (`delay 0`), which transmits data only when the changes become stable on the screen. You can control or disable smoothing by using the `delay` option. For example:

```
textcons speed 500 delay 10
```

- **To configure character mapping:**

In the ASCII character set, CONTROL characters (ASCII characters less than 32) are not printable and are not displayed. These characters can be used to represent items such as arrows, stars, or circles. Some of the characters are mapped to equivalent ASCII representations. [Table 7 \(page 230\)](#) lists the supported equivalents.

Table 7 Character equivalents

Character value	Description	Mapped equivalent
0x07	Small dot	.
0x0F	Sun	○
0x10	Right pointer	>
0x11	Left pointer	<
0x18	Up arrow	^
0x19	Down arrow	v
0x1A	Left arrow	<
0x1B	Right arrow	>
0x1E	Up pointer	^
0x1F	Down pointer	v
0xFF	Shaded block	Blank space

Using the Text-based Remote Console

1. Use SSH to connect to iLO.

Make sure that the terminal application character encoding is set to **Western (ISO-8859-1)**.

2. Log in to iLO.
3. At the prompt, enter `textcons`.

A message appears, indicating that the Text-based Remote Console is initiating.

To exit the Text-based Remote Console and return to the CLI session, press **Esc+Shift+9**.

Using Linux with the Text-based Remote Console

You can run the Text-based Remote Console on a Linux system that is configured to present a terminal session on the serial port. This feature enables you to use a remote logging service. You can log on to the serial port remotely and redirect output to a log file. Any system messages directed to the serial port are logged remotely.

Some keyboard combinations that Linux requires in text mode might not be passed to the Text-based Remote Console. For example, the client might intercept the **Alt+Tab** keyboard combination.

19 Using iLO Virtual Media

iLO Virtual Media

iLO Virtual Media provides a virtual device that can be used to boot a remote host server from standard media anywhere on the network. Virtual Media devices are available when the host system is booting. Virtual Media devices connect to the host server by using USB technology.

When you use Virtual Media, note the following:

- An iLO license key is required to use some forms of Virtual Media. For information about iLO licensing, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- You must have the Virtual Media privilege to use this feature.
- Only one of each type of virtual media can be connected at a time.
- The Virtual Media feature supports ISO images of up to 8 TB. The maximum ISO image file size also depends on factors such as the single file size limit for the file system where the ISO image is stored and the SCSI commands the server OS supports.
- In an operating system, an iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM behaves like any other drive. When you use iLO for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.
- When virtual devices are connected, they are available to the host server until you disconnect them. When you are finished using a Virtual Media device and you disconnect it, you might receive an “unsafe device removal” warning message from the host OS. You can avoid this warning by using the operating system feature to stop the device before disconnecting it.
- The iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM is available at server boot time for supported operating systems. Booting from a Virtual Floppy/USB key or Virtual CD/DVD-ROM enables you to perform tasks such as deploying an operating system from network drives and performing disaster recovery of failed operating systems.

NOTE: Using the iLO Virtual Floppy to boot a remote host server is supported only on ProLiant Gen8 servers. It is not supported on ProLiant Gen9 servers or Synergy compute modules.

- If the host server OS supports USB mass storage devices or secure digital devices, the iLO Virtual Floppy/USB key is available after the host server OS loads.
 - You can use the Virtual Floppy/USB key when the host server OS is running to upgrade drivers, create an emergency repair disk, and perform other tasks.
 - Having the Virtual Floppy/USB key available when the server is running can be useful if you must diagnose and repair the NIC driver.
 - The Virtual Floppy/USB key can be the physical floppy disk, USB key, or secure digital drive on which the web browser is running, or an image file stored on a local hard drive or network drive.
 - For optimal performance, Hewlett Packard Enterprise recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

- If the host server operating system supports USB mass storage devices, the iLO Virtual CD/DVD-ROM is available after the host server operating system loads.
 - You can use the Virtual CD/DVD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks.
 - Having the Virtual CD/DVD-ROM available when the server is running can be useful if you must diagnose and repair the NIC driver.
 - The Virtual CD/DVD-ROM can be the physical CD/DVD-ROM drive on which the web browser is running, or an image file stored on your local hard drive or network drive.
 - For optimal performance, Hewlett Packard Enterprise recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.
- You can use the .NET IRC to mount a Virtual Folder to access and copy files between a client and a managed server.
- Before you use the Virtual Media feature, review the operating system considerations in [“Virtual Media operating system information” \(page 232\)](#).
- You can also access the Virtual Media feature by using the .NET IRC or Java IRC, XML configuration and control scripts, the iLO RESTful API, or the SMASH CLP.
- If the Virtual Floppy/USB key or Virtual CD/DVD-ROM capability is enabled, you cannot typically access the floppy drive or CD/DVD-ROM drive from the client operating system.

△ **CAUTION:** To prevent file and data corruption, do not try to access the local media when you are using it as an iLO Virtual Media device.

Virtual Media operating system information

This section describes the operating system requirements to consider when you are using the iLO Virtual Media features.

Operating system USB requirement

To use Virtual Media devices, your operating system must support USB devices, including USB mass storage devices. For more information, see your operating system documentation.

During system boot, the ROM BIOS provides USB support until the operating system loads. Because MS-DOS uses the BIOS to communicate with storage devices, utility diskettes that boot DOS will also function with Virtual Media.

Configuring Windows 7 for use with iLO Virtual Media with Windows 7

By default, Windows 7 powers off the iLO virtual hub when no Virtual Media devices are enabled or connected during boot.

To change this setting, use the following procedure:

1. Open **Device Manager**.
2. Select **View→Devices by connection**.
3. Expand **Standard Universal PCI to USB Host Controller** to display the USB devices, including the Generic USB Hub.

The Generic USB Hub option is the iLO virtual USB hub controller.

4. Right-click **Generic USB Hub** and select **Properties**.
5. Click the **Power Management** tab.
6. Clear the **Allow the computer to turn off this device to save power** check box.

Operating system considerations: Virtual Floppy/USB key

- **Boot process and DOS sessions**—During the boot process and DOS sessions, the virtual floppy device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and a virtual floppy drive simultaneously.
- **Windows Server 2008 or later**—Virtual Floppy/USB key drives appear automatically after Windows recognizes the USB device. Use the virtual device as you would use a locally attached device.

To use a Virtual Floppy as a driver diskette during a Windows installation, disable the integrated diskette drive in the host RBSU, which forces the virtual floppy disk to appear as drive A.

To use a virtual USB key as a driver diskette during a Windows installation, change the boot order of the USB key drive. Hewlett Packard Enterprise recommends placing the USB key drive first in the boot order.
- **Windows Vista**—Virtual Media does not work correctly on Windows Vista when you use Internet Explorer 7 with Protected Mode enabled. If you attempt to use Virtual Media with Protected Mode enabled, various error messages appear. To use Virtual Media, select **Tools**→**Internet Options**→**Security**, clear **Enable Protected Mode**, and then click **Apply**. After you disable Protected Mode, close all open browser instances and restart the browser.
- **Red Hat Enterprise Linux and SUSE Linux Enterprise Server**—Linux supports the use of USB diskette and key drives.

Changing diskettes

When you are using a Virtual Floppy/USB key on a client machine with a physical USB disk drive, disk-change operations are not recognized. For example, if a directory listing is obtained from a floppy disk, and then the disk is changed, a subsequent directory listing shows the directory listing for the first disk. If disk changes are necessary when you are using a Virtual Floppy/USB key, make sure that the client machine contains a non-USB disk drive.

Operating system considerations: Virtual CD/DVD-ROM

- **MS-DOS**—The Virtual CD/DVD-ROM is not supported in MS-DOS.
- **Windows**—The Virtual CD/DVD-ROM appears automatically after Windows recognizes the mounting of the device. Use it as you would use a locally attached CD/DVD-ROM device.
- **Linux**—The requirements for Red Hat Enterprise Linux and SUSE Linux Enterprise Server follow:
 - **Red Hat Enterprise Linux**

On servers that have a locally attached CD/DVD-ROM, the Virtual CD/DVD-ROM device is accessible at `/dev/cdrom1`. However, on servers that do not have a locally attached CD/DVD-ROM, such as BL c-Class blade systems, the Virtual CD/DVD-ROM is the first CD/DVD-ROM accessible at `/dev/cdrom`.

You can mount the Virtual CD/DVD-ROM as a normal CD/DVD-ROM device by using the following command:

```
mount /mnt/cdrom1
```

- **SUSE Linux Enterprise Server**

The Virtual CD/DVD-ROM can be found at `/dev/scd0`, unless a USB-connected local CD/DVD-ROM is present. In that case, the Virtual CD/DVD-ROM uses `/dev/scd1`.

You can mount the Virtual CD/DVD-ROM as a normal CD/DVD-ROM device by using the following command:

```
mount /dev/scd0 /media/cdrom1
```

For instructions, see [“Mounting a USB Virtual Media CD/DVD-ROM on Linux systems” \(page 234\)](#).

Mounting a USB Virtual Media CD/DVD-ROM on Linux systems

1. Log in to iLO through the web interface.
2. Start the .NET IRC or Java IRC.
3. Select the **Virtual Drives** menu.
4. Select the CD/DVD-ROM to use.
5. Mount the drive by using the following commands:

For Red Hat Enterprise Linux:

```
mount /dev/cdrom1 /mnt/cdrom1
```

For SUSE Linux Enterprise Server:

```
mount /dev/scd0 /media/cdrom1
```

Operating system considerations: Virtual Folder

- **Boot process and DOS sessions**—The Virtual Folder device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and the Virtual Folder simultaneously.
- **Windows**—A Virtual Folder appears automatically after Windows recognizes the mounting of the virtual USB device. You can use the folder the same way that you use a locally attached device. Virtual Folders are nonbootable. Attempting to boot from the Virtual Folder might prevent the server from starting.
- **Red Hat Enterprise Linux and SUSE Linux Enterprise Server**—Linux supports the use of the Virtual Folder feature, which uses a FAT 16 file system format.

Using Virtual Media from the iLO web interface

The **Virtual Media** page allows you to perform the following tasks:

- View or change the Virtual Media port.
You can also change this value on the **Administration**→**Access Settings** page.
- View or eject local media, including locally stored image files, floppy disks, USB keys, CDs/DVD-ROMs, and virtual folders.
For information about connecting local media devices, see [“Remote Console Virtual Media” \(page 236\)](#).
- View, connect, eject, or boot from scripted media. Scripted media refers to connecting images hosted on a web server by using a URL. iLO will accept URLs in HTTP or HTTPS format. FTP is not supported.

Viewing and modifying the Virtual Media port

The Virtual Media port is the port that iLO uses to listen for incoming local Virtual Media connections. The default value is 17988.

Prerequisites

Configure iLO Settings privilege

Changing the Virtual Media port

1. Navigate to the **Virtual Media**→**Virtual Media** page.
2. Enter a new port number in the **Virtual Media Port** box.
3. Click **Change Port**.
The system prompts you to reset iLO.
4. Click **OK**.

Viewing local media

To view the connected local media devices, navigate to the **Virtual Media**→**Virtual Media** page.

Local media details

When local Virtual Media is connected, the details are listed in the following sections:

- **Virtual Floppy/USB Key/Virtual Folder Status**
 - **Media Inserted**—The Virtual Media type that is connected. **Local Media** is displayed when local media is connected.
 - **Connected**—Indicates whether a Virtual Media device is connected.
- **Virtual CD/DVD-ROM Status**
 - **Media Inserted**—The Virtual Media type that is connected. **Local Media** is displayed when local media is connected.
 - **Connected**—Indicates whether a Virtual Media device is connected.

Ejecting a local media device

1. Navigate to the **Virtual Media**→**Virtual Media** page.
2. Click the **Force Eject Media** button in the **Virtual Floppy/USB Key/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section.

Connecting scripted media

You can connect scripted media from the **Virtual Media** page. Use the .NET IRC or Java IRC, RIBCL/XML, or the iLO CLI to connect other types of Virtual Media. The **Virtual Media** page supports the connection of 1.44 MB floppy images (IMG) and CD/DVD-ROM images (ISO). The image must be on a web server on the same network as iLO.

1. Navigate to the **Virtual Media**→**Virtual Media** page.
2. Enter the URL for the scripted media in the **Scripted Media URL** box in the **Connect Virtual Floppy** (IMG files) or **Connect CD/DVD-ROM** section (ISO files).
3. On ProLiant Gen8 servers only: Select the **Boot on Next Reset** check box if you want the server to boot to this image only on the next server reboot.

The image will be ejected automatically on the second server reboot so that the server does not boot to this image twice.

If this check box is not selected, the image remains connected until it is manually ejected, and the server boots to it on all subsequent server resets, if the system boot options are configured accordingly.

NOTE: An error occurs if you try to enable the **Boot on Next Reset** check box when the server is in POST because you cannot modify the boot order during POST. Wait for POST to finish, and then try again.

NOTE: Using the iLO Virtual Floppy to boot a remote host server is supported only on ProLiant Gen8 servers. It is not supported on ProLiant Gen9 servers or Synergy compute modules.

4. Click **Insert Media**.
5. Optional: To boot to the connected image now, click **Server Reset** to initiate a server reset.

Viewing connected scripted media

Navigate to the **Virtual Media**→**Virtual Media** page.

Scripted media details

When scripted Virtual Media is connected, the details are listed in the **Virtual Floppy/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section:

- **Media Inserted**—The Virtual Media type that is connected. **Scripted Media** is displayed when scripted media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.
- **Image URL**—The URL that points to the connected scripted media.

Ejecting scripted media

1. Navigate to the **Virtual Media**→**Virtual Media** page.
2. To eject scripted media devices, click the **Force Eject Media** button in the **Virtual Floppy/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section.

NOTE: For server blades without an iLO license that grants full Virtual Media privileges, you cannot use the **Force Eject Media** option with a virtual media image that was mounted via URL. In this case, the connection is most likely the Onboard Administrator DVD Drive. This connection must be disconnected through the Onboard Administrator software. An iLO reset will also close the connection.

Remote Console Virtual Media

You can access Virtual Media on a host server by using the Remote Console, the iLO web interface, XML configuration and control scripts, the iLO RESTful API, and the CLP. This section describes how to use the Virtual Media feature with the .NET IRC or Java IRC.

Virtual Drives

The Virtual Drive feature supports the use of a physical floppy disk or CD/DVD-ROM, a USB key drive, an image file, or an image file through a URL.

Using a physical drive on a client PC

1. Start the .NET IRC or Java IRC.
2. Click the **Virtual Drives** menu, and then select the drive letter of a floppy disk, CD/DVD-ROM, or USB key drive on your client PC.

The virtual drive activity LED will show virtual drive activity.

NOTE: When you use the Remote Console with a version of the Windows operating system, you must have Windows administrator rights to mount a physical drive.

Using an image file

1. Start the .NET IRC or Java IRC.
2. Click the **Virtual Drives** menu, and then select **Image File Removable Media (.img files)** or **Image File CD-ROM/DVD (.iso files)**.
The .NET IRC or Java IRC prompts you to select a disk image.
3. Enter the path or file name of the image file in the **File name** text box, or browse to the image file location, and then click **Open**.
The virtual drive activity LED will show virtual drive activity.

Using an image file through a URL (IIS/Apache)

You can connect scripted media by using the .NET IRC or Java IRC. Scripted media supports only 1.44 MB floppy disk images (.img) and CD/DVD-ROM images (.iso). The image must be on a web server on the same network as iLO.

1. Start the .NET IRC or Java IRC.
2. Depending on the image type you will use, select **Virtual Drives**→**URL Removable Media (.img)** or **Virtual Drives**→**URL CD-ROM/DVD (.iso)**.
The **Image file at URL** dialog box opens.
3. Enter the URL for the image file that you want to mount as a virtual drive, and then click **Connect**.
The virtual drive activity LED does not show drive activity for URL-mounted virtual media.

Using the Create Media Image feature (Java IRC only)

When you use Virtual Media, performance is fastest when image files are used instead of physical disks. You can use industry-standard tools like DD to create image files or to copy data from a disk image file to a physical disk. You can also use the Java IRC to perform these tasks.

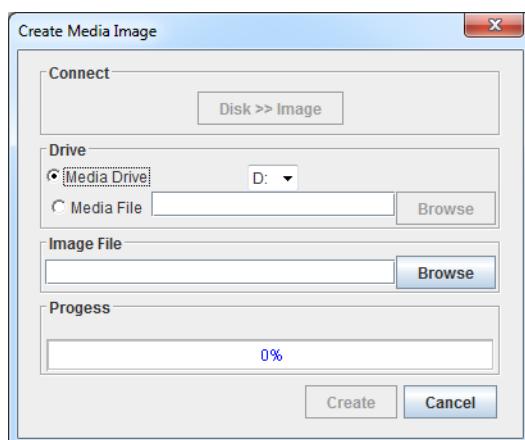
Creating a disk image file

The Create Media Image feature enables you to create disk image files from data in a file or on a physical disk.

To create an ISO-9660 disk image file (.img or .iso):

1. Start the Java IRC.
2. Select **Virtual Drives**→**Create Disk Image**.

The **Create Media Image** dialog box opens.



3. Verify that the **Disk>>Image** button is displayed. If the button label is **Image>>Disk**, click the button to change it to **Disk>>Image**.

4. Do one of the following:
 - If you will use a file, select the **Media File** option, and then click **Browse** and navigate to the file you want to use.
 - If you will use physical media, select the drive letter of the floppy disk, USB key, or CD-ROM in the **Media Drive** menu.
5. Enter the path and file name for the image file in the **Image File** text box.
6. Click **Create**.
iLO notifies you when the image creation is complete.
7. Click **Close**.
8. Confirm that the image was created in the specified location.

Copying data from an image file to a physical disk

The Create Media Image feature enables you to copy the data from a disk image file to a floppy disk or USB key. Only IMG disk image files are supported. Copying data to a CD-ROM is not supported.

To copy disk image data to a floppy disk or USB key:

1. Start the Java IRC.
2. Select **Virtual Drives** → **Create Disk Image**.
The dialog box opens.
3. In the **Create Media Image** window, click **Disk>>Image**.
The **Create Media Image** changes to the **Image>>Disk** option.
4. Select the drive letter of the floppy disk or USB key in the **Media Drive** menu.
5. Enter the path and file name for the existing image file in the **Image File** text box.
iLO notifies you when the disk creation is complete.
6. Click **Close**.
7. Confirm that the files were copied to the specified location.

Using a Virtual Folder (.NET IRC only)

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Using a Virtual Folder

1. Start the .NET IRC.
2. Select **Virtual Drives** → **Folder**.
3. In the **Browse For Folder** window, select the folder you want to use, and then click **OK**.
The Virtual Folder is mounted on the server with the name **iLO Folder**.

Virtual folders

Virtual folders enable you to access, browse to, and transfer files from a client to a managed server. You can mount and dismount a local or networked directory that is accessible through the client. After you create a virtual image of a folder or directory, the server connects to the image as a USB storage device, enabling you to browse to the server and transfer the files from the virtual image to the server.

This feature and many others are part of a licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

The Virtual Folder is nonbootable and read-only; the mounted folder is static. Changes to the client folder are not replicated in the mounted folder.

Setting up IIS for scripted Virtual Media

Before you set up IIS for scripted Virtual Media, verify that IIS is operational. Use IIS to set up a simple website, and then browse to the site to verify that it is working correctly.

Configuring IIS

To configure IIS to serve diskette or ISO-9660 CD images for read-only access:

1. Add a directory to your website and place your images in the directory.
2. Verify that IIS can access the MIME type for the files you are serving.

For example, if your diskette image files use the extension `.img`, you must add a MIME type for that extension. Use the IIS Manager to access the **Properties** dialog box of your website. On the **HTTP Headers** tab, click **MIME Types** to add MIME types.

Hewlett Packard Enterprise recommends adding the following types:

`.img application/octet-stream`
`.iso application/octet-stream`

3. Verify that the web server is configured to serve read-only disk images.
 - a. Use a web browser to navigate to the location of your disk images.
 - b. Download the disk images to a client.

If these steps complete successfully, the web server is configured correctly.

Configuring IIS for read/write access

1. Install Perl (for example, ActivePerl).
2. Customize the Virtual Media helper application as needed.

For a sample helper application, see [“Sample Virtual Media helper application” \(page 240\)](#).

3. Create a directory on your website for the Virtual Media helper script, and then copy the script to that directory.

The sample script uses the directory name `cgi-bin`, but you can use any name.

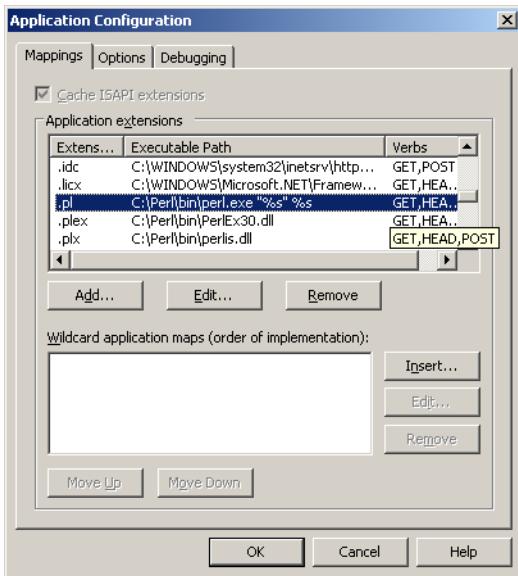
4. On the **Properties** page for your directory, under **Application Settings**, click **Create** to create an application directory.

The icon for your directory in IIS Manager changes from a folder icon to a gear icon.

5. Set the **Execute** permissions to **Scripts only**.
6. Verify that Perl is set up as a script interpreter.

To view the application associations, click **Configuration** on the **Properties** page. Ensure that Perl is configured as shown in [Figure 5 \(page 240\)](#).

Figure 5 Perl configuration example



7. Verify that Web Service Extensions allows Perl scripts to execute. If not, click **Web Service Extensions** and set **Perl CGI Extension** to **Allowed**.
8. Verify that the prefix variable in the helper application is set correctly.

To view a sample helper application, see “[Sample Virtual Media helper application](#)” (page 240).

Inserting Virtual Media with a helper application

When you are using a helper application with the `INSERT_VIRTUAL_MEDIA` command, the basic format of the URL is as follows:

`protocol://user:password@servername:port/path,helper-script`

where:

- `protocol`—Mandatory. Either HTTP or HTTPS.
- `user:password`—Optional. When present, HTTP basic authorization is used.
- `servername`—Mandatory. Either the host name or the IP address of the web server.
- `port`—Optional. A web server on a nonstandard port.
- `path`—Mandatory. The image file that is being accessed.
- `helper-script`—Optional. The location of the helper script on IIS web servers.

For detailed information about the `INSERT_VIRTUAL_MEDIA` command, see the iLO scripting and CLI guide.

Sample Virtual Media helper application

The following Perl script is an example of a CGI helper application that allows diskette writes on web servers that cannot perform partial writes. A helper application can be used in conjunction with the `INSERT_VIRTUAL_MEDIA` command to mount a writable disk.

When you are using the helper application, the iLO firmware posts a request to this application using the following parameters:

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

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

Example:

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working directory to the
# location of the image file that you are trying to write
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);

my $q = new CGI();           # Get CGI data

my $file = $q->param('file'); # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data = $q->param('data'); # Data to be written

#
# Change the file name appropriately
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
    $start = hex($1);
    $end = hex($2);
    $len = $end - $start + 1;
}

#
# Decode the data (a big hexadecimal string)
#
$decode = pack("H*", $data);

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

print "Content-Length: 0\r\n";
print "\r\n";
```

Virtual Media Boot Order

The Virtual Media Boot Order feature enables you to set the server boot options.

Changes made to the boot mode, boot order, or one-time boot status might require a server reset. iLO notifies you when a reset is required.

An error occurs if you try to change the server boot order when the server is in POST. You cannot modify the boot order during POST. If this error occurs, wait for POST to finish, and then try again.

Configuring the server boot mode

Servers that support the Unified Extensible Firmware Interface include the UEFI System Utilities software, which is embedded in the system ROM. On servers that support this feature, the iLO web interface **Boot Order** page includes the **Boot Mode** section.

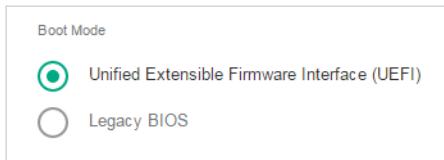
Use the **Boot Mode** setting to define how the server looks for OS boot firmware. You can select UEFI or the Legacy BIOS.

Prerequisites

Configure iLO Settings privilege

Changing the server boot mode

1. Navigate to the **Virtual Media**→**Boot Order** page.
2. Select **Unified Extensible Firmware Interface (UEFI)** or **Legacy BIOS**.



3. Click **Apply**.

iLO prompts you to confirm the change. When you change this setting, you cannot make additional changes on the **Boot Order** page until you reset the server.

4. Click **OK**.
5. Click **Server Reset**.

Configuring the server boot order

Prerequisites

Configure iLO Settings privilege

Changing the server boot order

1. Navigate to the **Virtual Media**→**Boot Order** page.

When Virtual Media is connected, the iLO web interface displays the Virtual Media type next to the **Virtual Floppy/USB key** and **Virtual CD/DVD-ROM** text at the top of the page.

2. Select a device in the **Server Boot Order** list, and click **Up** or **Down** to move it up or down in the boot order.



In Legacy BIOS mode, select from the following devices:

- **CD/DVD Drive**
- **Floppy Drive** (ProLiant Gen8 servers only)

- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card and additional NIC/FlexibleLOM cards are Network Device 1, Network Device 2, Network Device 3, and so on.

In UEFI mode, select an option from the list of available boot devices.

3. Click **Apply**.

iLO confirms that the boot order was updated successfully.

Changing the one-time boot status

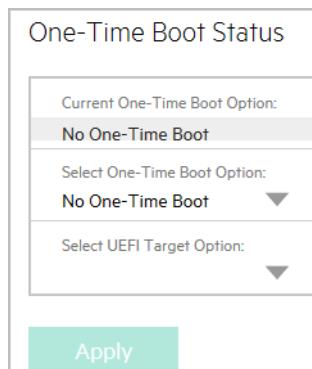
Use the one-time boot status feature to set the type of media to boot on the next server reset, without changing the predefined boot order. The procedure to use depends on whether the server uses Legacy BIOS mode or UEFI mode.

Prerequisites

Configure iLO Settings privilege

Changing the one-time boot status in Legacy BIOS mode

1. Navigate to the **Virtual Media**→**Boot Order** page.
2. Select an option from the **Select One-Time Boot Option** list.



The following options are available:

- **No One-Time Boot**
- **CD/DVD Drive**
- **Floppy Drive** (ProLiant Gen8 servers only)
- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
- **Intelligent Provisioning**
- **Embedded UEFI Shell**—When you select this option, the server boots to an embedded shell environment that is separate from the UEFI System Utilities.

3. Click **Apply**.

iLO confirms that the one-time boot option was updated successfully.

The **Current One-Time Boot Option** value is updated to show the selection.

Changing the one-time boot status in UEFI mode

1. Navigate to the **Virtual Media**→**Boot Order** page.
2. Select an option from the **Select One-Time Boot Option** list.

The following options are available:

- **No One-Time Boot**
- **CD/DVD Drive**
- **Floppy Drive** (ProLiant Gen8 servers only)
- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
- **Intelligent Provisioning**
- **UEFI Target**—When you select this option, you can select from the list of available boot devices in the **Select UEFI Target Option** list.
- **Embedded UEFI Shell**—When you select this option, the server boots to an embedded shell environment that is separate from the UEFI System Utilities.

3. If you selected **UEFI Target** in the **Select One-Time Boot Option** list, select a boot device from the **Select UEFI Target Option** list. For example, you might have a hard drive with two bootable partitions, and you can use this option to select the bootable partition to use on the next server reset.
4. Click **Apply**.

iLO confirms that the one-time boot option was updated successfully.

The **Current One-Time Boot Option** value is updated to show the selection.

Using the additional options

The **Additional Options** section on the **Boot Order** page provides buttons for resetting the server and booting to the system setup utilities.

Navigate to the **Virtual Media**→**Boot Order** page.

- Depending on whether your system supports the legacy system RBSU or the UEFI System Utilities, click **Boot to System RBSU** or **Boot to System Setup Utilities** to load the ROM-based setup utility on the next server reset. The Virtual Media and Configure iLO Settings privileges are required to use this feature.
- Click **Server Reset** to reboot the server. If a one-time boot option is specified, this setting takes precedence over the **Server Boot Order** value. The Virtual Power and Reset privilege is required to use this feature.

20 Using the power management features

Server power-on with iLO 4

Nonblade servers

Before the introduction of ProLiant Gen8 servers, some ProLiant servers (ML and DL) could be powered on through the power button within a few seconds after AC power was connected. If an AC power loss occurs on ProLiant Gen8 or Gen9 servers with iLO 4, approximately 30 seconds must elapse before the servers can power on again. If the power button is pressed during that time, it will blink, indicating a pending request.

This delay is a result of the iLO firmware loading, authenticating, and booting. iLO processes pending power-button requests when initialization is complete. If the server does not lose power, there is no delay. A 30-second delay occurs only during an iLO reset. The power button is disabled until iLO is ready to manage power.

A power-button watchdog allows the user to power on the system using the power button when iLO does not boot successfully.

The iLO firmware monitors and configures power thresholds to support managed-power systems (for example, using Hewlett Packard Enterprise power capping technology). Multiple system brownout, blackout, and thermal overloads might result when systems are allowed to boot before iLO can manage power. The managed-power state is lost because of AC power loss, so iLO must first boot to a restore state and allow power-on.

c-Class blade servers and Synergy compute modules

With ProLiant Gen8 and Gen9 blade servers and Synergy compute modules, the server cannot power on until the system is identified, iLO determines the power requirements of the server and enclosure or frame, and verifies that power is available. When AC power is applied to a server in an enclosure or frame, there is a short delay. If the system does not power on when the button is pressed check the OA (c-Class) or HPE OneView (ProLiant or Synergy) for more information. If an issue prevents server power on, an event is reported in the IML.

Brownout recovery

A brownout condition occurs when power to a running server is lost momentarily. Depending on the duration of the brownout and the server hardware configuration, a brownout might interrupt the operating system, but does not interrupt the iLO firmware.

iLO detects and recovers from power brownouts. If iLO detects that a brownout has occurred, server power is restored after the power-on delay unless **Auto-Power On** is set to **Always Remain Off**. After the brownout recovery, iLO firmware records a `Brown-out recovery` event in the iLO Event Log.

Graceful shutdown

The ability of the iLO processor to perform a graceful shutdown requires cooperation from the operating system. To perform a graceful shutdown, the iLO health driver must be loaded. iLO communicates with the health driver and uses the appropriate operating system method of shutting down the system safely to ensure that data integrity is preserved.

If the health driver is not loaded, the iLO processor attempts to use the operating system to perform a graceful shutdown through the power button. iLO emulates a physical power-button press (iLO momentary press) to prompt the operating system to shut down gracefully. The behavior of the operating system depends on its configuration and settings for a power-button press.

For more information about the iLO drivers, see [“iLO drivers and utilities” \(page 32\)](#).

The Thermal Shutdown option in the system RBSU or UEFI System Utilities allows you to disable the automatic shutdown feature. This configuration allows the disabling of automatic shutdown except in the most extreme conditions when physical damage might result.

Power efficiency

iLO enables you to improve power usage by using High Efficiency Mode. HEM improves the power efficiency of the system by placing the secondary power supplies in step-down mode. When the secondary supplies are in step-down mode, the primary supplies provide all DC power to the system. The power supplies are more efficient because there are more DC output watts for each watt of AC input.

NOTE: HEM is available on nonblade servers only.

When the system draws more than 70% of the maximum power output of the primary supplies, the secondary supplies return to normal operation (exit step-down mode). When power use drops below 60% capacity of the primary supplies, the secondary supplies return to step-down mode. HEM enables you to achieve power consumption equal to the maximum power output of the primary and secondary power supplies, while maintaining improved efficiency at lower power-usage levels.

HEM does not affect power redundancy. If the primary supplies fail, the secondary supplies immediately begin supplying DC power to the system, preventing any downtime.

Use the system RBSU or UEFI System Utilities to configure HEM. You cannot configure these settings through iLO. For more information, see the system RBSU user guide or the UEFI System Utilities user guide.

The configured HEM settings are displayed on the **System Information**→**Server Power** page.

Power-on protection

iLO 2.50 and later provides power-on protection for Synergy compute modules by preventing the server hardware from being powered on when the hardware cannot be identified. This situation might occur when a mezzanine card is installed incorrectly, or a server cannot communicate with a hardware component.

Power-on protection works in conjunction with the Auto Power-On and Virtual Power Button Momentary Press features. If the server hardware cannot be identified when server power is restored or a Momentary Press is requested, the server will not power on.

When the power-on protection feature prevents server power-on:

- An event is recorded in the IML.
- The server health status is set to Critical.
- If HPE OneView manages the server, an SNMP trap is sent to HPE OneView.

Power allocation (blade servers)

Blade servers operate in a shared power environment with an enclosure or frame. Before a server can be powered on, it must obtain a power allocation from its enclosure (ProLiant servers) or frame (Synergy compute modules).

If power-on is prevented, an error is recorded in the IML, and the server Health LED changes. The following errors might prevent power-on:

- **Electronic Keying or I/O Configuration Error**—There is a mismatch between the mezzanine devices in the server and the switches on the back of the enclosure.
- **Not Enough Power**—There is insufficient power available in the enclosure to power on the server.

- **Not Enough Cooling**—There is insufficient cooling available in the enclosure to cool the server.
- **Enclosure Busy**—The enclosure is busy collecting information about the blade. If this error occurs after server insertion and auto power-on is enabled, iLO will continue to request power until it is allowed. Otherwise, press the momentary press button again.
- **Power Hold by Manager Profile** (Synergy compute modules only)—HPE OneView has placed a power hold on this server.
- **Enclosure Error** (Synergy compute modules only)—An enclosure error occurred.

For troubleshooting information, see the error messages guide for your server.

Managing the server power

The **Virtual Power Button** section on the **Server Power** page displays the current power state of the server, as well as options for remotely controlling server power. **System Power** indicates the state of the server power when the page is first opened. The server power state can be **ON**, **OFF**, or **Reset**. Use the browser refresh feature to view the current server power state. The server is rarely in the **Reset** state.

Prerequisites

Virtual Power and Reset privilege

Changing the server power state

1. Navigate to the **Power Management**→**Server Power** page.
2. Click one of the following buttons:
 - **Momentary Press**
 - **Press and Hold**
 - **Reset**
 - **Cold Boot**

The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.

3. When prompted to confirm the request, click **OK**.

Virtual Power Button options

- **Momentary Press**—The same as pressing the physical power button. If the server is powered off, a momentary press will turn on the server power.
Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. Hewlett Packard Enterprise recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.
- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.
The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.
This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.

- **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.
- **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Configuring the System Power Restore Settings

The **System Power Restore Settings** section enables you to control system behavior after power is lost. You can also configure these settings by using the system RBSU or UEFI System Utilities during POST.

Prerequisites

The Configure iLO Settings privilege is required to perform this procedure.

Changing the System Power Restore Settings

1. Navigate to the **Power Management**→**Server Power** page.
2. Select an **Auto Power-On** value.

This setting determines how iLO behaves after power is restored—for example, when the server is plugged in or when a UPS is activated after a power outage. This setting is not supported with micro-UPS systems.

Changes to the **Auto Power On** value might not take place until after the next server reboot.

Auto Power-On:	<input type="radio"/> Always Power On <input type="radio"/> Always Remain Off <input checked="" type="radio"/> Restore Last Power State
----------------	---

3. Select a **Power-On Delay** value.

This setting staggers server automatic power-on in a data center. It determines the amount of time that iLO waits before powering on a server after iLO startup is complete. This setting is not supported with micro-UPS systems.

If a server does not support this feature, **N/A** is displayed.

Power-On Delay:	<input checked="" type="radio"/> Minimum Delay <input type="radio"/> 15 Second Delay <input type="radio"/> 30 Second Delay <input type="radio"/> 45 Second Delay <input type="radio"/> 60 Second Delay <input type="radio"/> Random up to 120 Seconds
-----------------	--

4. Click **Submit**.

Auto Power-On settings

Choose from the following Auto Power-On settings:

- **Always Power On**—Power on the server after the power-on delay (default for server blades).
- **Always Remain Off**—The server remains off until directed to power on.
- **Restore Last Power State**—Returns the server to the power state when power was lost. If the server was on, it powers on; if the server was off, it remains off. This option is the default setting for nonblade servers. It is not available on server blades.

Power-On Delay settings

On supported servers, choose from the following Power-On delay settings:

- **Minimum Delay**—Power-on occurs after iLO startup is complete.
- **15 Second Delay**—Power-on is delayed by 15 seconds.
- **30 Second Delay**—Power-on is delayed by 30 seconds.
- **45 Second Delay**—Power-on is delayed by 45 seconds.
- **60 Second Delay**—Power-on is delayed by 60 seconds.
- **Random up to 120 seconds**—The power-on delay varies and can be up to 120 seconds.

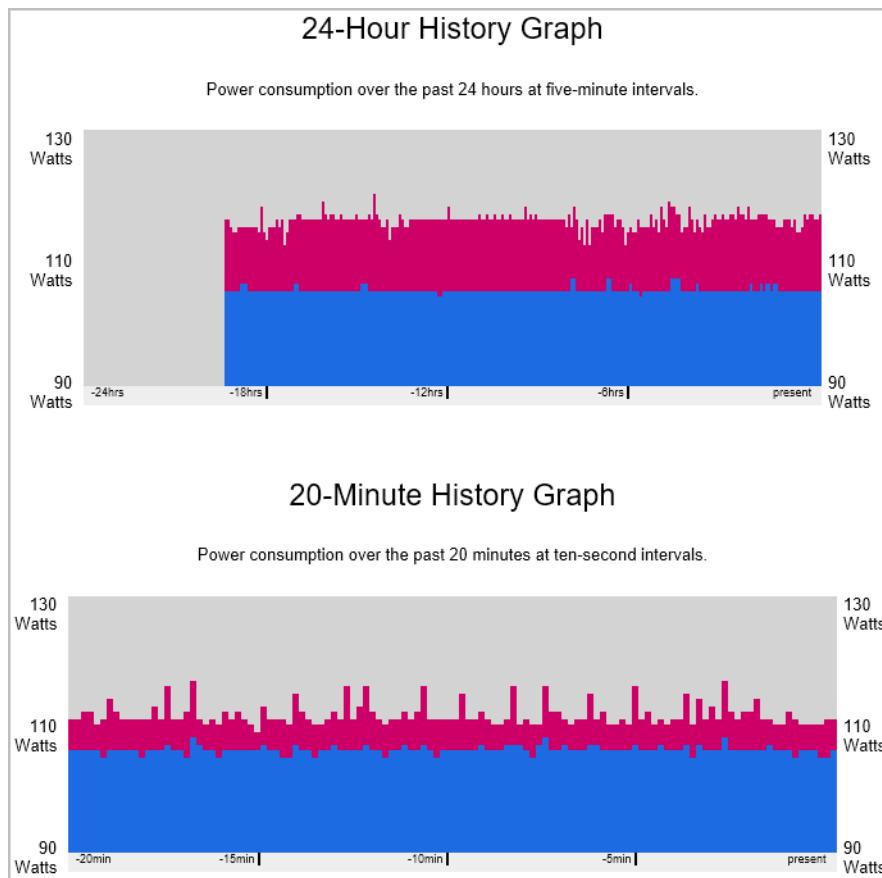
Viewing server power usage

Navigate to the **Power Management**→**Power Meter** page.

The **Power Meter** page enables you to view the server power consumption over time.

This feature and many others are part of an iLO licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Power meter graph details



The power-meter graphs display recent server power usage. The graph data is reset when iLO or the server is reset. The iLO firmware periodically samples peak power, average power, and power cap. The following graphs are displayed:

- **24-Hour History Graph**—Displays the power usage of the server over the previous 24 hours. The iLO firmware collects power usage information from the server every 5 minutes.

The bar graph displays the average values in blue and the peak values in red. The graph shows **No cap set** during a host power reset.

- **20-Minute History Graph**—Displays the power usage of the server over the previous 20 minutes. The iLO firmware collects power usage information from the server every 10 seconds. The bar graph displays the average values in blue and the peak values in red.

Power metering is not supported on servers with an installed Flex Slot Battery Backup Unit.



TIP: To view the power usage for a specific point in time, move the mouse cursor over the graph.

Power meter graph display options

When you view the power-meter graphs, use the **Display Options** to control the displayed information. You can view minimum, average, peak, and cap power information.



Select one or more of the following check boxes, and then click **Refresh Page** to update the graphs.

- **Min (static low)**—The minimum value observed during a measurement period. Typically, the 20-minute graph measures a minimum value every 10 seconds, which matches the average value. The 24-hour graph can capture minimum values lower than the 5-minute average value.
- **Avg**—The mean power reading during the sample.
- **Peak**—The highest instantaneous power reading during the sample. iLO records this value on a subsecond basis.
- **Cap**—The configured power cap during the sample. If the power cap is not configured or is not supported, the **Cap** option is not available.
 - A power cap limits average power draw for extended periods of time.
 - Power caps are not maintained during server reboots, resulting in temporary spikes during boot.
 - Power caps set for less than 50% of the difference between maximum power and idle power might become unreachable because of changes in the server. Hewlett Packard Enterprise does not recommend configuring power caps for less than 20%. Configuring a power cap that is too low for the system configuration might affect system performance.

The following options are also available:

- **Power Unit**—Select a value from the **Power Unit** list to change the power reading display to watts or BTU/hr.
- **Refresh Page**—Click the **Refresh Page** button to update the history graphs.

Viewing the current power state

1. Navigate to the **Power Management**→**Power Meter** page.

2. Scroll to the **Current State** section.

Current power state details

Current State	
Present Power Reading	95 Watts
Present Power Cap	0 Watts
Power Regulator Mode	Dynamic

The values displayed in the **Current State** table vary depending on the server type.

- **Present Power Reading**—The current power reading from the server. This value is displayed for all servers.
- **Present Power Cap**—The configured power cap for the server. This value is 0 if the power cap is not configured. This value is displayed for ML and DL servers, and server blades.
- **Power Input Voltage**—The supplied input voltage for the server. This value is displayed for ML and DL servers.
- **Power Regulator Mode**—The configured Power Regulator for ProLiant mode. This value is displayed for all servers. For information about the possible settings, see “[Power settings](#)” (page 252).
- **Power Supply Capacity**—The server power capacity. This value is displayed for SL and XL servers.
- **Peak Measured Power**—The highest measured power reading. This value is displayed for SL and XL servers.

Viewing the server power history

1. Navigate to the **Power Management**→**Power Meter** page.
2. Scroll to the **Power History** section.

Power history details

Power History			
	5 min	20 min	24 hr
Average Power	105 Watts	106 Watts	105 Watts
Maximum Power	116 Watts	117 Watts	120 Watts
Minimum Power	105 Watts	105 Watts	104 Watts

The **Power History** table shows power readings from three time periods: 5 minutes, 20 minutes, and 24 hours.

- **Average Power**—The average of the power readings for the specified time period. If the server has not been running for the specified time period, the value is the average of all readings since the server booted.
- **Maximum Power**—The maximum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the maximum of all readings since the server booted.
- **Minimum Power**—The minimum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the minimum of all readings since the server booted.

When multiple power supplies are removed from the server at the same time, there is a short time period in which iLO will not display information in the **Power History** section or in the **Power**

Meter graphs. This information will be displayed again after iLO collects information about the remaining installed power supplies.

Power settings

The **Power Settings** page enables you to view and control the power management features of the server. The power management features on this page vary based on the server configuration.

Power Regulator settings

The Power Regulator feature enables iLO to modify processor frequency and voltage levels based on operating conditions, to provide power savings with minimal effect on performance. The **Power Settings** page allows you to view and control the power regulator mode.

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- The server is not in POST. The Power Regulator settings cannot be changed while the server is in POST.

Configuring the Power Regulator settings

1. Navigate to the **Power Management**→**Power Settings** page.
2. Select a Power Regulator mode.
3. Click **Apply**.
 - For the **Dynamic Power Savings Mode**, **Static Low Power Mode**, and **Static High Performance Mode** settings, iLO notifies you that the Power Regulator settings changed.
 - For the **OS Control Mode** setting, iLO notifies you that you must reboot the server to complete the Power Regulator settings change.

If the settings do not change after you click **Apply**, the server might be in the boot process or require rebooting. Exit any ROM-based program that is running, allow POST to complete, and then try again.

4. If iLO notified you that a reboot is required, reboot the server.

More information

[Power Regulator modes](#)

Power Regulator modes

Choose from the following modes when you configure the Power Regulator settings:

- **Dynamic Power Savings Mode**—Automatically varies processor speed and power usage based on processor utilization. This option allows the reduction of overall power consumption with little or no impact to performance. It does not require OS support.
- **Static Low Power Mode**—Reduces processor speed and power usage. This option guarantees a lower maximum power usage for the system.
- **Static High Performance Mode**—Processors will run at maximum power/performance at all times, regardless of the OS power management policy.
- **OS Control Mode**—Processors will run at maximum power/performance at all times, unless the OS enables a power management policy.

Configuring power caps

Prerequisites

- Configure iLO Settings privilege
- An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.
- The server model supports power capping.
See the server specifications for support information.

Configuring a power cap

- Navigate to the **Power Management**→**Power Settings** page.
- Select the **Enable power capping** check box.
- Enter the **Power Cap Value** in watts, BTU/hr, or as a percentage.

The percentage is the difference between the maximum and minimum power values.

The power cap value cannot be set below the server minimum power value.

- Optional: When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.
- Click **Apply**.

iLO notifies you that the change was successful.

Power capping considerations

- During POST, the ROM runs two power tests that determine the peak and minimum observed power values.
Consider the values in the **Power Capping Settings** table when determining your power capping configuration.
 - Maximum Available Power**—The power supply capacity for a nonblade server, or the initial power-on request value for a server blade. This value is the **Maximum Power Cap** threshold. The server must not exceed this value.
 - Peak Observed Power**—The maximum observed power for the server. This value is the **Minimum High-Performance Cap** threshold, and it represents the maximum power that the server uses in the current configuration. A power cap set to this value does not affect server performance.
 - Minimum Observed Power**—The minimum observed power for the server. This value is the **Minimum Power Cap** threshold, and it represents the minimum power that the server uses. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- When a power cap is set, the average power reading of the server must be at or below the power cap value.
- Power capping settings are disabled when the server is part of an Enclosure Dynamic Power Cap. These values are set and modified by using Onboard Administrator or Insight Control Power Management.
- Power capping is not supported on servers with an installed Flex Slot Battery Backup Unit.

- Power capping is not supported on all servers. For more information, check the server specifications.
- You cannot use the iLO web interface to configure the power capping settings for SL servers and some XL servers. Use one of the following tools to configure the power capping settings for SL and XL servers:
 - HPE ProLiant Power Interface Control Utility
 - HPE Advanced Power Manager

See the server Quickspecs at <http://www.hpe.com/info/quickspecs> for information about the power management features your XL server supports.

Configuring battery backup unit settings

When power supplies cannot provide power to a server with a battery backup unit installed in one of the power supply bays, the server runs on power provided by the battery backup unit.

Use the following procedure to choose the action iLO takes when a server is running on a battery backup unit.

Prerequisites

Configure iLO Settings privilege

Configuring the battery backup settings

1. Navigate to the **Power Management**→**Power Settings** page.
2. In the **Battery Backup Unit Settings** section, select the action you want iLO to take when the server runs on the battery backup unit.
3. Click **Apply**.

iLO notifies you that the change was successful.

Battery backup unit options

You can configure iLO to take one of the following actions when a server is running on battery power:

- **No Action** (default)—Do nothing when the server is running on battery power. If power is not restored, the server will lose power when the battery is depleted.
- **Momentary Power Button Press**—When iLO detects that the server is running on battery power for at least 10 seconds, it sends a momentary power button press to the server. If the operating system is configured to react to the power button press, the operating system initiates a shutdown.

Send Shutdown Message to OS—When iLO detects that the server is running on battery power for at least 10 seconds, it sends a shutdown message to the host operating system. If the required server management software is installed, the operating system initiates a shutdown.

To verify server support for a battery backup unit, see the server QuickSpecs at the following website: <http://www.hpe.com/info/qs>.

Configuring SNMP alert settings

The **SNMP Alert on Breach of Power Threshold** feature enables the sending of an SNMP alert when power consumption exceeds a defined threshold.

Prerequisites

Configure iLO Settings privilege

Configuring the SNMP alert settings

1. Navigate to the **Power Management**→**Power Settings** page.
2. Select a value in the **Warning Trigger** list.

The warning trigger determines whether warnings are based on peak power consumption, average power consumption, or if they are disabled.

3. If you selected **Peak Power Consumption** or **Average Power Consumption** in the **Warning Trigger** list, enter the following:

- **Warning Threshold**—Sets the power consumption threshold, in watts. If power consumption exceeds this value for the specified time duration, an SNMP alert is triggered.
- **Duration**—Sets the length of time, in minutes, that power consumption must remain above the warning threshold before an SNMP alert is triggered. When an SNMP alert is generated, it is based on the power consumption data sampled by iLO. It is not based on the exact date and time that the **Duration** value was changed. The maximum duration is 240 minutes, and the duration must be a multiple of 5.

4. Click **Apply**.

Configuring the persistent mouse and keyboard

The **Other Settings** section on the **Power Settings** page allows you to enable or disable the persistent keyboard and mouse feature.

When this feature is enabled, the iLO virtual keyboard and mouse are always connected to the iLO UHCI USB controller. When this feature is disabled, the iLO virtual keyboard and mouse are connected dynamically to the iLO UHCI controller only when a Remote Console application is open and connected to iLO. Disabling the feature allows some servers to increase power savings by 15 watts when the server OS is idle and no virtual USB keyboard and mouse are connected.

For example, the power savings for a 24-hour period might be 15 watts x 24 hours, or 360 watt hours (.36 kilowatt-hours).

Prerequisites

Configure iLO Settings privilege

Configuring the persistent mouse and keyboard setting

1. Navigate to the **Power Management**→**Power Settings** page.
2. Select or clear the **Enable persistent mouse and keyboard** check box.

The persistent mouse and keyboard feature is disabled by default.

3. Click **Apply**.

iLO notifies you that the change was successful.

21 Working with enclosures, frames, and chassis

Using the Active Onboard Administrator

OA is the enclosure management processor, subsystem, and firmware base that supports the HPE BladeSystem and all managed devices in the enclosure.

The **Active Onboard Administrator** page allows you to view enclosure information, start the OA web interface, and toggle the enclosure UID LED. This page is displayed only when an enclosure is present.

Viewing OA information

Navigate to the **BL c-Class**→**Active Onboard Administrator** page.

This page provides general information about the primary OA in the enclosure in which the iLO processor is located.

OA details

HPE BladeSystem Onboard Administrator	
MAC Address	
System Health	OK
Blade location	Bay 5
Enclosure name	C7000-MixBladeEnc
Rack name	

- **MAC Address**—The MAC address of the active OA.
- **System Health**—The health of the active OA, as reported by the OA. A value of **unknown** means that the OA health has not been reported to iLO.
- **Blade location**—The location (enclosure bay) of the blade that is hosting the current iLO session.
- **Enclosure name**—The enclosure that the active OA is managing. You can change this value through the OA.
- **Rack name**—The rack that contains the enclosure managed by the active OA. You can change this value through the OA.

Starting the OA GUI

1. Navigate to the **BL c-Class**→**Active Onboard Administrator** page.

Onboard Administrator Address Selection	
Address Type	IP Address
<input checked="" type="radio"/> IPv4	
Onboard Administrator Buttons	
Onboard Administrator GUI	Enclosure UID light: <input checked="" type="radio"/> UID OFF
<input type="button" value="Launch"/>	<input type="button" value="Toggle UID"/>

2. If the OA supports multiple addresses, select the address to use from the options in the **Onboard Administrator Address Selection** table.

Depending on the configuration, the following options might be available:

- **IPv4**
- **IPv6 SLAAC**
- **IPv6 Static**
- **IPv6 DHCP**

3. Click **Launch**.

The OA web interface starts in a new browser window.

Toggling the enclosure UID LED

To change the state of the enclosure UID LED where iLO is located, click the **Toggle UID** button.

The UID LED status on this page represents the enclosure UID LED status when the iLO page loaded. To update the status, refresh the page.

Enclosure bay IP addressing

The First Time Setup Wizard prompts you to set up your enclosure bay IP addressing. For more information about the wizard, see the OA user guide.

Dynamic Power Capping for server blades

Dynamic Power Capping is an iLO feature available for c-Class server blades, and is accessed through OA. Dynamic Power Capping is available only if your system hardware platform, BIOS (ROM), and power microcontroller firmware version support this feature. If your system supports Dynamic Power Capping, iLO automatically runs in Dynamic Power Capping mode.

For information about the power setting options for c-Class server blades, see the OA user guide.

iLO virtual fan

In c-Class blade servers, OA controls the enclosure fans (also called virtual fans). The iLO firmware cannot detect these enclosure fans. Instead, the iLO firmware monitors an ambient temperature sensor on the blade server. This information is displayed in the iLO web interface, and OA retrieves it periodically. OA uses the sensor information collected from all iLO processors in the enclosure to determine enclosure fan speeds.

iLO option

The **iLO - Device Bay <XX>** page in OA provides the following links:

- **Web Administration**—Starts the iLO web interface
- **Integrated Remote Console**—Starts the .NET IRC
- **Remote Console**—Starts the Java IRC

Clicking a link on this page opens the requested iLO session in a new window that uses SSO, which does not require an iLO user name or password. If your browser settings prevent new windows from opening, these links do not work correctly.

The screenshot shows the 'iLO - Device Bay' page with the 'Event Log' tab selected. The 'Management Processor Information' section displays the following details:

Name	ILO
Address	[REDACTED]
MAC Address	[REDACTED]
Model	ILO4
Firmware Version	2.10 Oct 02 2014
iLO Federation Capable	Yes

The 'Management Processor IPv6 Information' section shows the 'Link Local Address' field as empty. The 'iLO Remote Management' section contains a note: 'Select the address that will be used for the links in the section below.' Below this note is a radio button next to a placeholder '(Link Local Address)' and a help icon.

Viewing frame information

1. Navigate to the **Synergy Frame→Frame Information** page.
2. Optional: To view server details, move the cursor over the server in the frame diagram.

The **Frame Information** page provides information about the frame that contains the Synergy compute module that includes the iLO processor.

Frame details

The 'Frame details' section displays the following information:

Frame health	Degraded
Enclosure UID light	UID OFF
Server location	Bay 1
Frame serial number	[REDACTED]
Frame unique ID (UUID)	[REDACTED]

- **Frame health**—The frame health status.
This status is also displayed in the frame diagram.
- **Enclosure UID light**—The state of the frame UID LED. The UID LED helps you identify and locate a frame.
This status value represents the frame UID LED status when the iLO page loaded. To update the status, refresh the page.
This status is also displayed in the frame diagram.
- **Server location**—The bay number of the server in the frame.
- **Frame serial number**—The frame serial number.
- **Frame unique ID (UUID)**—The frame UUID.

Toggling the frame UID LED

To change the state of the frame UID LED, click the frame UID icon  in the frame diagram.

The UID LED status on this page updates automatically with a maximum delay of 30 seconds when the UID LED status changes. To update the status immediately, refresh the page.

Server details

The frame diagram displays the following details when you move the cursor over a server:

- Server health status
- Server host name
- Server model
- Server UID status

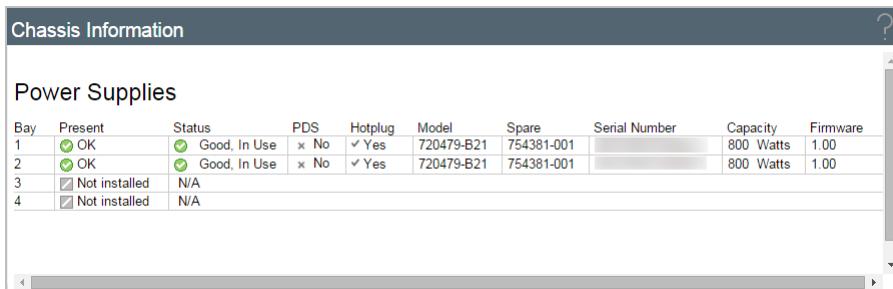
Toggling the server UID LED

To change the state of the server UID LED, click the server UID icon  in the frame diagram.

Viewing chassis information

Navigate to the **Chassis→Chassis Information** page.

The **Chassis Information** page is displayed for SL and XL servers.



The screenshot shows a table titled "Power Supplies" with the following data:

Bay	Present	Status	PDS	Hotplug	Model	Spare	Serial Number	Capacity	Firmware
1	 OK	 Good, In Use	 No	 Yes	720479-B21	754381-001		800 Watts	1.00
2	 OK	 Good, In Use	 No	 Yes	720479-B21	754381-001		800 Watts	1.00
3	 Not installed	N/A							
4	 Not installed	N/A							

Power Supplies list

The **Chassis Information** page displays the following details about the power supplies in the chassis.

Some power supplies do not provide information for all of the values on this page. If a power supply does not provide information for a value, **N/A** is displayed.

Bay

The chassis power supply bay number.

Present

Indicates whether a power supply is installed. The possible values are **OK** and **Not Installed**.

Status

The status of the power supply. The displayed value includes a status icon (**OK**, **Degraded**, **Failed**, or **Other**), and text that provides more information. The possible values follow:

- **Unknown**
- **Good, In Use**
- **Good, Standby**
- **General Failure**
- **Over Voltage Failure**
- **Over Current Failure**
- **Over Temperature Failure**

- **Input Voltage Lost**
- **Fan Failure**
- **High Input A/C Warning**
- **Low Input A/C Warning**
- **High Output Warning**
- **Low Output Warning**
- **Inlet Temperature Warning**
- **Internal Temperature Warning**
- **High Vaux Warning**
- **Low Vaux Warning**
- **Mismatched Power Supplies**

PDS

Whether the installed power supply is enabled for Power Discovery Services.

Power Discovery Services is an enhancement to the iPDU technology. If the chassis power supply is connected to an iPDU, an additional summary table on this page displays the linked iPDU.

Hotplug

Whether the power supply bay supports swapping the power supply when the chassis is powered on. If the value is **Yes**, and the power supplies are redundant, the power supply can be removed or replaced when the chassis is powered on.

Flex Slot Battery Backup Unit

The following information is displayed for supported chassis with an installed Flex Slot Battery Backup Unit:

- **Charge**—The current battery charge (percent).
- **Days Active**—The number of calendar days that the battery has been installed.
- **Battery Health**—The battery health status (0 to 100 percent).

Battery health issues are reported in the IML.

Power capping and power metering are not supported on chassis with an installed Flex Slot Battery Backup Unit.

For more information, see the Flex Slot Battery Backup Unit installation instructions.

Model

The model number of the power supply.

Spare

The part number of the spare power supply.

Serial Number

The serial number of the power supply.

Capacity

The capacity of the power supply (watts).

Firmware

The installed power supply firmware.

Intelligent Power Distribution Unit details

The **Intelligent Power Distribution Units** section is displayed only if the chassis power supplies are connected to an iPDU.

After iLO is reset, or when an iPDU is attached, it takes approximately 2 minutes for the iLO web interface to display the **Intelligent Power Distribution Units** table. This delay is due to the iPDU discovery process. The following information is displayed in the table:

- **ID**—The power supply bay number.
- **Part Number**—The iPDU part number.
- **Serial Number**—The iPDU serial number.
- **IP Address**—The iPDU IP address.
- **SSL Port**—The iPDU SSL port.
- **MAC Address**—The MAC address of the iPDU network port. This value helps you to identify each connected iPDU because each iPDU has a unique MAC address.

Smart Storage Battery details

- **Index**—The battery index number.
- **Present**—Whether a battery is installed. The possible values are **OK** and **Not Installed**.
- **Status**—The battery status. The possible values are **OK**, **Degraded**, **Failed**, or **Other**.
- **Model**—The battery model number.
- **Spare**—The part number of the spare battery.
- **Serial Number**—The battery serial number.
- **Capacity**—The battery capacity.
- **Firmware**—The installed battery firmware version.

22 Using the Embedded User Partition

iLO Embedded User Partition

iLO 4 stores files such as Active Health System data and the Intelligent Provisioning software in nonvolatile flash memory that is embedded on the system board. This flash memory is called the iLO NAND. ProLiant Gen9 servers and Synergy compute modules with a 4 GB iLO NAND allow you to use a 1 GB nonvolatile flash memory partition as if it was an SD-card attached to the server. When the Embedded User Partition is enabled, you can access it through the server operating system.

The Embedded User Partition is accessible through the server OS for read and write access when the server is configured for Legacy BIOS or UEFI boot mode.

To determine whether your server includes a 4 GB iLO NAND, see the server QuickSpecs at <http://www.hpe.com/info/qs/>.

You can use the Embedded User Partition for tasks such as:

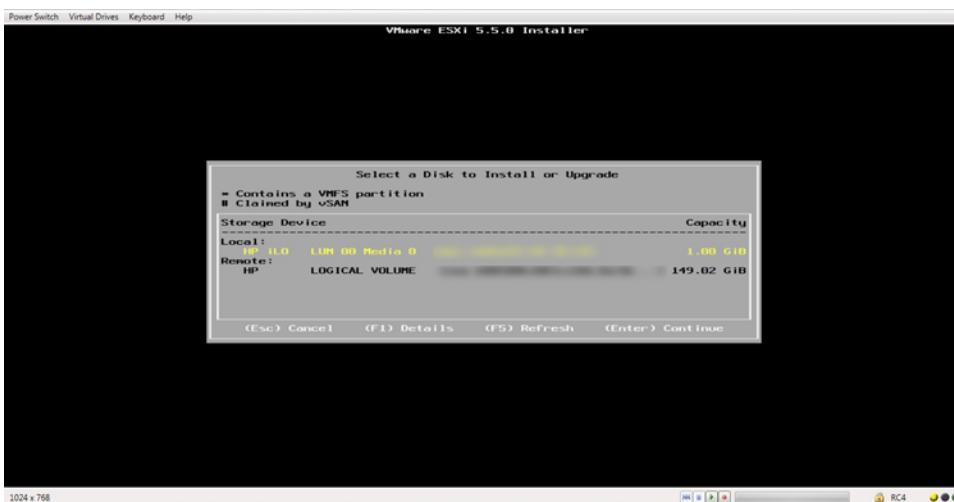
- Storing UEFI Shell scripts and test tools. UEFI scripts can be run automatically when the server boots to the embedded UEFI Shell. To use this feature, place a `startup.nsh` shell script file in the root directory of the Embedded User Partition.

This feature is supported only when the server is configured for the UEFI boot mode.

For more information, see the UEFI Shell user guide on the following website: <http://www.hpe.com/info/ProLiantUEFI/docs>.

- Installing and booting from VMware ESXi (UEFI mode only)

To select the Embedded User Partition for an OS or hypervisor installation, select the volume **HP iLO LUN <number>**.



- Storing iLO scripts
- Storing iLO language packs

! **IMPORTANT:** Do not use the Embedded User Partition for high-frequency write operations.

For information about configuring access to the Embedded User Partition, see “[Configuring the Embedded User Partition](#)” (page 263).

Configuring the Embedded User Partition

You can use the UEFI System Utilities, UEFI Shell, and RESTful Interface Tool to configure the Embedded User Partition.

Configuring the Embedded User Partition (UEFI System Utilities)

Use the following procedure to enable or disable the Embedded User Partition by using the UEFI System Utilities.

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**BIOS/Platform Configuration (RBSU)**→**System Options**→**USB Options**→**Embedded User Partition** and press **Enter**.
5. Select one of the following options:
 - **Enabled**
 - **Disabled** (default)
6. To save your selection, press **F10**.
7. Restart the server.
8. After you enable the Embedded User Partition, format it by using the server operating system software.
Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the UEFI Shell user guide.
2. Use the following command to enable the Embedded User Partition:
`sysconfig -s embeddeduserpartition=Enabled`
3. Restart the server.
4. After you enable the Embedded User Partition, format it by using the server operating system software.
Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition (RESTful Interface Tool)

1. Enable or disable the Embedded User Partition.

For information about configuring the Embedded User Partition with the RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: <http://www.hpe.com/info/restfulinterface/docs>.

2. After you enable the Embedded User Partition, format it by using the server operating system software.
Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition boot settings

You can use the UEFI System Utilities, UEFI Shell, RESTful Interface Tool, or iLO web interface to configure the Embedded User Partition boot settings.

Configuring the Embedded User Partition boot order setting (iLO web interface)

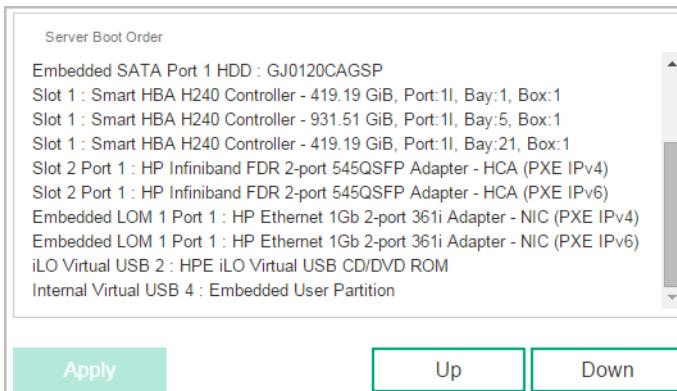
Use the following procedure to change the position of the Embedded User Partition in the **Server Boot Order** list.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Navigate to the **Virtual Media→Boot Order** page.
2. Select the Embedded User Partition device in the **Server Boot Order** list, and use the **Up** and **Down** buttons to change the boot order.

The Embedded User Partition is listed with a name similar to the following:

Internal Virtual USB 4 : Embedded User.



3. Click **Apply**.

The following message appears:

Successfully set boot order.

Configuring the Embedded User Partition for one-time boot (iLO web interface)

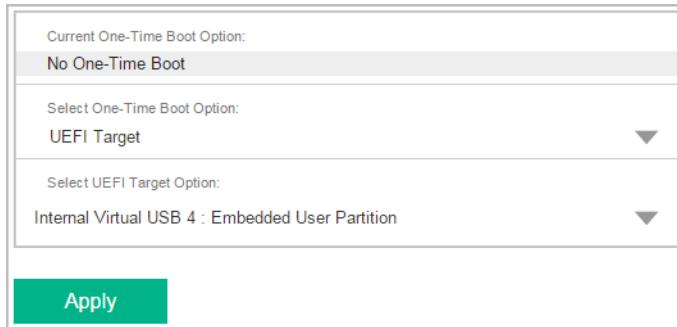
Use the following procedure to set the position of the Embedded User Partition in the **Server Boot Order** list.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Navigate to the **Virtual Media→Boot Order** page.
2. Select **UEFI Target** in the **Select One-Time Boot Option** list.
3. Select the Embedded User Partition from the **Select UEFI Target Option** list.

The Embedded User Partition is listed with a name similar to the following:

Internal Virtual USB 4 : Embedded User.



4. Click **Apply**.

The following message appears:

Successfully set one-time boot option.

The **Current One-Time Boot Option** value is updated to show the selection.

Configuring the Embedded User Partition boot order setting (UEFI System Utilities)

Use the following procedure to change the position of the Embedded User Partition in the **UEFI Boot Order** list.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.
4. From the **System Utilities** screen, select **System Configuration**→**BIOS/Platform Configuration (RBSU)**→**Boot Options**→**UEFI Boot Order** and press **Enter**.
5. From the **UEFI Boot Order** screen, press **Enter** to open the **UEFI Boot Order** list.
The Embedded User Partition is listed with a name similar to the following:
Internal Virtual USB 4 : Embedded User Partition.
6. Update the position of the Embedded User Partition in the boot order list, as needed.
 - Use the arrow keys to navigate within the boot order list.
 - To move an entry higher in the boot list, press the + key (plus).
 - To move an entry lower in the list, press the - key (minus).
7. To save your selection, press **F10**.
8. From the System Utilities screen, select **Exit and Resume Boot**.

For more information about the UEFI Boot Order list, see the UEFI System Utilities user guide.

Configuring the Embedded User Partition for one-time boot (UEFI System Utilities)

Use the following procedure to set the position of the Embedded User Partition in the **One Time Boot Menu**.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Optional: If you access the server remotely, start an iLO remote console session.
2. Restart or power on the server.
3. Press **F9** in the server POST screen.
The UEFI System Utilities start.

4. From the **System Utilities** screen, select **One Time Boot Menu**, and then press **Enter**.
5. From the **One-Time Boot Menu** screen, select the Embedded User Partition option, and then press **Enter**.

The Embedded User Partition is listed with a name similar to the following:

Internal Virtual USB 4 : Embedded User Partition.

The server resumes the boot process and boots from the Embedded User Partition.

For more information about the **One-Time Boot Menu**, see the UEFI System Utilities user guide.

Configuring the Embedded User Partition boot order setting (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the UEFI Shell user guide.
2. Use the following command to configure the Embedded User Partition boot order setting:

```
sysconfig -s uefibootorder=settingvalue
```

In this command, *settingvalue* is a UEFI boot order option.

For information about using this command, see the UEFI Shell user guide.

Configuring the Embedded User Partition for one-time boot (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the UEFI Shell user guide.
2. Use the following command to configure the Embedded User Partition for one-time boot:

```
boot -n settingvalue
```

Where *settingvalue* is the boot number of the device to use for one-time boot.

NOTE: For information about using this command, see the UEFI Shell user guide.

Configuring the Embedded User Partition boot order setting (RESTful Interface Tool)

For information about configuring the Embedded User Partition boot order setting with the RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: <http://www.hpe.com/info/restfulinterface/docs>.

Configuring the Embedded User Partition for one-time boot (RESTful Interface Tool)

For information about configuring the Embedded User Partition one-time boot settings with the RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: <http://www.hpe.com/info/restfulinterface/docs>.

23 Using iLO with other software products and tools

Viewing Location Discovery Services information

Prerequisites

An iLO license that supports this feature is installed. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Viewing Location Discovery Services information

Navigate to the **Information→Location Discovery Services** page.

The information displayed on this page varies depending on the server type.

This feature is not supported on Synergy compute modules.

Location Discovery Services details

Location Discovery Services	
Platform Type	DL/ML
Discovery Rack Support	Not Supported
Discovery Data Status	Server does not support Location Discovery Services
Rack Identifier	0
Rack Location Discovery Product Part Number	0
Rack Location Discovery Product Description	0
Rack U Height	0
U Location	0
Server UUID	50353138-3036-3730-4732-343930303031
Server U Height	0.00

- **Platform Type**—The server type.
- **Discovery Rack Support**—Whether the rack supports Location Discovery Services.
- **Discovery Data Status**—Whether there was an error during discovery.
- **Rack Identifier**—The rack identifier. If data is not available, the value **0** is displayed.
- **Rack Location Discovery Product Part Number**—The rack part number. If data is not available, the value **0** is displayed.
- **Rack Location Discovery Product Description**—The rack product name. If data is not available, the value **0** is displayed.
- **Rack U Height**—The rack height, in U rack units. Possible values are between 0 and 50. If data is not available, the value **0** is displayed.
- **U Location**—The side of the rack where the device is installed. Possible values are **Back**, **Front** (default), **Left**, and **Right**. If data is not available, the value **0** is displayed.
- **Server UUID**—The universally unique identifier of the server.

Additional information is listed, depending on the server type.

DL and ML server-specific data

- **Server U Height**—The server height, in U rack units. Possible values are between 1.00 and 50.00.
- **Server Rack U Position**—The rack U position that aligns with the base of the server. Possible values are between 1 and 50.

Blade enclosures and BL server-specific data

- **Bay Number**—The server bay in the enclosure.
- **Enclosure UUID**—The enclosure universally unique identifier.
- **Enclosure U Height**—The enclosure height, in U rack units. Possible values are between 1.00 and 50.00.
- **Enclosure Rack U Position**—The rack U position that aligns with the base of the enclosure. Possible values are between 1 and 50.

SL and XL server-specific data:

- **Bay Number**—The server bay in the enclosure.
- **Chassis UUID**—The chassis universally unique identifier.
- **Chassis U Height**—The chassis height, in U rack units. Possible values are between 1.00 and 50.00.
- **Chassis Rack U Position**—The rack U position that aligns with the base of the chassis. Possible values are between 1 and 50.

Location Discovery Services

Location Discovery Services is a component of HPE Discovery Services. Location Discovery Services automatically reports server locations to HPE SIM and Insight Control, eliminating this manual task for server administrators. Administrators can use the location information and system data with HPE Asset Manager to obtain more precise and complete asset data.

Location Discovery Services is a rack U location discovery solution for G3 and later racks. It enables iLO, OA, and the chassis firmware to report and display the rack ID and the server U position in the rack. Supported racks are programmed with unique U values in 7U and/or 8U modules, and are installed with the tag version number, rack identifier, part number, product name, rack height, and U position. Location Discovery Services supports 14U, 22U, 36U, 42U, and 47U racks.

The rack device reads the rack U location tag each time iLO receives AC power or iLO is reset. The U position value denotes the U position read by the device. The contact position offset is a fixed value for each model that indicates the position of the contact relative to the bottom U position of the device. It is normally 0, but can be a positive value when the contact cannot be placed at the bottom U position of the device. The bottom-most U position occupied by the device is calculated by subtracting the U offset from the U position.

This feature and many others are part of a licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

Using the HPE Insight Management Agents

The Insight Management Agents support a browser interface for access to run-time management data through the HPE System Management Homepage. The System Management Homepage is a secure web-based interface that consolidates and simplifies the management of individual servers and operating systems.

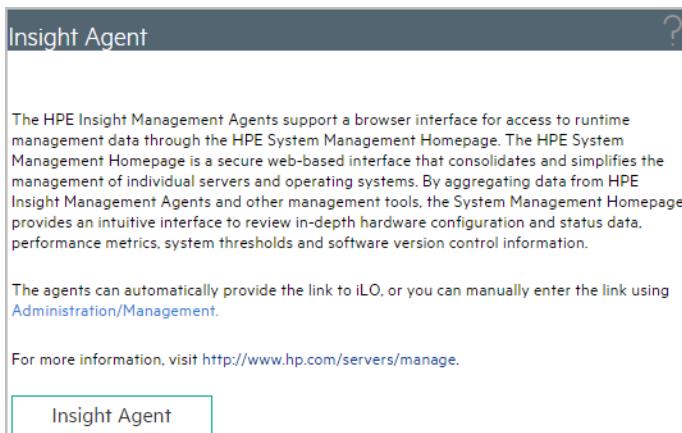
By aggregating data from the Insight Management Agents and other management tools, the System Management Homepage provides an intuitive interface to review the following:

- In-depth hardware configuration and status data
- Performance metrics
- System thresholds
- Software version control information

The agents can automatically provide the link to iLO, or you can manually enter the link on the **Administration→Management** page.

Opening the System Management Homepage

1. Navigate to the **Information→Insight Agent** page.



2. Click the **Insight Agent** button.

IPMI server management

Server management through IPMI is a standard method for controlling and monitoring the server. The iLO firmware provides server management based on the IPMI version 2.0 specification, which defines the following:

- Monitoring 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 identification of failed hardware components

IPMI communications depend on the BMC and the SMS. The BMC manages the interface between the SMS and the platform management hardware. The iLO firmware emulates the BMC functionality, and the SMS functionality can be provided by various industry-standard tools. For more information, see the IPMI specification on the Intel website at <http://www.intel.com/design/servers/ipmi/tools.htm>.

The iLO firmware provides the KCS interface, or open interface, for SMS communications. The KCS interface provides a set of I/O mapped communications registers. The default system base address for the I/O-mapped SMS interface is `0xCA2`, and it is byte aligned at this system address.

The KCS interface is accessible to the SMS software running on the local system. Examples of compatible SMS software applications follow:

- **IPMI version 2.0 Command Test Tool**—A low-level MS-DOS command-line tool that enables hex-formatted IPMI commands to be sent to an IPMI BMC that implements the KCS interface. You can download this tool from the Intel website at <http://www.intel.com/design/servers/ipmi/tools.htm>.
- **IPMItool**—A utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications. IPMItool can be used in a Linux environment. You can download this tool from the IPMItool website at <http://ipmitool.sourceforge.net/index.html>.

- **FreeIPMI**—A utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications. You can download FreeIPMI from the following website: <http://www.gnu.org/software/freeipmi/>.
- **IPMIUTIL**—A utility for managing and configuring devices that support the IPMI version 1.0, 1.5, and version 2.0 specifications. You can download IPMIUTIL from the following website: <http://ipmiutil.sourceforge.net/>

When emulating a BMC for the IPMI interface, iLO supports all mandatory commands listed in the IPMI version 2.0 specification. The SMS should use the methods described in the specification for determining which IPMI features are enabled or disabled in the BMC (for example, using the Get Device ID command).

If the server OS is running, and the iLO health driver is enabled, any IPMI traffic through the KCS interface can affect health driver performance and system health. Do not issue any IPMI commands through the KCS interface that might have a negative effect on health driver monitoring. This restriction includes any command that sets or changes IPMI parameters, such as Set Watchdog Timer and Set BMC Global Enabled. Any IPMI command that simply returns data is safe to use, such as Get Device ID and Get Sensor Reading.

Advanced IPMI tool usage on Linux

The Linux IPMI tool has the capability to securely communicate with the iLO firmware by using the IPMI 2.0 RMCP+ protocol. This is the `ipmitool lanplus` protocol feature.

For example: To retrieve the iLO Event Log, enter:

```
ipmitool -I lanplus -H <iLO ip address> -U <username> -P <password> sel list
```

Output example:

```
1 | 03/18/2000 | 00:25:37 | Power Supply #0x03 | Presence detected | Deasserted
2 | 03/18/2000 | 02:58:55 | Power Supply #0x03 | Presence detected | Deasserted
3 | 03/18/2000 | 03:03:37 | Power Supply #0x04 | Failure detected | Asserted
4 | 03/18/2000 | 03:07:35 | Power Supply #0x04 | Failure detected | Asserted
```

Using iLO with HPE Insight Control server provisioning

HPE Insight Control server provisioning is integrated with iLO to enable the management of remote servers and the performance of Remote Console operations, regardless of the state of the OS or hardware.

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

For more information about HPE Insight Control server provisioning, see the documentation on the HPE Insight Control website at <http://www.hpe.com/info/insightcontrol>.

Using Enterprise Secure Key Manager with iLO

The **Key Manager** page enables you to connect to an operational key manager, change redundancy settings, view the key manager connection settings, test the connection, and view key management events.

iLO 4.1.40 and later supports HPE Enterprise Secure Key Manager 3.1 and later, which can be used in conjunction with HPE Secure Encryption.

- HPE Secure Encryption supports HPE Smart Array controllers and provides data-at-rest encryption for direct-attached HDD or SSD storage connected to Hewlett Packard Enterprise

servers. It provides an integrated solution to encrypting HDD or SSD volumes by using 256-bit XTS-AES algorithms.

- ESKM generates, stores, serves, controls, and audits access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys.
- iLO manages the key exchange between the ESKM and the Smart Array controller. iLO uses a unique user account based on its own MAC address for communicating with the ESKM. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the ESKM with administrator privileges. For more information about the deployment user account, see the HPE Secure Encryption installation and user guide.

This feature and many others are part of a licensing package. For more information, see the following website: <http://www.hpe.com/info/ilo/licensing>.

For information about HPE Secure Encryption and ESKM, see the HPE Secure Encryption installation and user guide.

Configuring key manager servers

1. Navigate to the **Administration→Key Manager** page.

Enterprise Secure Key Manager

Key Manager Servers

Primary Key Server

Address Port

Secondary Key Server

Address Port

Require Redundancy **Apply**

Key Manager Configuration

iLO Account on ESKM

Name Group

ESKM Local CA Certificate Name

This is the name of the Local CA in ESKM that is used to sign the ESKM server certificate. iLO will retrieve this certificate from the ESKM server.

Imported Certificate Details

Issuer: Not Present

Subject: Not Present

ESKM Administrator Account

Login Name Password **Update ESKM**

Credentials are required to update ESKM servers.

Test ESKM Connections

Enterprise Secure Key Manager Events

2. Enter the following information:
 - **Primary Key Server**—The primary key server hostname, IP address, or FQDN and port. This string can be up to 79 characters long.
 - **Secondary Key Server**—The secondary key server hostname, IP address, or FQDN and port. This string can be up to 79 characters long.
3. Optional: For configurations with a primary and secondary key server, select the **Require Redundancy** check box to check for server redundancy.

Hewlett Packard Enterprise recommends enabling this option. When this option is disabled, iLO will not verify that encryption keys are copied to both of the configured key servers.
4. Click **Apply**.

Adding key manager configuration details

1. Navigate to the **Administration**→**Key Manager** page.

The listed **iLO Account on ESKM** account name is **ilo-<iLO MAC address>**. The account name is read-only and is used when iLO communicates with the ESKM.
2. Enter the following information in the **Key Manager Configuration** section:
 - **Group**—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.
 - **ESKM Local CA Certificate Name** (optional)—To ensure that iLO is communicating with a trusted ESKM server, enter the name of the local certificate authority certificate in ESKM. It is typically named **Local CA** and is listed in ESKM under Local CAs. iLO will retrieve the certificate and use it to authenticate the ESKM servers for all future transactions.
 - **Login Name**—The Local User name with administrator permissions that is configured on the ESKM. This user name is the ESKM *deployment user*.

The deployment user account must be created before you add key manager configuration details in iLO.
 - **Password**—The password for the Local User name with administrator permissions that is configured on the ESKM.
3. Click **Update ESKM**.

iLO verifies that an account named **ilo-<iLO MAC address>** exists on the ESKM. If the account exists, iLO verifies that the account password is correct. iLO generates this password automatically.

If the password is incorrect, iLO updates the password. The password might be incorrect if iLO was restored to the factory default settings.

If the account does not exist, iLO creates it.

If iLO is not a member of an ESKM Local Group, it will try to create a group with the requested name. If iLO is already a member of an ESKM Local Group, it will ignore the group entered in [Step 2](#), and will use the existing group assignment that is present on the ESKM. Attempted group changes in iLO do not affect current key group permissions that are set on the ESKM. If a new group assignment is needed, update the ESKM before updating the iLO settings.

If you entered the **ESKM Local CA Certificate Name** in [Step 2](#), certificate information is listed in the **Imported Certificate Details** section of the ESKM page.

See the Secure Encryption installation and user guide for more information about groups and their use with key management.

Testing the ESKM configuration

After the key manager configuration is complete in iLO, you can use the **Test ESKM Connections** feature to verify the configuration settings. The tests confirm that iLO and the ESKM servers are set up to provide key management services for HPE Secure Encryption. During the test, iLO attempts the following tasks:

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

To test the ESKM configuration:

1. Navigate to the **Administration→Key Manager** page.
2. Click **Test ESKM Connections**.

The test results are displayed in the **Enterprise Secure Key Manager Events** table.

Viewing ESKM events

1. Navigate to the **Administration→Key Manager** page.
2. Scroll to the **Enterprise Secure Key Manager Events** section.

Each event is listed with a time stamp and description.

Clearing the ESKM log

1. Navigate to the **Administration→Key Manager** page.
2. Click **Clear ESKM Log**.
3. When prompted to confirm the request, click **OK**.

iLO and remote management tools

iLO 4.1.30 and later allows remote management through supported tools such as HPE OneView.

The association between iLO and a remote management tool is configured by using the remote management tool. For instructions, see your remote management tool documentation.

When iLO is under the control of a remote management tool, the iLO web interface includes the following enhancements:

- A message similar to the following is displayed on the iLO login page:

This system is being managed by <remote management tool name>. Changes made locally in iLO will be out of sync with the centralized settings, and could affect the behavior of the remote management system.
- A page called <Remote Management Tool Name> is added to the iLO navigation tree.

Starting a remote management tool from iLO

When iLO is under the control of a remote management tool, use the following procedure to start the remote manager user interface from iLO.

1. Navigate to the <Remote Management Tool Name> page.
2. Click **Launch**.

The remote management tool starts in a separate browser window.

Deleting a remote manager configuration

If you discontinue the use of a remote management tool in your network, you can remove the association between the tool and iLO.

This feature is not supported on Synergy compute modules.

(!) **IMPORTANT:** Hewlett Packard Enterprise recommends that you remove the server from the remote management tool before you delete the remote manager configuration in iLO. Do not delete the remote manager configuration for a tool that is in use on the network and is managing the server that contains the current iLO system.

1. Navigate to the <Remote Management Tool Name> page.
2. Click the **Delete** button in the **Delete this remote manager configuration from this iLO** section.

A warning message similar to the following appears:

Proceed with this deletion only if this iLO is no longer under the control of <Remote Management Tool Name>.

3. Click **OK**.

The <Remote Management Tool Name> page is removed from the iLO navigation tree.

Using iLO with HPE OneView

HPE OneView interacts with the iLO management processor to configure, monitor, and manage ProLiant servers or Synergy compute modules. It configures seamless access to the iLO remote console, enabling you to launch the iLO remote console from the HPE OneView user interface in a single click. The role assigned to your appliance account determines your iLO privileges.

HPE OneView manages the following iLO settings:

- The remote management tool
- SNMP v1 trap destination
- SNMP v1 read community
- SSO certificate—A trusted certificate is added to the **Administration**→**Security**→**HPE SSO** page.
- NTP (time server) configuration
- User Account—An administrative user account is added to iLO.
- Firmware version—When you add a server to HPE OneView, the iLO firmware is updated automatically if a supported version is not already installed. For more information, see the HPE OneView support matrix.
- The appliance is added as a destination for iLO RESTful API events.
- Remote support registration

(!) **IMPORTANT:** For best performance when using HPE OneView with iLO 4, Hewlett Packard Enterprise recommends that you do not delete or change these settings by using the iLO web interface. Changing the device configuration from the iLO firmware could cause it to become out of synchronization with HPE OneView.

For more information about HPE OneView, see <http://www.hpe.com/info/oneview/docs>.

Server signatures (Synergy compute modules only)

When HPE OneView manages a Synergy compute module, iLO generates a server signature that allows HPE OneView to manage unique network settings, virtual identifiers, and adapter settings.

The server signature is refreshed and verified for compliance each time iLO starts. It includes information such as the frame bay and UUID, the HPE OneView domain IP address, and the server device signatures.

If the server is moved to a different frame or bay, or its hardware configuration changes upon insertion into a bay, the server signature changes. When this change occurs, the settings configured by HPE OneView are cleared, an event is logged in the iLO event log, and a iLO RESTful API event is generated. This process prevents duplicate addresses and helps HPE OneView ensure that the server has a unique profile.

In most cases, HPE OneView automatically rediscovers and configures the server. If this discovery and configuration does not occur, use the HPE OneView software to refresh the frame that contains the server.

The server signature data cannot be viewed or edited in the iLO web interface, but it can be read with a REST client. For more information, see <http://www.hpe.com/info/restfulinterface/docs>.

Using iLO with HPE SIM

The iLO firmware is integrated with HPE SIM in key operating environments, providing a single management console from a standard web browser. While the operating system is running, you can establish a connection to iLO by using HPE SIM.

Integration with HPE SIM provides the following:

- **Support for SNMP trap delivery to an HPE SIM console**—The HPE SIM console can be configured to forward SNMP traps to a pager or email address.
- **Support for management processors**—All iLO devices installed in servers on the network are discovered in HPE SIM as management processors.
- **Grouping of iLO management processors**—All iLO devices can be grouped logically and displayed on one page.
- **HPE Management Agents or Agentless Management**—iLO, combined with Agentless Management or the HPE Management Agents, provides remote access to system management information through the iLO web interface.
- **Support for SNMP management**—HPE SIM can access Insight Management Agent information through iLO.

HPE SIM features

HPE SIM enables you to do the following:

- Identify iLO processors.
- Create an association between an iLO processor and its server.
- Create links between an iLO processor and its server.
- View iLO and server information and status.
- Control the amount of information displayed for iLO.

The following sections summarize these features. For detailed information, see the HPE SIM user guide.

Establishing SSO with HPE SIM

1. Configure iLO for HPE SIM SSO and add HPE SIM trusted servers.

2. Log in to the HPE SIM server that you specified in [Step 1](#), and discover the iLO processor. After you complete the discovery process, SSO is enabled for iLO. For more information about HPE SIM discovery tasks, see the HPE SIM user guide.

More information

[HPE SSO](#)

iLO identification and association

HPE SIM can identify an iLO processor and create an association between iLO and a server. You can configure iLO to respond to HPE SIM identification requests by setting the **Level of Data Returned** value on the **Administration**→**Management** page. For more information, see [“Configuring Insight Management integration” \(page 124\)](#).

Viewing iLO status in HPE SIM

HPE SIM identifies iLO as a management processor. HPE SIM displays the management processor status on the **All Systems** page.

The iLO management processor is displayed as an icon on the same row as its host server. The color of the icon represents the status of the management processor.

For a list of device statuses, see the HPE SIM user guide.

iLO links in HPE SIM

For ease of management, HPE SIM creates links to the following:

- iLO and the host server from any **System(s)** list
- The server from the **System** page for iLO
- iLO from the **System** page for the server

The **System(s)** list pages display iLO, the server, and the relationship between iLO and the server.

- To display the iLO web interface, click a status icon.
- To display the **System** page of the device, click the iLO or server name.

Viewing iLO in HPE SIM System lists

iLO management processors can be viewed in HPE SIM. A user who has full configuration rights can create and use customized system collections to group management processors. For more information, see the HPE SIM user guide.

Receiving SNMP alerts in HPE SIM

You can configure iLO to forward alerts from the management agents of the host operating system and to send iLO alerts to HPE SIM.

HPE SIM supports full SNMP management. iLO supports SNMP trap delivery to HPE SIM. You can view the event log, select the event, and view additional information about the alert.

Configuring the receipt of SNMP alerts in HPE SIM:

1. To enable iLO to send SNMP traps, navigate to the **Administration**→**Management** page and configure the settings for SNMP, SNMP alerting, and Insight Management Integration. Enter the IP address of the HPE SIM computer in the **SNMP Alert Destination(s)** box.

For more information, see [“Configuring SNMP settings” \(page 116\)](#).

2. To discover iLO in HPE SIM, configure iLO as a managed device for HPE SIM.

This configuration enables the NIC interface on iLO to function as a dedicated management port, isolating management traffic from the NIC interface for the remote host server. For instructions, see the HPE SIM user guide.

For major events that are not cleared, iLO traps appear in **All Events**. To obtain more information about the event, click **Event Type**.

HPE SIM port matching

HPE SIM is configured to start an HTTP session to check for iLO at port 80. If you want to change the port number, you must change it in both iLO and HPE SIM.

- To change the port in iLO, navigate to the **Administration**→**Access Settings** page, and then enter the new port number in the **Web Server Non-SSL Port** box.
- To change the port number in HPE SIM, add the port to the `config\identification\additionalWsDisc.props` file in the HPE SIM installation directory. If iLO uses the default port (80), you do not need to edit this file.

The port entry must be on a single line with the port number first, and with all other items identical to the following example (including capitalization). This example shows the correct entry for discovering iLO at port 55000.

```
55000=iLO 4,  
,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser
```

Reviewing iLO license information in HPE SIM

HPE SIM displays the license status of the iLO management processors. You can use this information to determine how many and which iLO devices have an optional license installed.

To view license information, select **Deploy**→**License Manager**. To ensure that the displayed data is current, run the **Identify Systems** task for your management processors. For more information, see the HPE SIM user guide.

24 Kerberos authentication and Directory services

Kerberos authentication with iLO

Kerberos support enables a user to log in to iLO by clicking the **Zero Sign In** button on the login page instead of entering a user name and password. To log in successfully, the client workstation must be logged in to the domain, and the user must be a member of a directory group for which iLO is configured. If the workstation is not logged in to the domain, the user can log in to iLO by using the Kerberos UPN and domain password.

Because a system administrator establishes a trust relationship between iLO and the domain before user sign-on, any form of authentication (including two-factor authentication) is supported. For information about configuring a user account to support two-factor authentication, see the server operating system documentation.

Configuring Kerberos authentication

Process overview:

1. [Configure the iLO host name and domain name.](#)
2. [Prepare the domain controller for Kerberos support.](#)
3. [Generate a Kerberos keytab file.](#)
4. [Verify that your environment meets the Kerberos authentication time requirements.](#)
5. [Configure Kerberos support in iLO](#)
6. [Configure supported browsers for single-sign-on](#)
7. [Install an iLO Advanced license to enable Kerberos Authentication.](#)

Configuring the iLO hostname and domain name for Kerberos authentication

If a DHCP server does not supply the domain name or DNS servers you want to use:

1. Navigate to the **Network**→**iLO Dedicated Network Port** page.
2. Click the **IPv4** tab.
3. Clear the following check boxes, and then click **Submit**.
 - **Use DHCPv4 Supplied Domain Name**
 - **Use DHCPv4 Supplied DNS Servers**
4. Click the **IPv6** tab.
5. Clear the following check boxes, and then click **Submit**.
 - **Use DHCPv6 Supplied Domain Name**
 - **Use DHCPv6 Supplied DNS Servers**
6. Click the **General** tab.
7. Optional: Update the **iLO Subsystem Name (Hostname)**.
8. Update the **Domain Name**.
9. Click **Submit**.
10. Click **Reset** to restart iLO.

iLO hostname and domain name requirements for Kerberos authentication

- **Domain Name**—The iLO domain name value must match the Kerberos realm name, which is typically the domain name converted to uppercase letters. For example, if the parent domain name is `somedomain.net`, the Kerberos realm name is `SOME DOMAIN.NET`.
- **iLO Subsystem Name (Hostname)**—The configured iLO hostname must be identical to the iLO hostname that you use when you generate the keytab file. The iLO hostname is case sensitive.

Preparing the domain controller for Kerberos support

In a Windows Server environment, Kerberos support is part of the domain controller, and the Kerberos realm name is usually the domain name converted to uppercase letters.

1. Create and enable computer accounts in the domain directory for each iLO system.

Create the user account in the **Active Directory Users and Computers** snap-in. For example:

- iLO hostname: myilo
- Parent domain name: somedomain.net
- iLO domain name (fully qualified): myilo.somedomain.net

2. Ensure that a user account exists in the domain directory for each user who is allowed to log in to iLO.

3. Create universal and global user groups in the domain directory.

To set permissions in iLO, you must create a security group in the domain directory. Users who log in to iLO are granted the sum of the permissions for all groups of which they are a member. Only universal and global user groups can be used to set permissions. Domain local groups are not supported.

Generating a keytab file for iLO in a Windows environment

1. Use the `Ktpass.exe` tool to generate a keytab file and set the shared secret.

For Windows Vista only: See Microsoft hotfix KB960830 and use `Ktpass.exe` version 6.0.6001.22331 or later.

2. Optional: Use the `Setspn` command to assign the Kerberos SPN to the iLO system.

3. Optional: Use the `Setspn -L <iLO name>` command to view the SPN for the iLO system.

Verify that the `HTTP/myilo.somedomain.net` service is displayed.

More information

[Ktpass](#)

[Setspn](#)

[Error when running Setspn for iLO Kerberos configuration](#)

[Failure generating Kerberos Keytab file for iLO Zero Sign In configuration](#)

Ktpass

Syntax

`Ktpass [options]`

Description

`Ktpass` generates a binary file called the keytab file, which contains pairs of service principal names and encrypted passwords for Kerberos authentication.

Parameters

`+rndPass`

Specifies a random password.

`-ptype KRB5_NT_SRV_HST`

The principal type. Use the host service instance (KRB5_NT_SRV_HST) type.

`-princ <principal name>`

Specifies the case-sensitive principal name. For example, `HTTP/myilo.somedomain.net@SOMEDOMAIN.net`.

- The service type must use uppercase letters (`HTTP`).
- The iLO hostname must use lowercase letters (`myilo.somedomain.net`).
- The REALM name must use uppercase letters (`@SOMEDOMAIN.NET`).

`-mapuser <user account>`

Maps the principal name to the iLO system domain account.

`-out <file name>`

Specifies the file name for the `.keytab` file.

`kvno`

Override key version number.

ⓘ **IMPORTANT:** Do not use this parameter. This option causes the `knvo` in the keytab file to be out of sync with the `kvno` in Active Directory.

Example command

```
Ktpass +rndPass -ptype KRB5_NT_SRV_HST -princ
HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -mapuser myilo$@somedomain.net
-out myilo.keytab
```

Example output

```
Targeting domain controller: domaincontroller.example.net
Using legacy password setting method
Successfully mapped HTTP/iloname.example.net to iloname.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to myilo.keytab:
Keytab version: 0x502
keysize 69 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
(KRB5_NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
(0x5a5c7c18ae23559acc2 9d95e0524bf23)
```

The `Ktpass` command might display a message about not being able to set the UPN. This is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. Click **OK** to close the window and continue creating the keytab file.

Setspn

Syntax

```
Setspn [options]
```

Description

The `Setspn` displays, modifies, and deletes SPNs.

Parameters

`-A <SPN>`

Specifies an SPN to add.

`-L`

Lists the current SPN for a system.

Example command

```
SetSPN -A HTTP/myilo.somedomain.net myilo
```

The SPN components are case sensitive. The primary (service type) must be in uppercase letters, for example, (HTTP). The instance (iLO hostname) must be in lowercase letters, for example, myilo.somedomain.net.

The SetSPN command might display a message about not being able to set the UPN. This is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. Click **OK** to close the window and continue creating the keytab file.

Verifying that your environment meets the Kerberos authentication time requirement

For Kerberos authentication to function properly, the date and time must be synchronized between the iLO processor, the KDC, and the client workstation. Set the date and time in iLO with the server, or obtain the date and time from the network by enabling the SNTP feature in iLO.

Verify that the date and time of the following are set to within 5 minutes of one another:

- The iLO date and time setting
- The client running the web browser
- The servers performing the authentication

More information

[Configuring iLO SNTP settings](#)

Configuring Kerberos support in iLO

Using the iLO web interface to configure iLO for Kerberos login

1. Configure the iLO Kerberos-specific parameters.
2. Configure directory groups.

More information

[Configuring Kerberos authentication settings in iLO](#)

[Adding directory groups](#)

Using XML configuration and control scripts to configure iLO for Kerberos login

Use the following sample scripts as a template for setting the iLO parameters for directories:

- `Set_Server_Name.xml` shows how to set the iLO hostname.
- `Mod_Schemaless_Directory.xml` shows how to configure directory groups.
- `Mod_Network_Settings.xml` shows how to configure SNTP settings.
- `Mod_Kerberos_Config.xml` shows how to configure Kerberos-specific parameters.

You can download sample XML scripts from <http://www.hpe.com/support/ilo4>. For more information, see the iLO scripting and command line guide.

Using the CLI, CLP, or SSH interface to configure iLO for Kerberos login

- **iLO Hostname**—You can change the iLO hostname in the `Hostname` property of the `/map1/dnsendpt1` target.
- **Directory groups**—You can configure directory group names and permissions in the properties of the `/map1/oemhp_dircfg1` target. The group SIDs cannot be configured through this interface.

- **iLO Date/Time, SNTP Settings**—The current date and time and the SNTP settings cannot be displayed through this interface.
- **Kerberos-specific configuration parameters**—You can configure Kerberos parameters in the properties of the `oemhp_dircfg1`, `target`.

For information about configuring the iLO parameters by using the CLI, CLP, or SSH, see the iLO scripting and command line guide.

Configuring supported browsers for single sign-on

Users who are allowed to log in to iLO must be members of the groups for which permissions are assigned. For Windows clients, locking and unlocking the workstation refreshes the credentials that are used to log in to iLO. Home versions of the Windows operating system do not support Kerberos login.

The procedures in this section enable login if Active Directory is configured correctly for iLO, and iLO is configured correctly for Kerberos login.

Enabling single-sign-on in Internet Explorer

The following procedure is based on Internet Explorer 11. Other browser versions might have different steps.

Process overview:

1. [Enable authentication in Internet Explorer](#).
2. [Add the iLO domain to the Intranet zone](#).
3. [Enable the Automatic login only in Intranet zone setting](#).
4. If any options were changed in steps 1–3, close and restart Internet Explorer.
5. [Verify the single sign-on configuration](#).

Enabling authentication in Internet Explorer

1. Select **Tools**→**Internet options**.
2. Click the **Advanced** tab.
3. Scroll to the **Security** section.
4. Verify that the **Enable Integrated Windows Authentication** option is selected.
5. Click **OK**.

Adding the iLO domain to the Intranet zone

1. Select **Tools**→**Internet options**.
2. Click the **Security** tab.
3. Click the **Local intranet** icon.
4. Click the **Sites** button.
5. Click the **Advanced** button.
6. Enter the site to add in the **Add this website to the zone** box.
On a corporate network, `*.example.net` is sufficient.
7. Click **Add**.
8. Click **Close**.
9. Click **OK** to close the **Local intranet** dialog box.
10. Click **OK** to close the **Internet Options** dialog box.

Enabling the Automatic logon only in Intranet zone setting

1. Select **Tools**→**Internet options**.
2. Click the **Security** tab.

3. Click the **Local intranet** icon.
4. Click **Custom level**.
5. Scroll to the **User Authentication** section.
6. Verify that the **Automatic logon only in Intranet zone** option is selected.
7. Click **OK** to close the **Security Settings — Local Intranet Zone** window.
8. Click **OK** to close the **Internet Options** dialog box.

Enabling single-sign on in Firefox

1. Enter `about:config` in the browser location bar to open the browser configuration page. If the message `This might void your warranty!` appears, click the **I'll be careful, I promise!** button.
2. Enter `network.negotiate` in the **Search** box.
3. Double-click `network.negotiate-auth.trusted-uris`.
4. Enter the iLO DNS domain name (for example, `example.net`), and then click **OK**.
5. Test the configuration. For more information, see [“Verifying the single sign-on \(Zero Sign In\) configuration” \(page 283\)](#).

Chrome

Configuration is not required for Chrome.

Verifying the single sign-on (Zero Sign In) configuration

1. Navigate to the iLO login page (for example, `http://iloname.example.net`).
2. Click the **Zero Sign In** button.

More information

[iLO Credential prompt appears during Kerberos login attempt](#)

Verifying that login by name works

1. Navigate to the iLO login page.
2. Enter the user name in the Kerberos UPN format (for example, `user@EXAMPLE.NET`).
3. Enter the associated domain password.
4. Click **Log In**.

More information

[iLO Credential prompt appears during Kerberos login by name attempt](#)

Directory integration

Using a directory with iLO provides the following benefits:

- **Scalability**—The directory can be leveraged to support thousands of users on thousands of iLO processors.
- **Security**—Robust user-password policies are inherited from the directory. User-password complexity, rotation frequency, and expiration are policy examples.
- **User accountability**—In some environments, users share iLO accounts, which makes it difficult to determine who performed an operation.
- **Role-based administration** (HPE Extended Schema configuration)—You can create roles (for example, clerical, remote control of the host, complete control) and associate them with users or user groups. A change to a single role applies to all users and iLO devices associated with that role.

- **Single point of administration** (HPE Extended Schema configuration)—You can use native administration tools like MMC to administer iLO users.
- **Immediacy**—A single change in the directory rolls out immediately to associated iLO processors. This feature eliminates the need to script this process.
- **Simpler credentials**—You can use existing user accounts and passwords in the directory without having to record a new set of credentials for iLO.
- **Flexibility** (HPE Extended Schema configuration)—You can create a single role for a single user on a single iLO processor, a single role for multiple users on multiple iLO processors, or a combination of roles suited to your enterprise. With the HPE Extended Schema configuration, access can be limited to a time of day or a certain range of IP addresses.
- **Compatibility**—iLO directory integration supports Active Directory.
- **Standards**—iLO directory support is based on the LDAP 2.0 standard for secure directory access.

Choosing a directory configuration to use with iLO

Before you configure iLO for directories, you must choose between the schema-free and HPE Extended Schema configuration options.

Consider the following questions:

1. Can you apply schema extensions to your directory?

- **Yes**—Continue to question 2.
- **No**—You are using Active Directory, and your company policy prohibits applying extensions.

No—Directory integration with the HPE Extended Schema does not fit your environment.

Use group-based schema-free directory integration. Consider deploying an evaluation server to assess the benefits of directory integration with the HPE Extended Schema configuration.

2. Is your configuration scalable?

The following questions can help you determine whether your configuration is scalable:

- Are you likely to change the rights or privileges for a group of directory users?
- Will you regularly script iLO changes?
- Do you use more than five groups to control iLO privileges?

Depending on your answer to these questions, choose from the following options:

- **No**—Deploy an instance of the schema-free directory integration to evaluate whether this method meets your policy and procedural requirements. If necessary, you can deploy an HPE Extended Schema configuration later.
- **Yes**—Use the HPE Extended Schema configuration.

More information

[Schema-free directory authentication](#)

[HPE Extended Schema directory authentication](#)

Schema-free directory authentication

When you use the schema-free directory authentication option, users and groups reside in the directory, and group privileges reside in the iLO settings. iLO uses the directory login credentials to read the user object in the directory and retrieve the user group memberships, which are

compared to the group configuration stored in iLO. If the directory user account is verified as a member of a configured iLO directory group, iLO login is successful.

Advantages of schema-free directory integration:

- Extending the directory schema is not required.
- Minimal setup is required for users in the directory. If no setup exists, the directory uses existing users and group memberships to access iLO. For example, if you have a domain administrator named User1, you can copy the DN of the domain administrator security group to iLO and give it full privileges. User1 would then have access to iLO.

Disadvantage of schema-free directory integration

- Group privileges are administered on each iLO system. This disadvantage has minimal impact because group privileges rarely change, and the task of changing group membership is administered in the directory and not on each iLO system. Hewlett Packard Enterprise provides tools that enable you to configure many iLO systems at the same time.

Schema-free configuration options

The schema-free setup options are the same, regardless of the method you use to configure the directory. You can configure the directory settings for minimum login flexibility, better login flexibility, or maximum login flexibility.

- **Minimum login flexibility**—With this configuration, you can log in to iLO by entering your full DN and password. You must be a member of a group that iLO recognizes.

To use this configuration, enter the following settings:

- The directory server DNS name or IP address and LDAP port. Typically, the LDAP port for an SSL connection is 636.
- The DN for at least one group. This group can be a security group (for example, CN=Administrators,CN=BuiltIn,DC=HPE,DC=com for Active Directory) or any other group, as long as the intended iLO users are group members.

- **Better login flexibility**—With this configuration, you can log in to iLO by entering your login name and password. You must be a member of a group that iLO recognizes. At login time, the login name and user context are combined to make the user DN.

To use this configuration, enter the minimum login flexibility settings and at least one directory user context.

For example, if a user logs in as JOHN.SMITH, and the user context CN=USERS,DC=HPE,DC=COM, is configured, iLO uses the following DN: CN=JOHN.SMITH,CN=USERS,DC=HPE,DC=COM.

- **Maximum login flexibility**—With this configuration, you can log in to iLO by using your full DN and password, your name as it appears in the directory, the NetBIOS format (domain\login_name), or the email format (login_name@domain).

To use this configuration, configure the directory server address in iLO by entering the directory DNS name instead of the IP address. The DNS name must be resolvable to an IP address from both iLO and the client system.

Prerequisites for using schema-free directory integration

1. Install Active Directory and DNS.

2. Install the root CA to enable SSL. iLO communicates with the directory only over a secure SSL connection.
For information about using Certificate Services with Active Directory, see the Microsoft documentation.
3. Ensure that the directory DN of at least one user and the DN of a security group that contains that user are available. This information is used for validating the directory setup.
4. [Install an iLO Advanced license to enable Directory Service Authentication.](#)
5. [Verify that the correct DNS server is specified on the iLO network settings IPv4 or IPv6 page.](#)

Using the iLO web interface to configure iLO for schema-free directory integration

1. [Configure the iLO schema-free directory parameters.](#)
2. [Configure directory groups.](#)

Using XML configuration and control scripts to configure iLO for schema-free directory integration

1. Download the iLO RIBCL script samples from the following website: <http://www.hpe.com/support/ilo4>.
2. Use the `Mod_Directory.xml` file as a template for enabling directory login and specifying the directory server address.
3. Use the `Mod_Schemaless_Directory.xml` script as a template for specifying the schema-free directory settings.

Required values for the schema-free integration with Active Directory:

The following values are required in the `Mod_Directory.xml` file:

- Directory Server Address—`DIR_SERVER_ADDRESS`
- Directory Server LDAP Port—`DIR_SERVER_PORT`
- Directory User Context—`DIR_USER_CONTEXT_1`
- Enable schema-free directory integration—`DIR_ENABLE_GRP_ACCT`

The following values are required in the `Mod_Schemaless_Directory.xml` file:

- The group container in the directory—`DIR_GRPACCT1_NAME`
- iLO privileges for the group—`DIR_GRPACCT1_PRIV`
- Enable schema-free directory integration—`DIR_ENABLE_GRP_ACCT`

For more information about the scripting values, see the iLO scripting and CLI guide.

Using the CLI, CLP, or SSH interface to configure iLO for schema-free directory integration

1. Establish an ssh session to iLO and navigate to the target.

2. Use the `set` command (under `oemhp_dirauth` property) for the following directory settings values:
 - `oemhp_dirauth`—Enables or disables directory authentication.
 - `oemhp_dirsrvaddr`—Sets the directory server IP address or DNS name. The schema-free directory configuration requires a DNS name.
 - `oemhp_ldapport`—Sets the directory server port.
 - `oemhp_usercntxt1`—Sets the directory login search context 1.
 - `oemhp_group1_name`—Sets the Security group DN.
 - `oemhp_group1_priv`—Sets the group privileges.

For information about using the CLI to configure schema-free directory integration, see the iLO scripting and CLI guide.

Setting up a schema-free configuration (Directories Support for ProLiant Management Processors)

Hewlett Packard Enterprise recommends using Directories Support for ProLiant Management Processors (HPLOMIG) to configure multiple iLO processors for directories.

For more information, see [“Directories Support for ProLiant Management Processors utility \(HPLOMIG.exe\)” \(page 303\)](#).

Schema-free nested groups (Active Directory only)

Many organizations have users and administrators arranged in groups. This arrangement is convenient because you can associate a group with one or more iLO systems. You can update the configuration by adding or deleting group members.

Microsoft Active Directory supports placing one group in another group to create a nested group. In a schema-free configuration, users who are indirect members (a member of a group that is a nested group of the primary group) are allowed to log in to iLO.

HPE Extended Schema directory authentication

Using the HPE Extended Schema directory authentication option enables you to do the following:

- Authenticate users from a shared, consolidated, scalable user database.
- Control user privileges (authorization) by using the directory service.
- Use roles in the directory service for group-level administration of iLO management processors and iLO users.

Advantages of HPE Extended Schema directory integration

- Groups are maintained in the directory, not on each iLO.
- Flexible access control—Access can be limited to a time of day or a certain range of IP addresses.

Process overview: Configuring the HPE Extended Schema with Active Directory

1. Plan

Review the following:

- [Directory-enabled remote management](#)
- [Directory services schema](#)
- [Active Directory requirements for the HPE Extended Schema configuration](#)

2. **Install**

- a. **Install an iLO Advanced license to enable directory service authentication.**
- b. **Download the Directories Support for ProLiant Management Processors package and install the utilities required by your environment.**

You can install the Schema extender, snap-ins, and the Directories Support for ProLiant Management Processors utility.

- c. **Run the Schema Extender to extend the schema.**
- d. **Install the appropriate snap-ins for your directory service** on one or more management workstations.

3. **Update**

Set directory server settings and the DN of the management processor objects on the Directory Settings page in the iLO web interface.

You can also complete this step by using the Directories Support for ProLiant Management Processors software.

4. **Manage roles and objects**

- a. Use the snap-ins to create a management device object and a role object.
- b. Assign rights to the role object, as necessary, and associate the role with the management device object.
- c. Add users to the role object.

5. **Handle exceptions**

The iLO utilities are easier to use with a single role. If you plan to create multiple roles in the directory, you might need to use directory scripting utilities, like LDIFDE or VBScript utilities. These utilities create complex role associations. For more information, see **“Tools for configuring multiple iLO systems at a time” (page 302)**.

Prerequisites for configuring Active Directory with the HPE Extended Schema configuration

1. Install Active Directory and DNS.
2. Install the root CA to enable SSL. iLO communicates with the directory only over a secure SSL connection.

For information about using Certificate Services with Active Directory, see the Microsoft documentation.

iLO requires a secure connection to communicate with the directory service. This connection requires the installation of the Microsoft CA. For more information, see the Microsoft Knowledge Base Article 321051: *How to Enable LDAP over SSL with a Third-Party Certification Authority*.

3. Before you install snap-ins and schema for Active Directory, read the following Microsoft Knowledge Base article: 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed*.

Directory services support

iLO software is designed to run with the Microsoft Active Directory Users and Computers snap-in, enabling you to manage user accounts through the directory.

iLO supports Microsoft Active Directory with the HPE Extended Schema configuration.

Installing the iLO directory support software

1. Download the Directories Support for ProLiant Management Processors package from the following website: <http://www.hpe.com/support/ilo4>.

2. Install the .NET Framework 2.0 on the target server.
The .NET 2.0 Framework is used to install the Directories Support for ProLiant Management Processors software.
3. Double-click downloaded EXE file.
4. Click **Next**.
5. Select **I accept the terms in the license agreement**, and then click **Next**.
The **Directories Support** window opens.
6. In the **Directories Support** window, click **Schema Extender** to install the schema extender software.
 - a. In the Schema Extender setup wizard window, click **Next**.
 - b. In the **License Agreement** window, select **I Agree**, and then click **Next**.
 - c. In the **Select Installation Folder** window, select the installation directory and user preference, and then click **Next**.
 - d. When prompted to confirm the installation request, click **Next**.
The **Installation Complete** window opens.
7. To install the snap-ins for your console, verify that the MMC Console is closed, and then click **Snap-ins (x86)** or **Snap-ins (x64)**.
 - a. In the snap-ins setup wizard window, click **Next**.
 - b. In the **License Agreement** window, select **I Agree**, and then click **Next**.
 - c. Read the details in the Information window, and then click **Next**.
 - d. When prompted to confirm the installation request, click **Next**.
The **Installation Complete** window opens.
8. Click **Directories Support for ProLiant Management Processors** to install the Directories Support for ProLiant Management Processors software.
 - a. In the Welcome window, click **Next**.
 - b. In the **License Agreement** window, select **I Agree**, and then click **Next**.
 - c. In the **Select Installation Folder** window, select the installation directory and user preference, and then click **Next**.
 - d. When prompted to confirm the installation request, click **Next**.
The **Installation Complete** window opens.

For detailed instructions for running this tool, see [“Directories Support for ProLiant Management Processors utility \(HPLOMIG.exe\)” \(page 303\)](#).

Directories Support for ProLiant Management Processors install options

- **Schema Extender**—The `.xml` files bundled with the Schema Extender contain the schemas that are added to the directory. Typically, one of these files contains a core schema that is common to all of the supported directory services. The other files contain product-specific schemas. The schema installer requires the .NET Framework.
You cannot run the schema installer on a domain controller that hosts Windows Server Core. For security and performance reasons, Windows Server Core does not use a GUI. To use

the schema installer, you must install a GUI on the domain controller or use a domain controller that hosts an earlier version of Windows.

- **Snap-ins (x86) or Snap-ins (x64)**—The management snap-in installer installs the snap-ins required to manage iLO objects in a Microsoft Active Directory Users and Computers directory or Novell ConsoleOne directory.

iLO snap-ins are used to perform the following tasks in creating an iLO directory:

- Creating and managing the iLO objects and role objects
- Making the associations between the iLO objects and the role objects

- **Directories Support for ProLiant Management Processors**—This utility allows you to configure Kerberos authentication and Directory services with iLO.

The **HPLOMIG.exe** file, the required DLLs, the license agreement, and other files are installed in the directory **C:\Program Files (x86)\Hewlett Packard Enterprise\Directories Support for ProLiant Management Processors**. You can select a different directory. The installer creates a shortcut to Directories Support for ProLiant Management Processors on the **Start** menu.

If the installation utility detects that the .NET Framework is not installed, it displays an error message and exits.

Running the Schema Extender

1. Start the Management Devices Schema Extender from the Windows **Start** menu.
 - Windows 7 and Windows Server 2008—Click the Windows menu, and then select **All Programs**→**Hewlett-Packard**→**Management Devices Schema Extender**.
 - For Windows 8 and Windows Server 2012—Click the Windows menu, and look for the **Management Devices Schema Extender**.
 - For Windows 10—Click the Windows menu, and then select **All apps**→**Hewlett-Packard**→**Management Devices Schema Extender**.
2. Verify that **Lights Out Management** is selected, and then click **Next**.
3. Read the information in the **Preparation** window, and then click **Next**.
4. In the **Schema Preview** window, click **Next**.
5. In the **Setup** window, enter the following details:
 - Directory server type, name, and port.
 - Directory login information and SSL preferenceFor more information about these values, see “[Schema Extender required information](#)” (page 291).

The **Results** window displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Schema Extender required information

- **Directory Server**
 - **Type**—The directory server type.
 - **Name**—The directory server name.
 - **Port**—The port to use for LDAP communications.
- **Directory Login**
 - **Login Name**—A user name to log in to the directory.
A directory user name and password might be required to complete the schema extension.
When you enter credentials, use the `Administrator` login along with the domain name, for example, `Administrator@domain.com` or `domain\Administrator`.
Extending the schema for Active Directory requires a user who is an authenticated schema administrator, that the schema is not write protected, and that the directory is the FSMO role owner in the tree. The installer attempts to make the target directory server the FSMO schema master of the forest.
 - **Password**—A password to log in to the directory.
 - **Use SSL for this Session**—Sets the form of secure authentication to be used. If this option is selected, directory authentication through SSL is used. If this option is not selected and Active Directory is selected, Windows authentication is used.

Directory services objects

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and users or groups within the directory service. User management of iLO requires the following basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

After the snap-ins are installed, iLO objects and iLO roles can be created in the directory. By using the Active Directory Users and Computers tool, the user completes the following tasks:

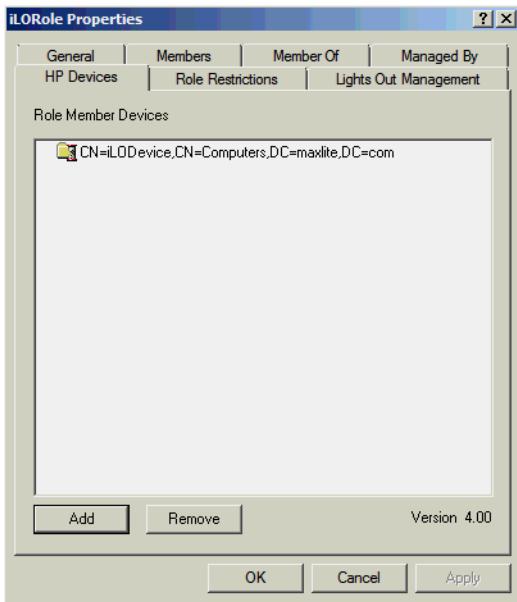
- Creates iLO and role objects
- Adds users to the role objects
- Sets the rights and restrictions of the role objects

NOTE: After the snap-ins are installed, restart ConsoleOne and MMC to show the new entries.

Managing roles and objects with the Active Directory snap-ins

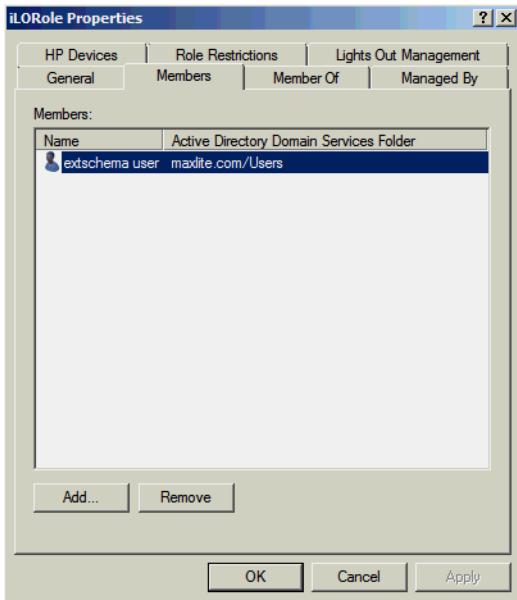
The following management options are available in Active Directory Users and Computers after you install the Hewlett Packard Enterprise snap-ins.

HP Devices tab



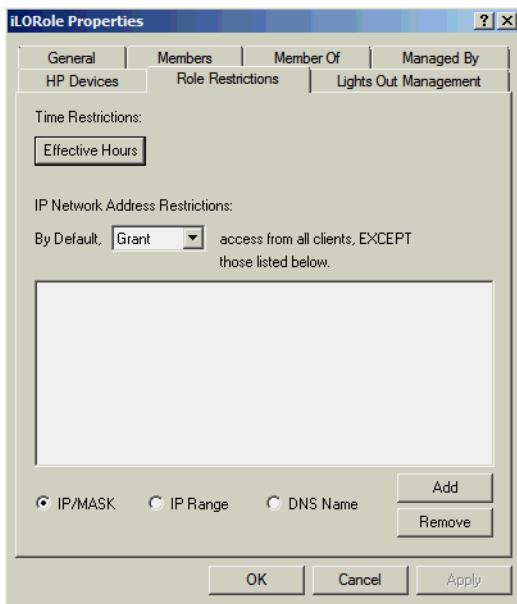
This tab enables you to add the Hewlett Packard Enterprise devices to be managed within a role. Clicking **Add** enables you to navigate to a device and add it to the list of member devices. Selecting an existing device and clicking **Remove** removes the device from the list of valid member devices.

Members tab



After user objects are created, this tab enables you to manage the users within the role. Clicking **Add** enables you to navigate to the user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.

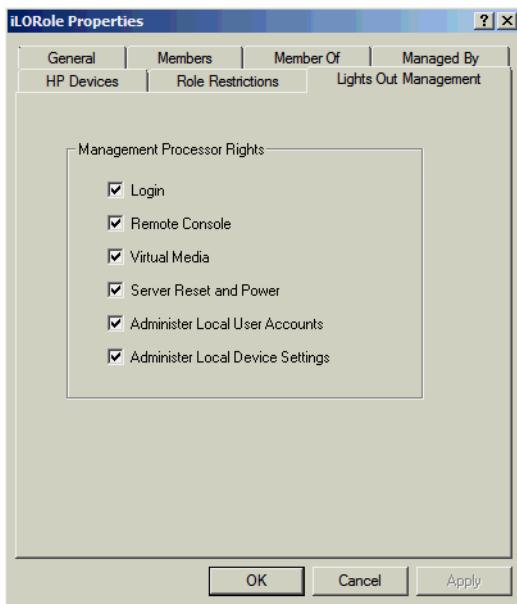
Role Restrictions tab



This tab enables you to set the following types of role restrictions:

- Time restrictions—Click **Effective Hours** to select the times available for logon for each day of the week, in half-hour increments. You can change a single square by clicking it, or you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.
- IP network address restrictions, including IP/mask, IP range, and DNS name.

Lights Out Management tab



After you create a role, use this tab to select rights for the role. You can make users and group objects members of the role, giving the users or group of users the rights granted by the role.

User rights to any iLO system are calculated as the sum of all rights assigned by all roles in which the user is a member, and in which the iLO is a managed device. Using the example in [“Creating and configuring directory objects for use with iLO in Active Directory” \(page 295\)](#), if a user is in

both the `remoteAdmins` and `remoteMonitors` roles, they will have all available rights, because the `remoteAdmins` role has all rights.

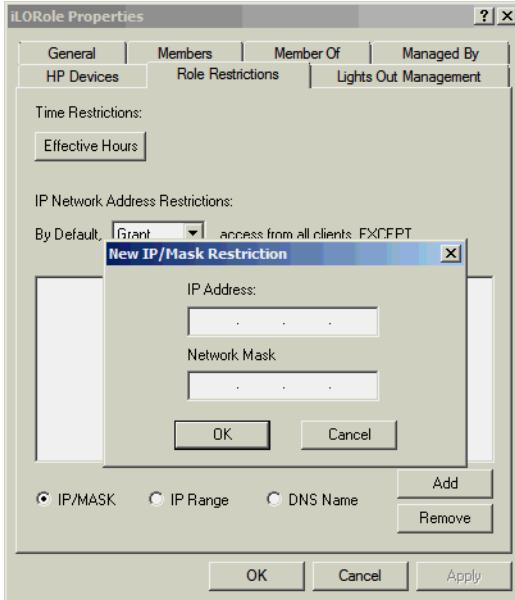
The available rights follow:

- **Login**—Controls whether users can log in to the associated devices.
- **Remote Console**—Enables users to access the iLO Remote Console.
- **Virtual Media**—Enables users to access the iLO Virtual Media feature.
- **Server Reset and Power**—Enables users to use the iLO Virtual Power button.
- **Administer Local User Accounts**—Enables users to administer user accounts. Users can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—Enables the user to configure the iLO management processor settings.

Setting a client IP address or DNS name restriction

1. From the **By Default** list on the **Role Restrictions** tab, select whether to **Grant** or **Deny** access from all addresses except the specified IP addresses, IP address ranges, and DNS names.
2. Select one of the following restriction types, and then click **Add**.
 - **DNS Name**—Allows you to restrict access based on a single DNS name or a subdomain, entered in the form of `host.company.com` or `*.domain.company.com`.
 - **IP/MASK**—Allows you to enter an IP address or network mask.
 - **IP Range**—Allows you to enter an IP address range.
3. Enter the required information in the restriction settings window, and then click **OK**.

The following example shows the **New IP/Mask Restriction** window.



4. Click **OK**.

The changes are saved, and the **iLORole Properties** dialog box closes.

Sample configuration: Active Directory and HPE Extended Schema

The following sections provide an example of how to configure Active Directory with iLO.

Configuration process overview

1. Install Active Directory and DNS.
2. Install the root CA.
3. Verify that version 2.0 or later of the .NET Framework is installed.
The iLO LDAP component requires this software.
The LDAP component does not work with a Windows Server Core installation.
4. [Install the latest Directories Support for ProLiant Management Processors software.](#)
5. [Extend the schema by using the Schema Extender.](#)
6. [Install the Hewlett Packard Enterprise LDAP component snap-ins.](#)
7. Create the Hewlett Packard Enterprise device and role.
8. Log in to iLO and enter the directory settings and directory user contexts on the **Administration**→**Security**→**Directory** page.
9. [Verify that the correct DNS server is specified on the iLO network settings IPv4 or IPv6 page.](#)

Snap-in installation and initialization for Active Directory

1. Run the snap-in installer.
2. Configure the directory service to have the appropriate objects and relationships for iLO management.

At a minimum, you must create the following:

- One role object that contains one or more users and one or more iLO objects
- One iLO object that corresponds to each iLO management processor that uses the directory
 - a. Use the management snap-ins from Hewlett Packard Enterprise to create the iLO role and user role objects.
 - b. Use the management snap-ins from Hewlett Packard Enterprise to build associations between the iLO object and the role objects.
 - c. Point the iLO object to the admin and user role objects. (Admin and user roles automatically point back to the iLO object.)

More information

[Managing roles and objects with the Active Directory snap-ins](#)
[Directory services objects](#)

Creating and configuring directory objects for use with iLO in Active Directory

The following example describes how to set up roles and Hewlett Packard Enterprise devices in an enterprise directory with the domain `testdomain.local`. This domain consists of two organizational units, **Roles** and **iLOs**. The steps in this section are completed by using the Hewlett Packard Enterprise-provided Active Directory Users and Computers snap-ins.

For more information about using the Active Directory snap-ins, see “[Managing roles and objects with the Active Directory snap-ins](#)” (page 291).

Create the iLOs organizational unit and add LOM objects

1. Create an organizational unit called **iLOs** that contains the iLO devices managed by the domain.
2. Right-click the **iLOs** organizational unit in the `testdomain.local` domain, and then select **New HP Object**.
3. Select **Device** in the **Create New Object** dialog box.

4. Enter an appropriate name in the **Name** box.

In this example, the DNS hostname of the iLO device, `rib-email-server`, is used as the name of the Lights-Out Management object.

5. Click **OK**.

Create the Roles organizational unit and add role objects

1. Create an organizational unit called **Roles**.
2. Right-click the **Roles** organizational unit, and then select **New HP Object**.
3. Select **Role** in the **Create New Management Object** dialog box.
4. Enter an appropriate name in the **Name** box.

In this example, the role contains users trusted for remote server administration and is called `remoteAdmins`.

5. Click **OK**.
6. Repeat the process, creating a role for remote server monitors called `remoteMonitors`.

Assign rights to the roles and associate the roles with users and devices

1. Right-click the `remoteAdmins` role in the **Roles** organizational unit in the `testdomain.local` domain, and then select **Properties**.
2. In the **remoteAdmins Properties** dialog box, click the **HP Devices** tab, and then click **Add**.
3. In the **Select Users** dialog box, enter the Lights-Out Management object (`rib-email-server` in folder `testdomain.local/iLOs`).
4. Click **OK**
5. Click **Apply**.
6. Click the **Members** tab, and add users by using the **Add** button.
7. Click **OK**
8. Click **Apply**.

The devices and users are now associated.

9. Click the **Lights Out Management** tab.

All users and groups within a role will have the rights assigned to the role on all of the iLO devices that the role manages.

10. Select the check box next to each right, and then click **Apply**.

In this example, the users in the `remoteAdmins` role will have full access to the iLO functionality.

11. Click **OK**.

12. Repeat the process to edit the `remoteMonitors` role as follows:

- a. Add the `rib-email-server` device to the list on the **HP Devices** tab.
- b. Add users to the `remoteMonitors` role on the **Members** tab.
- c. Select the **Login** right on the **Lights Out Management** tab.

With this right, members of the `remoteMonitors` role will be able to authenticate and view the server status.

Configure iLO and associate it with a Lights-Out Management object

Enter settings similar to the following on the **Administration**→**Security**→**Directory** page:

```
LOM Object Distinguished Name =  
cn=rib-email-server,ou=ILOs,dc=testdomain,dc=local  
Directory User Context  
1 = cn=Users,dc=testdomain,dc=local
```

Directory-enabled remote management (HPE Extended Schema configuration)

This section is for administrators who are familiar with directory services and the iLO product and want to use the HPE schema directory integration option for iLO.

Directory-enabled remote management enables you to:

- **Create Lights-Out Management objects**

You must create one LOM device object to represent each device that will use the directory service to authenticate and authorize users. You can use the Hewlett Packard Enterprise snap-ins to create LOM objects.

Hewlett Packard Enterprise recommends giving the LOM device objects meaningful names, such as the device network address, DNS name, host server name, or serial number.

- **Configure Lights-Out management devices**

Every LOM device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. In general, you can configure each device with the appropriate directory server address, LOM object DN, and user contexts. The server address is the IP address or DNS name of a local directory server or, for more redundancy, a multihost DNS name.

Roles based on organizational structure

Often, administrators in an organization are placed in a hierarchy in which subordinate administrators must assign rights independently of ranking administrators. In this case, it is useful to have one role that represents the rights assigned by higher-level administrators, and to allow subordinate administrators to create and manage their own roles.

Using existing groups

Many organizations have users and administrators arranged in groups. In many cases, it is convenient to use the existing groups and associate them with one or more LOM role objects. When the devices are associated with the role objects, the administrator controls access to the Lights-Out devices associated with the role by adding or deleting members from the groups.

When you use Microsoft Active Directory, you can place one group within another (that is, use nested groups). Role objects are considered groups and can include other groups directly. Add the existing nested group directly to the role, and assign the appropriate rights and restrictions. You can add new users to either the existing group or the role.

When you use trustee or directory rights assignments to extend role membership, users must be able to read the LOM object that represents the LOM device. Some environments require that the trustees of a role also be read trustees of the object to authenticate users successfully.

Using multiple roles

Most deployments do not require that the same user must be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can only grant rights, never revoke them. If one role grants a user a right, then the user has the right, even if the user is in another role that does not grant that right.

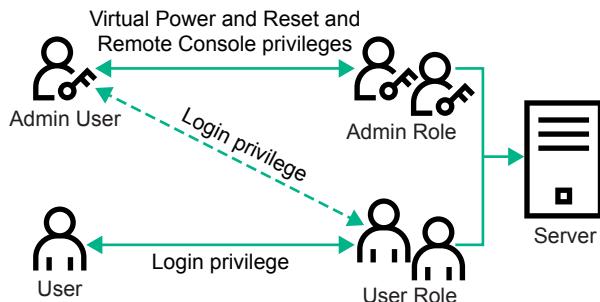
Typically, a directory administrator creates a base role with the minimum number of rights assigned, and then creates additional roles to add rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization might have two types of users: Administrators of the LOM device or host server, and users of the LOM device. In this situation, it makes sense to create two roles, one for the administrators and one for the users. Both roles include some of the same devices

but grant different rights. Sometimes it is useful to assign generic rights to the lesser role and include the LOM administrators in that role, as well as the administrative role.

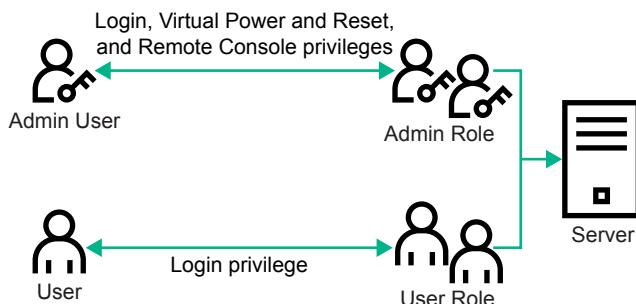
Figure 6 shows an example in which the Admin user gains the Login privilege from the User role, and advanced privileges are assigned through the Admin role.

Figure 6 Multiple roles (overlapping)



If you do not want to use overlapping roles, you could assign the Login, Virtual Power and Reset, and Remote Console privileges to the Admin role, and assign the Login privilege to the User role.

Figure 7 Multiple roles (separate)

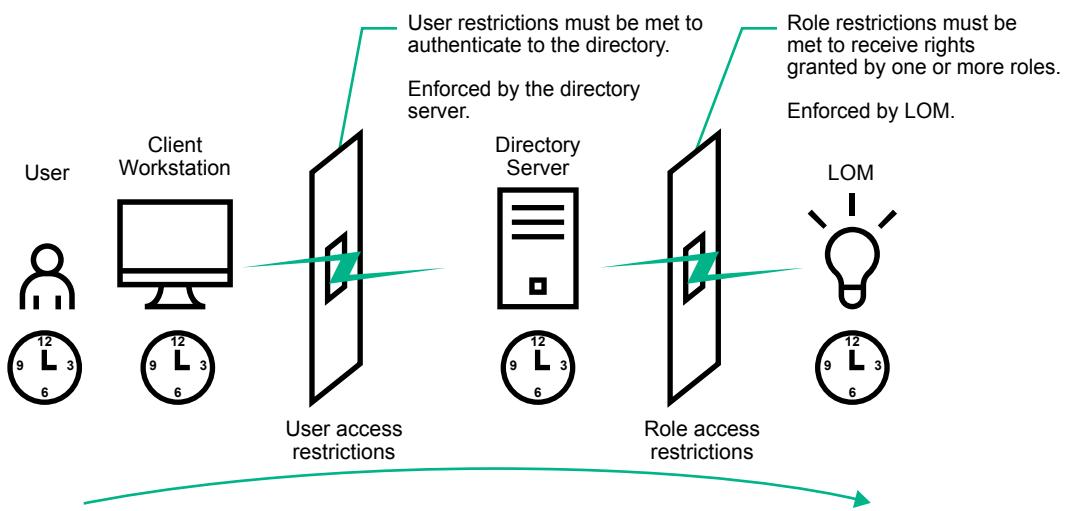


How role access restrictions are enforced

Two sets of restrictions can limit directory user access to LOM devices.

- **User access restrictions** limit user access to authenticate to the directory.
- **Role access restrictions** limit an authenticated user's ability to receive LOM privileges based on rights specified in one or more roles.

Figure 8 Directory login restrictions



User access restrictions

User address restrictions

Administrators can place network address restrictions on a directory user account. The directory server enforces these restrictions.

For information about the enforcement of address restrictions on LDAP clients, such as a user logging in to a LOM device, see the directory service documentation.

Network address restrictions placed on a user in a directory might not be enforced as expected when a directory user logs in through a proxy server. When a user logs in to a LOM device as a directory user, the LOM device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when the user accesses the LOM device. When a proxy server is used, the network address of the authentication attempt is that of the LOM device, not that of the client workstation.

IP address range restrictions

IP address range restrictions enable the administrator to specify network addresses that are granted or denied access.

The address range is typically specified in a low-to-high range format. An address range can be specified to grant or deny access to a single address. Addresses that fall within the low-to-high IP address range meet the IP address restriction.

IP address and subnet mask restrictions

IP address and subnet mask restrictions enable the administrator to specify a range of addresses that are granted or denied access.

This format is similar to an IP address range restriction, but it might be more native to your networking environment. An IP address and subnet mask range is typically specified through a subnet address and address bit mask that identifies addresses on the same logical network.

In binary math, if the bits of a client machine address, combined with the bits of the subnet mask, match the subnet address in the restriction, the client meets the restriction.

DNS-based restrictions

DNS-based restrictions use the network name service to examine the logical name of the client machine by looking up machine names assigned to the client IP addresses. DNS restrictions require a functional name server. If the name service goes down or cannot be reached, DNS restrictions cannot be matched and the client machine fails to meet the restriction.

DNS-based restrictions can limit access to a specific machine name or to machines that share a common domain suffix. For example, the DNS restriction **www.example.com** matches hosts that are assigned the domain name **www.example.com**. However, the DNS restriction ***.example.com** matches any machine that originates from the **example** company.

DNS restrictions might cause ambiguity because a host can be multihomed. DNS restrictions do not necessarily match one to one with a single system.

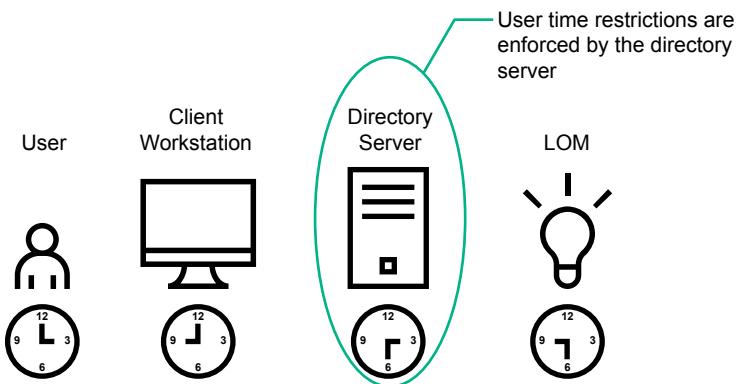
Using DNS-based restrictions might create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address restrictions, consider your organizational security policies.

User time restrictions

Time restrictions limit the ability of a user to log in (authenticate) to the directory. Typically, time restrictions are enforced using the time at the directory server. If the directory server is located in a different time zone, or if a replica in a different time zone is accessed, time-zone information from the managed object can be used to adjust for relative time.

The directory server evaluates user time restrictions, but the determination might be complicated by time-zone changes or the authentication mechanism.

Figure 9 User time restrictions



Role access restrictions

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users who have dynamic rights that can change based on the time of day or network address of the client.

When directories are enabled, access to an iLO system is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO.

To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC to view the **Security** tab.

Role-based time restrictions

Administrators can place time restrictions on LOM roles. Users are granted the rights specified for the LOM devices listed in the role only if they are members of the role and meet the time restrictions for the role.

Role-based time restrictions can be met only if the time is set on the LOM device. LOM devices use local host time to enforce time restrictions. If the LOM device clock is not set, the role-based

time restriction fails unless no time restrictions are specified for the role. The time is normally set when the host is booted.

The time setting can be maintained by configuring SNTP, which allows the LOM device to compensate for leap years and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing LOM firmware, can cause the LOM device clock not to be set. The host time must be correct for the LOM device to preserve the time setting across firmware flashes.

Role-based address restrictions

The LOM firmware enforces role-based address restrictions based on the client IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

Address restrictions can be difficult to manage when access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

Multiple restrictions and roles

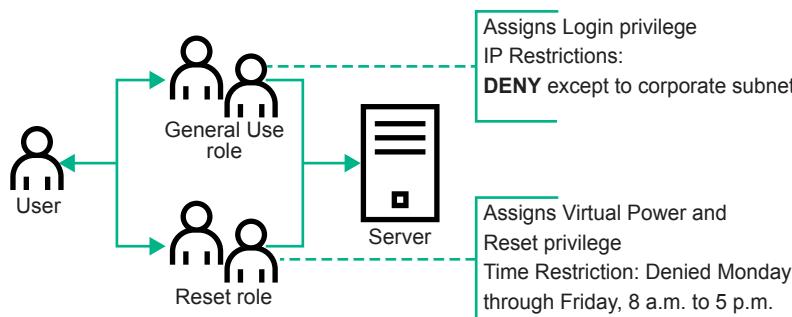
The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which LOM administrators are allowed to use the LOM device from within the corporate network, but can reset the server only after regular business hours.

Directory administrators might be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to after hours might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

[Figure 10 \(page 301\)](#) shows a security policy that dictates that general use is restricted to clients in the corporate subnet, and server reset capability is restricted to after hours.

Figure 10 Creating restrictions and roles

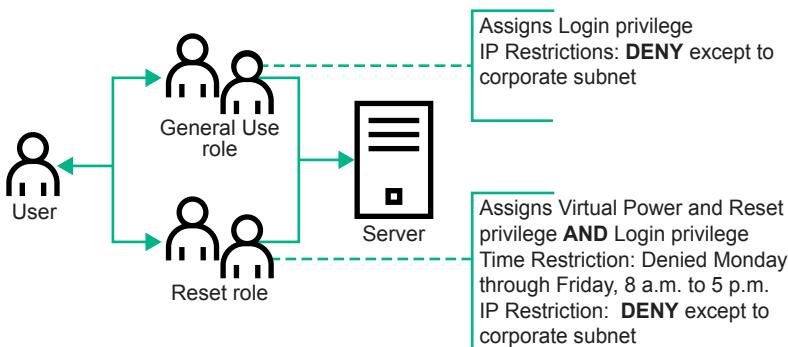


Alternatively, the directory administrator might create a role that grants the login right and restrict it to the corporate network, and then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration might create another role that grants the login right to users from addresses outside the corporate network. This role might unintentionally grant the LOM administrators in the server reset role the ability to reset the server from anywhere, if they satisfy the role time constraints.

The configuration shown in [Figure 10](#) meets corporate security requirements. However, adding another role that grants the login right can inadvertently grant server reset privileges from outside

the corporate subnet after hours. A more manageable solution is to restrict the Reset role and the General Use role, as shown in [Figure 11 \(page 302\)](#).

Figure 11 Restricting the Reset and General Use roles



Tools for configuring multiple iLO systems at a time

Configuring large numbers of LOM objects for Kerberos authentication and directory services is time consuming. You can use the following utilities to configure several LOM objects at a time.

- **Directories Support for ProLiant Management Processors**—This software includes a GUI that provides a step-by-step approach to configuring Kerberos authentication and directory services with large numbers of management processors. Hewlett Packard Enterprise recommends using this tool when you want to configure several management processors. For more information, see [“Directories Support for ProLiant Management Processors utility \(HPLOMIG.exe\)” \(page 303\)](#).
- **Traditional import utilities**—Administrators familiar with tools such as LDIFDE or the NDS Import/Export Wizard can use these utilities to import or create LOM device directory objects. Administrators must still configure the devices manually, but can do so at any time. Programmatic or scripting interfaces can be used to create LOM device objects in the same way as users or other objects. For information about attributes and attribute data formats when you are creating LOM objects, see [“Directory services schema” \(page 365\)](#).

User login using directory services

The **Login Name** box on the iLO login page accepts directory users and local users.

The maximum length of the login name is 39 characters for local users and 127 characters for directory users.

When you connect through the diagnostics port (on servers that support this feature), Zero Sign In and directory user login are not supported and you must use a local account.

- **Directory users**—The following formats are supported:

- LDAP fully distinguished names (Active Directory)

Example: CN=John Smith,CN=Users,DC=HPE,DC=COM, or @HPE.com

The short form of the login name does not notify the directory which domain you are trying to access. Provide the domain name or use the LDAP DN of your account.

- DOMAIN\user name format (Active Directory)

Example: HPE\jsmith

- username@domain format (Active Directory)

Example: jsmith@hpe.com

Directory users specified using the @ searchable form might be located in one of three searchable contexts, which are configured on the **Security→Directory** page.

- Username format (Active Directory)

Example: John Smith

Directory users specified using the username format might be located in one of three searchable contexts, which are configured on the **Security→Directory** page.

- **Local users**—Enter the Login Name of your iLO local user account.

Directories Support for ProLiant Management Processors utility (HPLOMIG.exe)

The Directories Support for ProLiant Management Processors software (HPLOMIG.exe) is available from the following website: <http://www.hpe.com/support/ilo4>.

This software is for customers who want to simplify the migration of iLO processors to management by directories. The software automates some of the steps necessary for the management processors to support directory services.

HPLOMIG.exe can do the following:

- Discover management processors on the network.
- Upgrade the management processor firmware.
- Name the management processors to identify them in a directory.
- Create objects in the directory that correspond to each management processor, and associate them with a role.
- Configure the management processors to enable them to communicate with the directory.

If enhanced security features, such as **FIPS mode** and **Enforce AES/3DES Encryption**, are enabled on the iLO systems to be configured with HPLOMIG, the HPLOMIG client must meet the following requirements:

- Windows .NET Framework v4.5 is installed.
- The operating system supports TLS v1.1 or v1.2.

The following table lists the OS and Windows .NET Framework requirements for using HPLOMIG:

Operating system	Windows .NET Framework	HPLOMIG with AES/3DES encryption and FIPS mode disabled in iLO	HPLOMIG with AES/3DES encryption or FIPS mode enabled in iLO
Windows Vista	4.0 or earlier	Supported	Not Supported
Windows Server 2008 ¹	4.5	Supported	Not Supported
Windows 7	4.0 or earlier	Supported	Not Supported
Windows Server 2008 R2	4.5	Supported	Supported
Windows 8	4.0 or earlier	Supported	Not Supported
Windows 8.1	4.5	Supported	Supported
Windows Server 2012			
Windows Server 2012 R2			
Microsoft Windows Server 2016 - Server Core and Server with a Desktop			

¹ Windows Vista and Windows Server 2008 do not support TLS v1.1 or v1.2, even if the .NET Framework version 4.5 is installed.

Directories Support for ProLiant Management Processors Compatibility

The Directories Support for ProLiant Management Processors utility operates on Microsoft Windows and requires the Microsoft .NET Framework v3.5 or later. The utility supports the following operating systems:

- Windows Server 2008 32-bit, 64-bit
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Microsoft Windows Server 2016 - Server Core and Server with a Desktop
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

Configuring directory authentication with HPLOMIG

1. Discover the iLO management processors on the network.
2. Optional: Update the iLO firmware on the management processors.
3. Specify the directory configuration settings.
4. Depending on your configuration, do one of the following:
 - Name the management processors and then Configure the directory (HPE Extended Schema only)
 - Configure the management processors to use the default schema (Schema-free only)
5. Depending on your configuration:
 - Configure extended schema settings
 - Configure schema-free settings
6. Configure directory objects (HPE Extended Schema only)
7. Configure communication between iLO and the directory.

Discovering management processors

1. Select **Start**→**All Programs**→**Hewlett Packard Enterprise**→**Directories Support for ProLiant Management Processors**.
2. On the **Welcome** page, click **Next**.
3. In the **Find Management Processors** window, enter the management processor search criteria in the **Addresses** box.

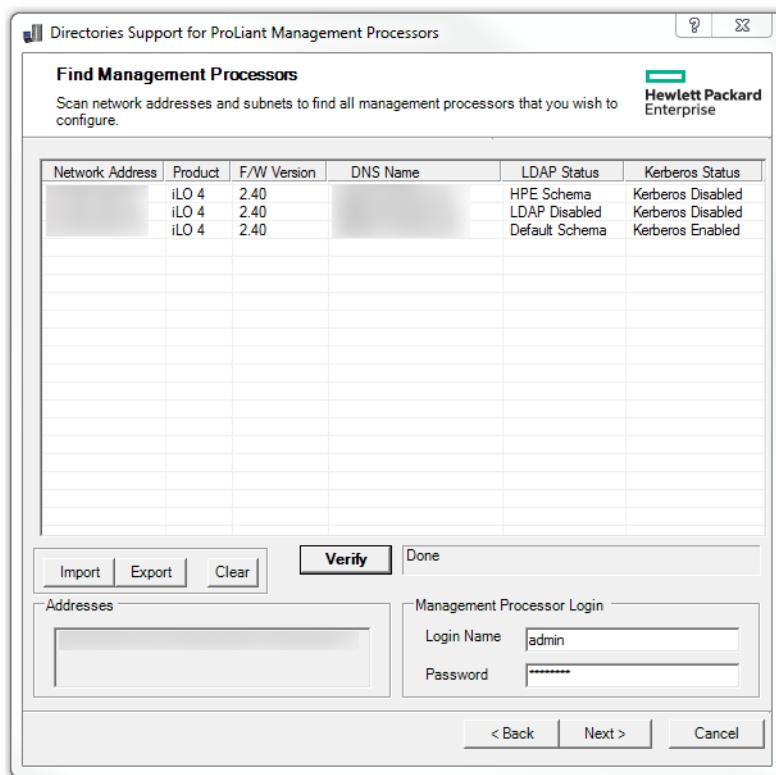


TIP: You can also enter a list of management processors from a file by clicking **Import** and then selecting the file.

4. Enter an iLO login name and password, and then click **Find**.

If you click **Next**, click **Back**, or exit the utility during discovery, operations on the current network address are completed, but operations on subsequent network addresses are canceled.

When the search is complete, the management processors are listed and the **Find** button changes to **Verify**.



More information

[HPLOMIG management processor search criteria](#)

[HPLOMIG management processor import list requirements](#)

HPLOMIG management processor search criteria

You can search for management processors by using DNS names, IP addresses, or IP address wildcards.

The following rules apply when you enter values in the **Addresses** box:

- DNS names, IP addresses, and IP address wildcards must be delimited either with semicolons or commas, not both.
- The IP address wildcard uses the asterisk (*) character in the third and fourth octet fields. For example, IP address 16.100.*.* is valid, and IP address 16.*.*.* is invalid.
- Ranges can be specified by using a hyphen. For example, 192.168.0.2-10 is a valid range. A hyphen is supported only in the rightmost octet.
- After you click **Find**, HPLOMIG begins pinging and connecting to port 443 (the default SSL port) to determine whether the target network address is a management processor. If the device does not respond to the ping or connect appropriately on port 443, the utility determines that it is not a management processor.

HPLOMIG management processor import list requirements

You can import a simple text file with one management processor listed on each line.

The supported columns, which are delimited with semicolons, follow:

- Network Address
- Product
- F/W Version
- DNS Name
- TPM Status
- User Name
- Password
- LDAP Status
- Kerberos Status
- License Type

For example, one line in the text file might have the following information:

```
16.100.225.20;iLO;1.10;ILOTPilot2210;Not Present;user;password;Default Schema;Kerberos Disabled;iLO Advanced
```

If, for security reasons, the user name and password cannot be included in the file, leave these columns blank, but enter the semicolons.

Optional: Upgrading firmware on management processors (HPLOMIG)

After you click **Next** in the **Find Management Processors** window, the next task is to update the iLO firmware, if needed. The upgrade process might take a long time, depending on the number of selected management processors. The firmware upgrade of a single management processor might take up to 5 minutes to complete.

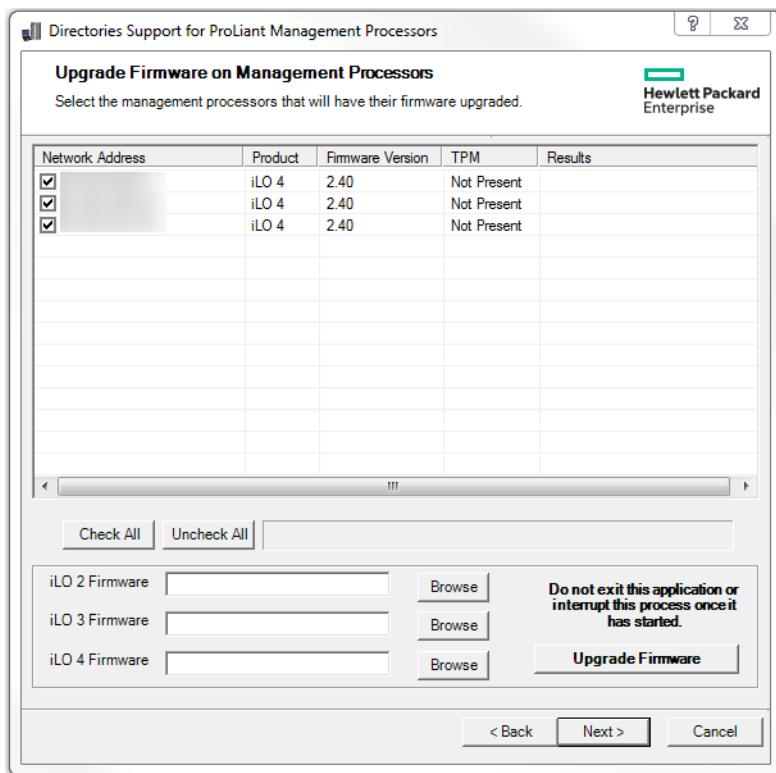
① **IMPORTANT:** Hewlett Packard Enterprise recommends that you test the upgrade process and verify the results in a test environment before running HPLOMIG on a production network. An incomplete transfer of the firmware image to a management processor might result in the need to reprogram the management processor locally.

Prerequisites

Binary images of the firmware for the management processors must be accessible from the system that is running HPLOMIG. These binary images can be downloaded from <http://www.hpe.com/support/ilo4>.

Upgrading firmware

1. Navigate to the **Upgrade Firmware on Management Processors** window if it is not already open.



2. Select the management processors to upgrade.
3. For each selected management processor, click **Browse**, and then select a firmware image file. You can also manually enter the path to the firmware image.
4. Click **Upgrade Firmware**.

The selected management processors are upgraded. Although HPLOMIG enables you to upgrade hundreds of management processors, only 25 management processors are upgraded simultaneously. Network activity is considerable during this process.

If an upgrade fails, a message is displayed in the **Results** column, and the utility continues to upgrade the other selected management processors.

During the firmware upgrade process, all buttons are deactivated to prevent navigation.

5. After the upgrade is complete, click **Next**.

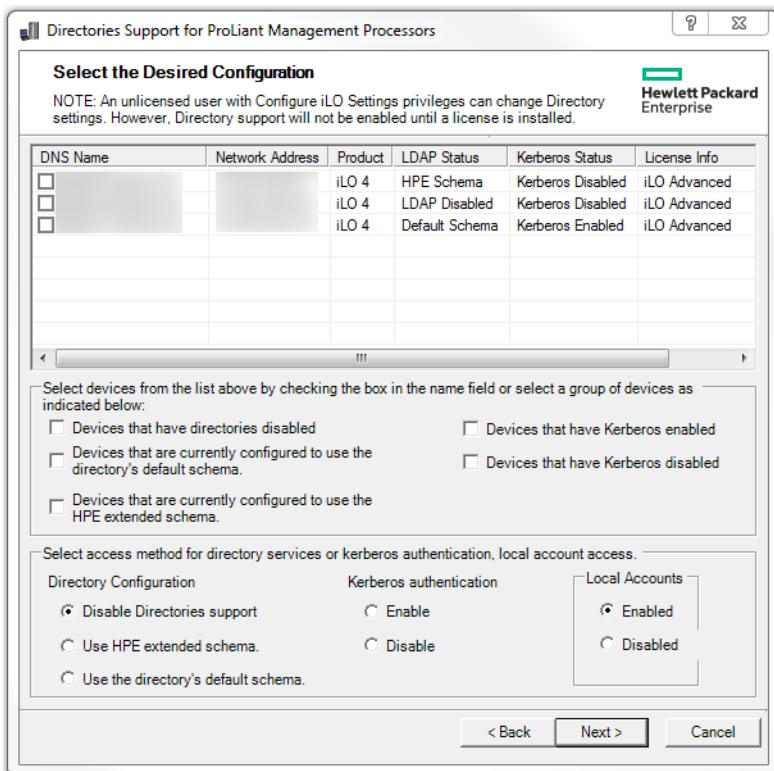
More information

[Obtaining the iLO firmware image file](#)

Selecting directory configuration options

After you click **Next** in the **Upgrade Firmware on Management Processors** window, the next task is to select the management processors to configure, and to specify the directory options to enable.

1. Navigate to the **Select the Desired Configuration** window if it is not already open.



2. Select the iLO management processors to configure.

The selection filters help to prevent an accidental overwrite of iLOs that are already configured for HPE schema, or iLOs that have directories disabled.

3. Select the directory, Kerberos, and local account settings in the **Directory Configuration**, **Kerberos authentication**, and **Local accounts** sections.

4. Click **Next**.

The selections you make on this page determine the windows that are displayed when you click **Next**.

5. If you selected a schema free configuration, skip to “[Configuring management processors \(Schema-free configuration only\)](#)” (page 315). If you selected an HPE Extended Schema configuration, continue to “[Naming management processors \(HPE Extended Schema only\)](#)” (page 309).

More information

[Management processor selection methods](#)

[Directory access methods and settings](#)

[Configuring Kerberos authentication settings in iLO](#)

[Configuring schema-free directory settings in iLO](#)

[Configuring HPE Extended Schema directory settings in iLO](#)

Management processor selection methods

Use the following methods to select iLO management processors to configure:

- Click the check box next to each management processor in the list that you want to configure.
- To select iLO management processors that match a specific status, click the check box next to any of the following filters:
 - **Devices that have directories disabled**
 - **Devices that are currently configured to use the directory's default schema**
 - **Devices that are currently configured to use the HPE Extended Schema**
 - **Devices that have Kerberos enabled**
 - **Devices that have Kerberos disabled**

Directory access methods and settings

- **Disable Directories support**—Disable directory support on the selected systems.
- **Use HPE Extended Schema**—Use a directory with the HPE Extended Schema with the selected systems.
- **Use Directory's default schema**—Use a schema-free directory with the selected systems.
- **Kerberos authentication**—Enable or disable Kerberos authentication on the selected systems.
- **Local Accounts**—Enable or disable local user accounts on the selected systems.

More information

[Kerberos settings](#)

[Schema-free directory settings](#)

[HPE Extended Schema directory settings](#)

Naming management processors (HPE Extended Schema only)

After you click **Next** in the **Select the Desired Configuration** window, the next task is to name the iLO management device objects in the directory.

You can create names by using one or more of the following:

- The network address
- The DNS name
- An index
- Manual creation of the name
- The addition of a prefix to all
- The addition of a suffix to all

To name the management processors, click the **Object Name** column and enter the name, or do the following:

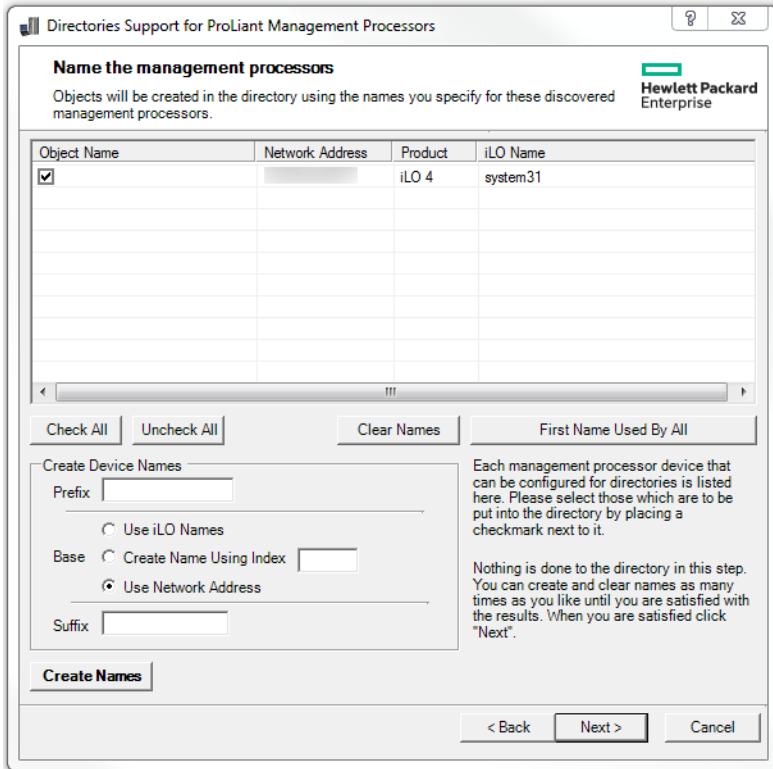
1. Select **Use iLO Names**, **Create Name Using Index**, or **Use Network Address**.
2. Optional: Enter the suffix or prefix text you want to add to all names.

3. Click **Create Names**.

The names appear in the **Object Name** column as they are generated. At this point, names are not written to the directory or the management processors. The names are stored until the next Directories Support for ProLiant Management Processors window is displayed.

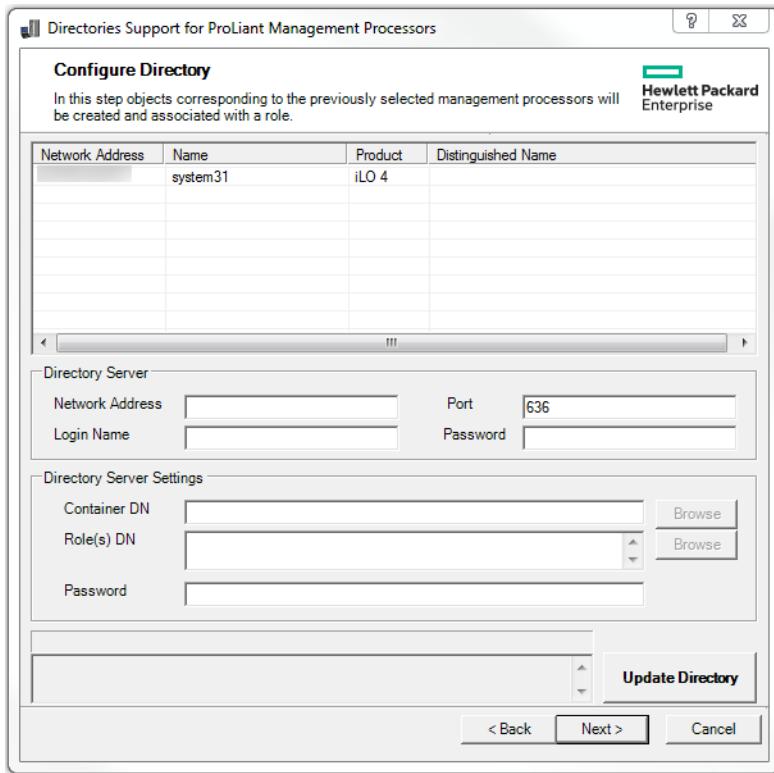
4. Optional: To change the names, click **Clear Names**, and rename the management processors.

5. When the names are correct, click **Next**.



Configuring directories when HPE Extended Schema is selected

The **Configure Directory** window enables you to create a device object for each discovered management processor and to associate the new device object with a previously defined role. For example, the directory defines a user as a member of a role (such as administrator) who has a collection of privileges on a specific device object.

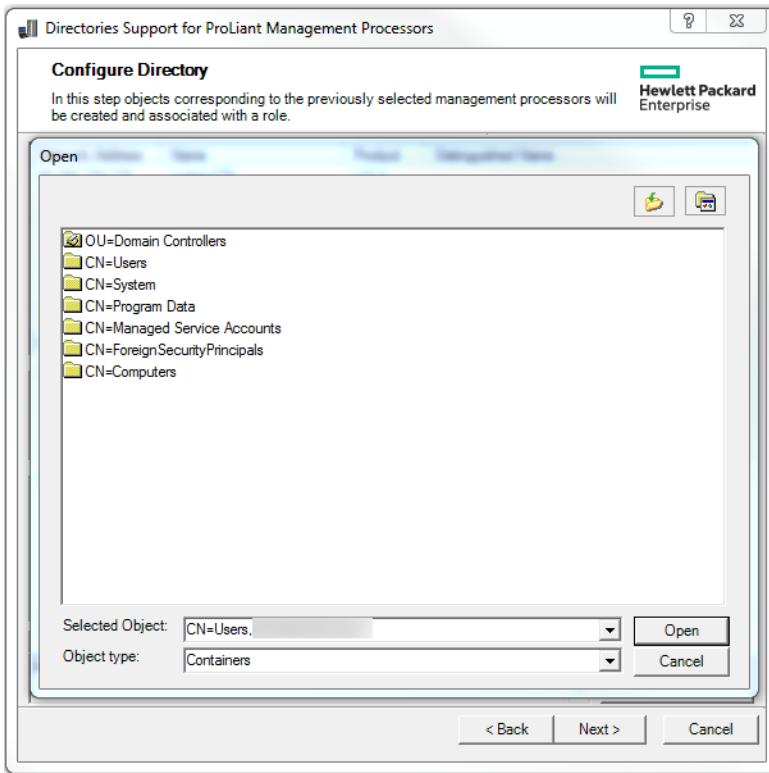


The boxes on the **Configure Directory** window follow:

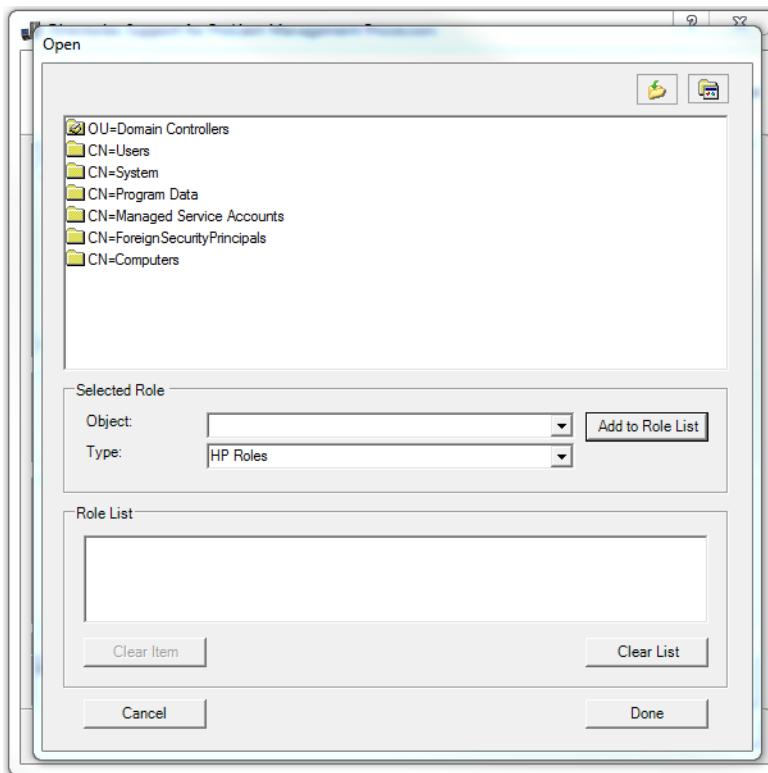
- **Network Address**—The network address of the directory server, which can be a valid DNS name or IP address.
- **Port**—The SSL port to the directory. The default port is 636. Management processors can communicate with the directory only by using SSL.
- **Login Name** and **Password**—Enter the login name and password for an account that has domain administrator access to the directory.
- **Container DN**—After you have the network address, port, and login information, you can click **Browse** to search for the container DN. The container is where the migration utility will create the management processor objects in the directory.
- **Role(s) DN**—After you have the network address, port, and login information, you can click **Browse** to search for the role DN. The role is where the role to be associated with the device objects resides. The role must be created before you run this utility.

To configure the device objects to be associated with a role:

1. Enter the network address, login name, and password for the designated directory server.
2. Enter the container DN in the **Container DN** box, or click **Browse** to select a container DN.



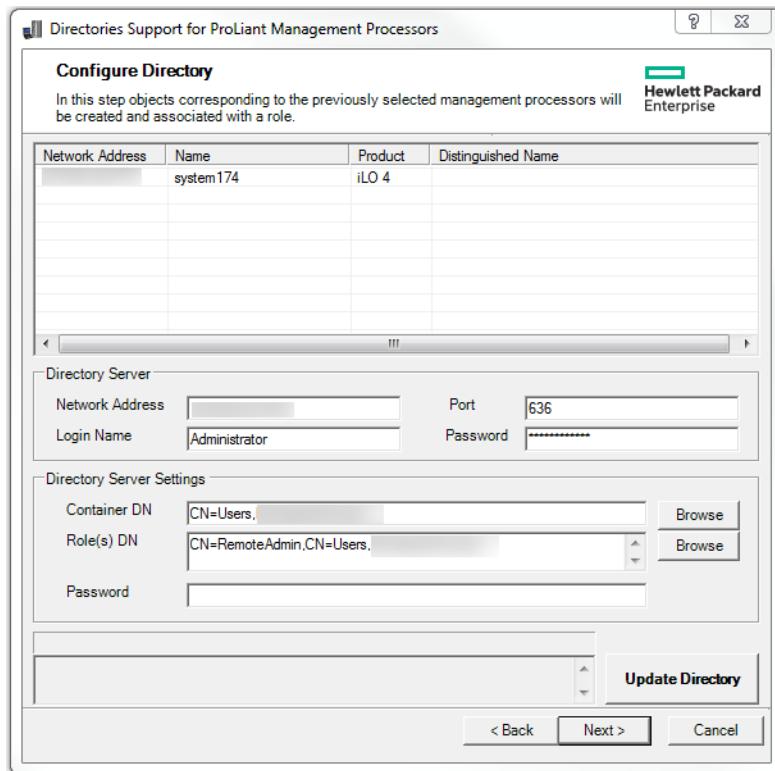
3. Associate device objects with a member of a role by entering the role DN in the **Role(s) DN** box, or click **Browse** to select a role DN.



4. Click **Update Directory**.

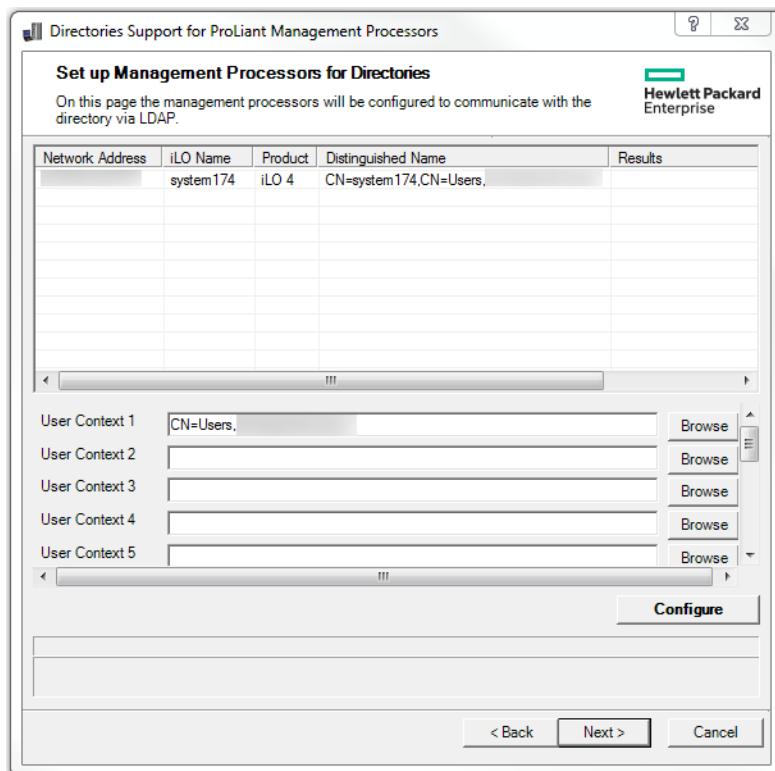
The utility connects to the directory, creates the management processor objects, and adds them to the selected roles.

5. After the device objects have been associated with a role, click **Next**.
 The values you entered are displayed in the **Configure Directory** window.

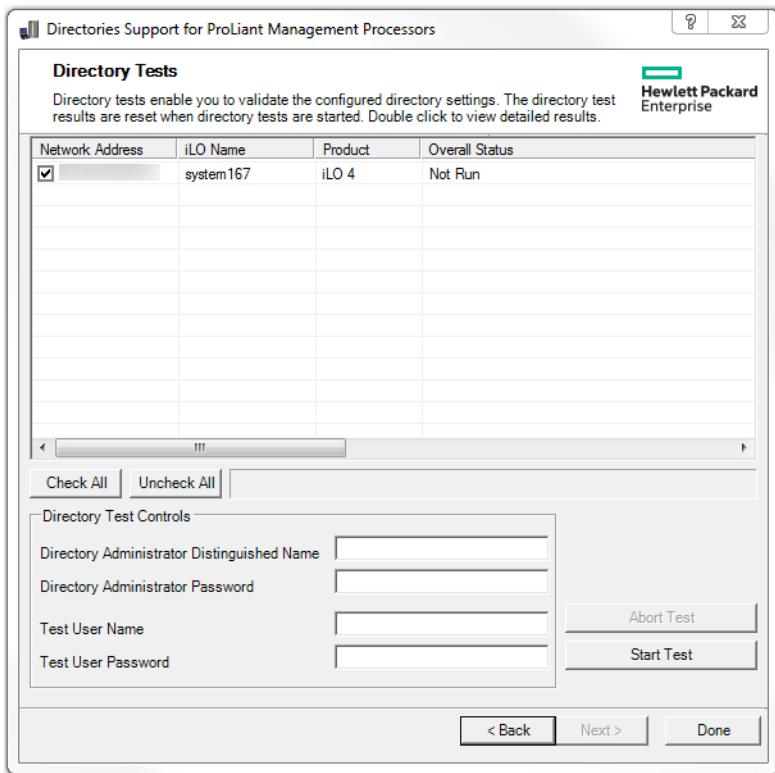


6. Define the user contexts.

The user contexts define where the users who will log in to iLO are located in the LDAP structure. You can enter the organizational unit DN or click **Browse** to select user contexts.



7. Click **Configure**, and then click **Next** when the button is available.

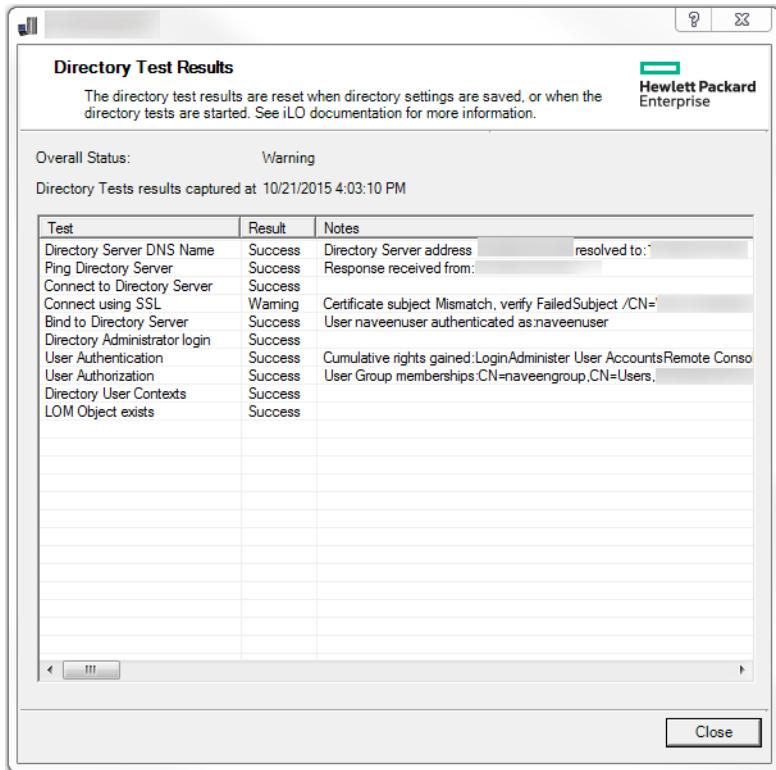


8. Optional: Test the directory settings.

This feature is supported with HPLOMIG 4.80 and later, and iLO 4 2.40 and later.

- Select one or more iLO systems.
- In the **Directory Test Controls** section, enter the following:
 - Directory Administrator Distinguished Name and Directory Administrator Password**—Searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.
Hewlett Packard Enterprise recommends that you use the same credentials that you used when creating the iLO objects in the directory. iLO does not store these credentials; they are used to verify the iLO object and user search contexts.
 - Test User Name and Test User Password**—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.
Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. iLO does not store these credentials.
- Click **Start Test**.
Several tests begin in the background, starting with a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

- To view the individual test results, double-click an iLO system in the list.



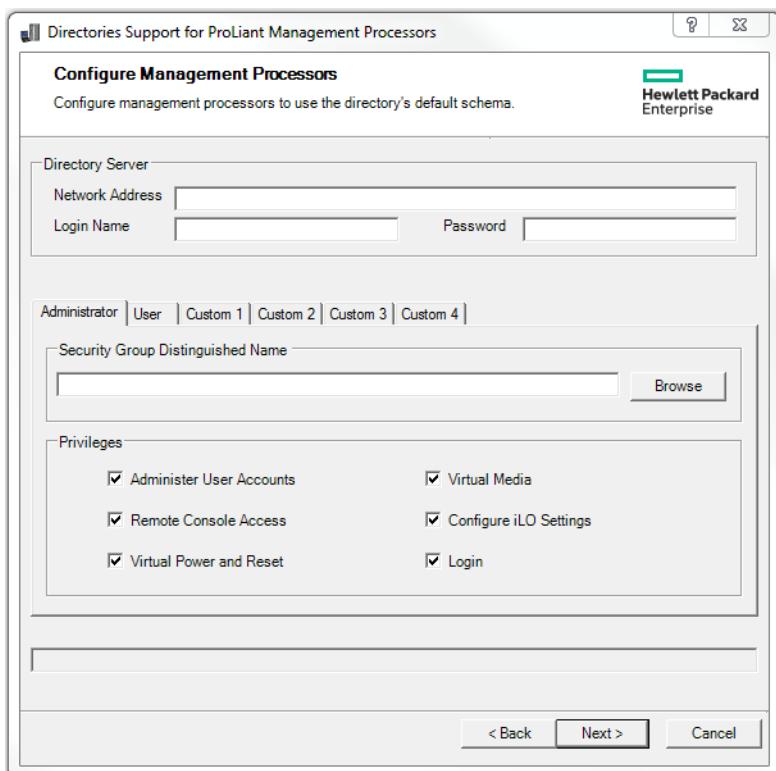
For more information, see [“Running directory tests” \(page 81\)](#).

10. Click **Done**.

Configuring management processors (Schema-free configuration only)

After you click **Next** in the **Select the Desired Configuration** window, the next task is to configure the selected management processors to use the default directory schema.

1. Navigate to the **Configure Management Processors** window if it is not already open.



2. Enter the directory server settings.
3. Enter the security group DN.
4. Select the iLO privileges you want to associate with the security group.
5. Click **Next**.

More information

Management processor settings

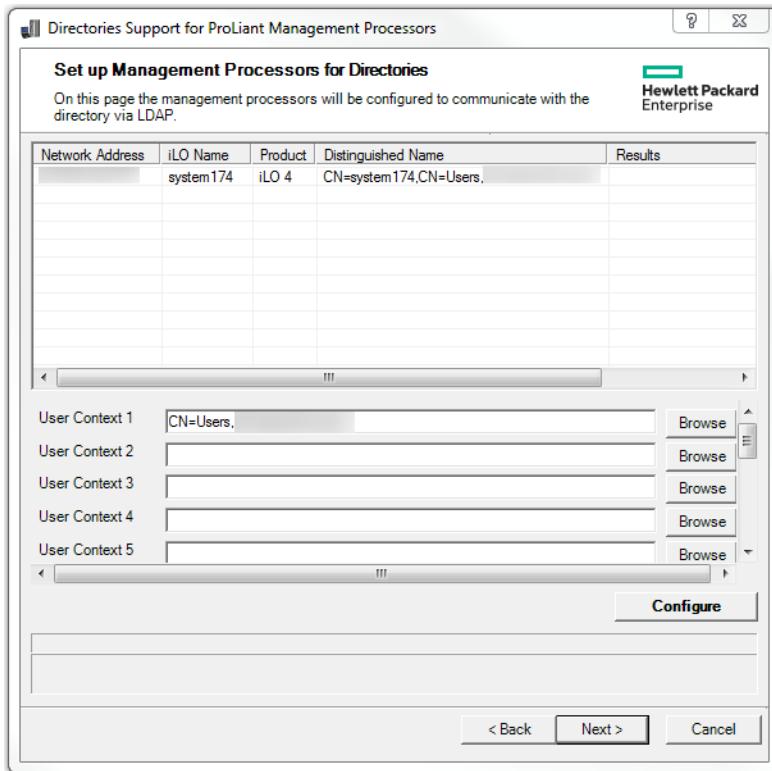
Management processor settings

- **Network Address**—The network address of the directory server, which can be a valid DNS name or IP address.
- **Login Name and Password**—Enter the login name (DN) and password for an account that has domain administrator access to the directory.
- **Security Group Distinguished Name**—The DN of the group in the directory that contains a set of iLO users with a common set of privileges. If the directory name, login name, and password are correct, you can click **Browse** to navigate to and select the group.
- **Privileges**—The iLO privileges associated with the selected group. If the user is a member of the group, the login privilege is implied.

Setting up management processors for directories

After you click **Next** in the **Name Management Processors** or **Configure Management Processors** window, the next step is to set up the management processors to communicate with the directory.

1. Navigate to the **Set up Management Processors for Directories** window if it is not already open.

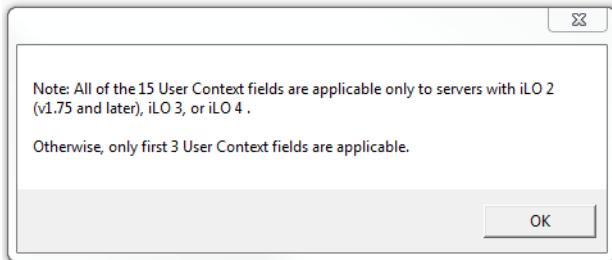


2. Enter the user contexts, or click **Browse**, and then select an OU.
Up to 15 user contexts are supported.

3. Click **Configure**.

The migration utility connects to the selected management processors, and updates their configurations as specified.

When you click **Configure**, the utility might display a message similar to the following:



4. Click **OK**.

5. When the process is complete, click **Next** to open the **Directory Tests** screen.

6. Optional: Test the directory settings.

This feature is supported with HPLOMIG 4.80 and later, and iLO 4 2.40 and later.

a. Select one or more iLO systems.

b. In the **Directory Test Controls** section, enter the following:

- **Directory Administrator Distinguished Name** and **Directory Administrator Password**—Searches the directory for iLO objects, roles, and search contexts. This user must have the right to read the directory.

Hewlett Packard Enterprise recommends that you use the same credentials that you used when creating the iLO objects in the directory. iLO does not store these credentials; they are used to verify the iLO object and user search contexts.

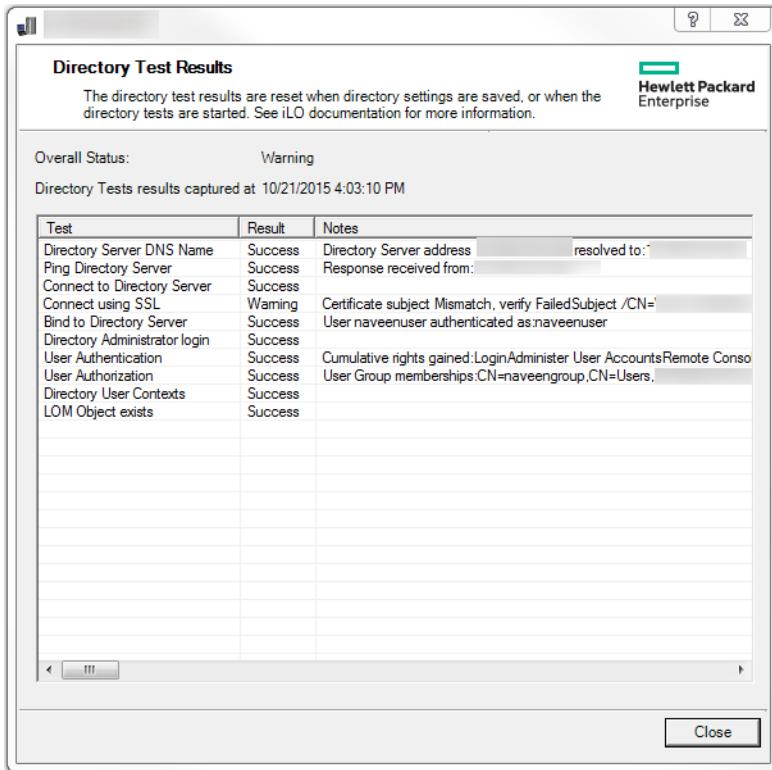
- **Test User Name** and **Test User Password**—Tests login and access rights to iLO. This name does not need to be fully distinguished because user search contexts can be applied. This user must be associated with a role for this iLO.

Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. iLO does not store these credentials.

c. Click **Start Test**.

Several tests begin in the background. The first test is a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

7. To view the individual test results, double-click an iLO system.



For more information, see [“Running directory tests” \(page 81\)](#).

8. Click **Done**.

More information

[Directory user contexts](#)

25 Troubleshooting

Using the iLO Virtual Serial Port with Windbg

If you want to debug a server, you can use the iLO Virtual Serial Port feature with the Windows Windbg kernel debugger running on a local test system.

Prerequisites

PuTTY is installed on the local test system.

You can download PuTTY from the following website: <http://www.putty.org/>.

Debugging a server

1. Using the iLO web interface of the server with kernel issues, navigate to the **Administration**→**Access Settings** page, and configure the **Serial Command Line Interface Speed**.
The default value is 9600.
2. Configure the debug options in Windows (the `boot.ini` parameters for the serial connection). Use `debugport=com2`, and set the baud rate to match the configured **Serial Command Line Interface Speed**.
3. Start or restart the server.
4. Press **F9** in the server POST screen.
The system RBSU or UEFI System Utilities start.
5. Configure the following settings:
 - Disable EMS and BIOS Serial Console
 - Set the Virtual Serial Port to `COM 2`.For information about using the system RBSU or UEFI System Utilities, see the system RBSU user guide or the UEFI System Utilities user guide.
6. To access the selection menu for the Windows debug boot option, reboot the server.
7. From the local test system, use PuTTY to connect to iLO and log in.
8. Enter the IP address for the session host name. Use the default settings for an SSH session.
When the PuTTY iLO CLI session opens, a user login window opens, unless the PuTTY session is configured to use private keys.
It might take a minute for the prompt to appear.
9. At the `</>hpiLO->` prompt, enter the following command:
`windbg_enable`
This command opens a socket to the Virtual Serial Port on port 3002.
10. To start the Windows debugger, enter the following command:
`windbg -k com:port=<IP-address>,ipport=3002`
`<IP-address>` is the iLO IP address, and 3002 is the socket to connect to (the raw serial data socket for iLO).
The `ipport` parameter is optional. The default port is 3002.
You can add other `windbg` command-line parameters if necessary. Hewlett Packard Enterprise recommends using the `-b` parameter for the initial breakpoint.

11. Go to the server console (or access the iLO Remote Console), and press **Enter** to boot the debug selection on the OS load menu.
This step might take several minutes.
12. When you are finished debugging the host server, use PuTTY to connect to the CLI and turn off the debug socket to the Virtual Serial Port. Then, enter the following command:
`windbg_disable`
You can disconnect and reconnect the Windows debugger as long as you keep the iLO debug socket enabled.

More information

[iLO security features](#)
[Administering SSH keys](#)

Using the ProLiant Preboot Health Summary

If a ProLiant Gen9 server will not start up, you can use iLO to display diagnostic information on an external monitor. When the server is off and power is available, iLO runs on auxiliary power and can control the server video adapter to show the Preboot Health Summary.

Prerequisites

- The server supports a UID button or an SUV connector.
To verify server support for these features, see the server user guide.
- The server is off, and power is available.
- The remote console is not in use and a firmware update is not in progress. The Preboot Health Summary cannot be accessed when the UID is in the **BLINK** state.

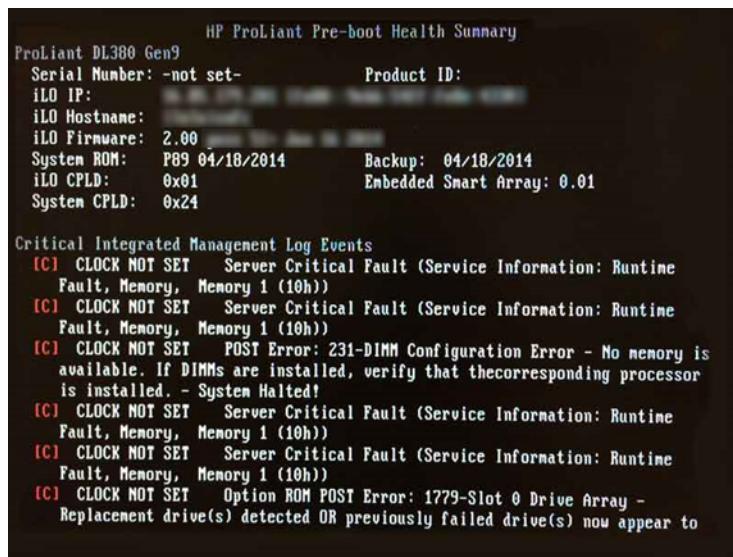
Viewing the Preboot Health Summary

- Use one of the following methods to access the Preboot Health Summary:
 - Press the UID button on the server.

⚠ **CAUTION:** To use this feature, press and release the UID button. Holding it down at any time for more than 5 seconds initiates a graceful iLO reboot or a hardware iLO reboot. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

- Log in to the iLO web interface, and change the UID state to **UID ON**. To change the UID state, click the UID icon at the bottom right corner of any iLO web interface window.
- Connect the SUV cable to the SUV connector.

The Preboot Health Summary screen is displayed on the server monitor. This screen remains until the server is powered on, the UID state is changed to **UID OFF**, an SUV connector is removed, or an iLO reboot completes.



HP ProLiant Pre-boot Health Summary
ProLiant DL380 Gen9
Serial Number: -not set- Product ID:
iLO IP:
iLO Hostname:
iLO Firmware: 2.00
System ROM: P89 04/18/2014 Backup: 04/18/2014
iLO CPLD: 0x01 Embedded Smart Array: 0.01
System CPLD: 0x24

Critical Integrated Management Log Events

- [C] CLOCK NOT SET Server Critical Fault (Service Information: Runtime Fault, Memory, Memory 1 (10h))
- [C] CLOCK NOT SET Server Critical Fault (Service Information: Runtime Fault, Memory, Memory 1 (10h))
- [C] CLOCK NOT SET POST Error: 231-DIMM Configuration Error - No memory is available. If DIMMs are installed, verify that the corresponding processor is installed. - System Halted!
- [C] CLOCK NOT SET Server Critical Fault (Service Information: Runtime Fault, Memory, Memory 1 (10h))
- [C] CLOCK NOT SET Server Critical Fault (Service Information: Runtime Fault, Memory, Memory 1 (10h))
- [C] CLOCK NOT SET Option ROM POST Error: 1779-Slot 0 Drive Array - Replacement drive(s) detected OR previously failed drive(s) now appear to

Preboot Health Summary details

The following information is displayed when you view the Preboot Health Summary:

- Server model number
- Server serial number
- Product ID
- iLO IP address (IPv4 and IPv6)—This value is displayed only if **Show iLO IP during POST** is set to **Enabled** on the **Administration**→**Access Settings** page in iLO.

For more information, see [“iLO access settings” \(page 61\)](#).

- iLO Hostname
- iLO firmware version
- ProLiant System ROM version
- ProLiant System ROM – Backup version
- iLO CPLD version
- System CPLD version

- Embedded Smart Array version number—This value is displayed only if server POST has successfully completed since the last auxiliary power cycle.
- **Critical** events—The most recent **Critical** events from the IML are displayed, with the most recent event displayed first.

Event log entries

For a list of the errors that might appear in the iLO Event Log, see the error messages guide for your server at the following website: <http://www.hpe.com/info/enterprise/docs>.

Incorrect time stamp on iLO Event Log entries

Symptom

iLO Event Log entries have an incorrect date or time.

Cause

The NTP server addresses or the time zone is configured incorrectly.

Action

Verify that the SNTP settings are configured correctly.

More information

[Configuring iLO SNTP settings](#)

Login and iLO access issues

iLO firmware login name and password not accepted

Symptom

An iLO firmware login attempt fails.

Solution 1

Cause

The user account information was entered incorrectly.

Action

Enter the correct user account information.

- Passwords are case-sensitive.
- User names are not case-sensitive. Uppercase and lowercase characters are treated the same (for example, Administrator is treated as the same user as administrator).

Solution 2

Cause

The user account is invalid.

Action

Try the following:

- Verify that the user account exists and has the Login privilege.
- Ask a user with the Administer User Accounts privilege to change the account password. If a login attempt fails after the password change, ask the user to delete and re-add the user account.
- Try to log in by using the default account information, which is on the serial label pull tab.
- If there is only one administrator account, and the password was forgotten, do one of the following:
 - Use the iLO security setting on the system maintenance switch. Log in and establish a new administrator user account.
 - Use HPONCFG to establish an administrator account and password. For more information, see the iLO scripting and command line guide.

More information

[iLO security with the system maintenance switch](#)

iLO management port not accessible by name

Symptom

The iLO management port is not accessible by name.

Cause

The environment is not configured to support accessing the iLO management port by name.

Action

The iLO management port can register with a WINS server or DDNS server to provide the name-to-IP-address resolution required to access the iLO management port by name.

Verify that your environment meets the following requirements:

- The WINS or DDNS server must be up and running before the iLO management port is powered on.
- The iLO management port has a valid route to the WINS or DDNS server.
- The iLO management port is configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the required IP addresses.
- The clients used to access the iLO management port are configured to use the same DDNS server where the IP address of the iLO management port is registered.

If you use a WINS server and a nondynamic DNS server, iLO management port access might be faster if you configure the DNS server to use the WINS server for name resolution. For more information, see the Microsoft documentation.

More information

[Setting up iLO by using the ROM-based setup utilities](#)
[iLO network settings](#)

iLO RBSU unavailable after iLO and server reset

Symptom

The iLO RBSU is unavailable after the server is reset immediately after iLO was reset.

Cause

The iLO firmware was not fully initialized when the server performed its initialization and tried to start the iLO RBSU.

Action

Reset the server a second time.

Unable to access the iLO login page

Symptom

The iLO web interface login page will not load.

Solution 1

Cause

The SSL encryption level in the browser is not set to 128-bit or higher.

The SSL encryption level in iLO is set to 128-bit or higher and cannot be changed. The browser and iLO encryption levels must be the same.

Action

Verify that the SSL encryption level of your browser is set to 128-bit or higher.

Solution 2

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

Ensure that your Shared Network Port configuration follows the NIC teaming guidelines. For more information, see [“NIC teaming with Shared Network Port configurations” \(page 24\)](#).

Unable to return to iLO login page after iLO reset

Symptom

The iLO login page will not open after an iLO reset.

Action

Clear the browser cache and restart the browser.

Unable to connect to iLO after changing network settings

Symptom

iLO is inaccessible after an update to the network settings.

Cause

The NIC and the switch settings are not the same.

Action

Verify that both sides of the connection (the NIC and the switch) have the same settings for transceiver speed autoselect, speed, and duplex.

For example, if one side is autoselecting the connection, the other side must use the same setting.

For information about configuring the iLO network settings, see [“iLO network settings” \(page 96\)](#).

An iLO connection error occurs after an iLO firmware update

Symptom

You cannot connect to iLO after updating the firmware by using the web interface.

Action

Clear the browser cache and try again.

Unable to connect to iLO processor through NIC

Symptom

The iLO processor is inaccessible through the NIC.

Action

Try the following solutions:

- Confirm that the green LED indicator (link status) on the iLO RJ-45 connector is on. This condition indicates a good connection between the PCI NIC and the network hub.
Look for intermittent flashes of the green LED indicator, which indicates normal network traffic.
- To confirm that the NIC is enabled, and to verify the assigned IP address and subnet mask, run the iLO RBSU or the iLO 4 Configuration Utility.
- To view the status of DHCP requests, run the iLO RBSU, and use the **Advanced** option on the **Network Autoconfiguration** page.
- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with a browser by entering the IP address of the NIC as the URL. You can see the iLO login page from this address.
- Reset iLO.

NOTE: If a network connection is established, you might have to wait up to 90 seconds for the DHCP server request.

Unable to log in to iLO after installing iLO certificate

Symptom

iLO is inaccessible after the iLO self-signed certificate is installed in the browser certificate store.

Cause

When you reset iLO to the factory default settings or change the iLO hostname, a new self-signed certificate is generated. In some browsers, if the self-signed certificate is installed permanently, you might not be able to log in to iLO after a new self-signed certificate is generated.

Action

Do not install the iLO self-signed certificate in the browser certificate store. If you want to install a certificate, request a permanent certificate from a CA and import it into iLO. For instructions, see “[Administering SSL certificates](#)” (page 74).

Unable to connect to iLO IP address

Symptom

Cannot connect to iLO via the iLO IP address.

Cause

The web browser is configured to use a proxy server.

Action

Configure the browser to connect to iLO without using the proxy server.

For example, in Internet Explorer:

1. Select **Tools**→**Internet Options**.
2. Click **Connections**.
3. Click **LAN settings**.
4. Click **Advanced** in the **Proxy server** section.
5. Enter the iLO IP address or DNS name in the **Exceptions** box.
6. To save the changes, click **OK**.

iLO communications fail

Symptom

iLO communications fail.

Cause

A firewall is preventing iLO communications through one or more TCP/IP ports.

Action

Configure the firewall to allow communications on the ports iLO uses. For information about viewing and changing the iLO port configuration, see “[iLO access settings](#)” (page 61).

Secure Connection Failed error when using Firefox to connect to iLO

Symptom

The following error occurs when you try to use Firefox to connect to iLO:

`sec_error_reused_issuer_and_serial`.

Solution 1

Cause

The installed certificate contains the same serial number as another certificate issued by the certificate authority.

Action

1. Click the menu button, and then select **Options**.
2. Click **Advanced**.
3. Click the **Certificates** tab.

4. Click **View Certificates**.
Click the **Servers** tab, and then delete any certificates related to iLO.
5. Click the **Others** tab, and then delete any certificates related to iLO.
6. Click **OK**.
7. Start Firefox and connect to iLO.

NOTE: The steps in Solution 1 are based on Firefox ESR 24. The procedure to use might vary depending on the installed version of Firefox.

Solution 2

Cause

The installed certificate contains the same serial number as another certificate issued by the certificate authority.

Action

1. Close the Firefox application.
2. Navigate to the Firefox AppData folder, and then delete all of the *.db files in all of the Firefox directories.

The AppData folder is typically in the following location: C:\\Users\\<user name>\\AppData\\Local\\Mozilla\\Firefox\\

Certificate error when navigating to iLO web interface

Symptom

When you navigate to the iLO web interface, a certificate error appears.

Solution 1

Action

If you are using Internet Explorer, complete the following procedure:

1. Click the **Continue to this website (not recommended)** link.
2. Log in to iLO.
3. Optional: To prevent the certificate warning from appearing in future iLO web interface sessions, [install an SSL certificate](#).

Solution 2

Action

If you are using Firefox, complete the following procedure:

1. Click **I Understand the Risks**, and then click **Add Exception**.
2. In the **Add Security Exception** dialog box, enter `https://<iLO hostname or IP address>` in the **Location** box.
3. Click **Confirm Security Exception**.

The security exception is saved and the iLO login screen appears.

4. Log in to iLO.
5. Optional: [Install an SSL certificate](#).

Solution 3

Action

If you are using Chrome, complete the following procedure:

1. When the security warning appears, click **Advanced**.
2. Click **Proceed to <iLO hostname or IP address> (unsafe)**.
3. Log in to iLO.
4. Optional: To prevent the certificate warning from appearing in future iLO web interface sessions, [install an SSL certificate](#).

Solution 4

Action

1. Navigate to the **Administration**→**Security**→**SSL Certificate** page.

2. Obtain and import an SSL certificate.

3. Reset iLO.

For instructions, see [“Obtaining and importing an SSL certificate” \(page 75\)](#).

iLO login page displays a Website Certified by an Unknown Authority message

Symptom

The message **Website Certified by an Unknown Authority** is displayed when you navigate to the iLO login page.

Action

1. To ensure that you are browsing to the correct management server (not an imposter), view the certificate.
 - Verify that the **Issued To** name is your management server. Perform any other steps you feel necessary to verify the identity of the management server.
 - If you are not sure that you navigated to the correct management server, do not proceed. You might be browsing to an imposter and giving your sign-in credentials to that imposter when you sign in. Contact the administrator. To cancel the connection, exit the certificate window, and then click **No** or **Cancel**.
2. After verifying the items in [Step 1](#), you have the following options:
 - Accept the certificate temporarily for this session.
 - Accept the certificate permanently.
 - Stop now and import the certificate into your browser from a file provided by your administrator.

More information

[Administering SSL certificates](#)

iLO inaccessible on a server managed by HPE OneView

Symptom

iLO cannot be accessed on a server that HPE OneView manages.

Cause

The server signature changed, and HPE OneView has not rediscovered and configured the server.

Action

Use HPE OneView to refresh the frame that contains the server.

Unable connect to an iLO system with the iOS mobile app

Symptom

The connection fails when you try to connect to an iLO system by using the iOS mobile app.

Solution 1

Cause

iLO is configured incorrectly or there is a local network problem.

Action

To confirm this cause, try to connect to iLO by using a laptop or desktop computer on the same network as iLO. If the connection fails, check the iLO and network configuration.

Solution 2

Cause

There is a firewall between your iOS device and iLO.

Action

To confirm this cause, try to connect to iLO from the Safari browser on your iOS device.

Do one of the following:

- Configure the firewall to allow exceptions for the iLO web server SSL port (HTTPS) and the Remote Console port. By default, the web server SSL port uses port 443 and the Remote Console port uses port 17990.
- Configure iLO to work with the exceptions allowed by most firewalls. Typically, firewalls allow exceptions for addresses on ports 80 and 443. Change the iLO web server Non-SSL Port from the default value (80) to another value, and then configure the Remote Console port to use port 80.

You can configure the iLO port values on the **Administration→Access Settings** page in the iLO web interface.

- Use a VPN connection to connect your iOS device to the network.

A VPN connection typically involves obtaining an Oath token or something similar and an account from your IT department. After configuring the VPN on your iOS device, use the Oath token to generate a onetime password, and then log in to the network that includes the iLO you want to use.

Contact your IT administrator for information about how to set up a VPN on your iOS device.

iLO responds to pings intermittently or does not respond

Symptom

iLO responds to pings intermittently or does not respond.

Solution 1

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

Ensure that your Shared Network Port configuration follows the NIC teaming guidelines. For more information, see [“NIC teaming with Shared Network Port configurations” \(page 24\)](#).

Running an XML script with iLO fails

Symptom

When you run an XML script against iLO, the session does not start or terminates unexpectedly.

Solution 1

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

Ensure that your Shared Network Port configuration follows the NIC teaming guidelines. For more information, see [“NIC teaming with Shared Network Port configurations” \(page 24\)](#).

Directory issues

Logging in to iLO with Kerberos authentication fails

Symptom

A Kerberos login attempt fails.

Solution 1

Cause

The client does not have a ticket or has an invalid ticket.

Action

To lock the client PC and get a new ticket, press **Ctrl+Alt+Del**.

Solution 2

Cause

Kerberos login is configured incorrectly. Possible reasons follow:

- The Kerberos realm that the client PC is logged in to does not match the Kerberos realm for which iLO is configured.
- The key in the Kerberos keytab stored in iLO does not match the Active Directory key.
- iLO is configured for an incorrect the KDC server address.
- The date and time do not match between the client PC, the KDC server, and iLO. Set the date and time on these systems to the same value. The date and time on these systems must not differ by more than 5 minutes.

Action

Verify that your environment meets the requirements for Kerberos support. For more information, see [“Kerberos authentication with iLO” \(page 278\)](#).

Solution 3

Cause

There is a problem with the directory user account:

- The iLO computer account does not exist in Active Directory, or the account is disabled.
- The user logged in to the client PC is not a member of a universal or global directory group authorized to access iLO.

Action

Verify that the user account exists and that it is a member of a group that is authorized to access iLO.

Solution 4

Cause

The DNS server is not working correctly. iLO requires a functioning DNS server for Kerberos support.

Action

Repair the DNS server.

Solution 5

Cause

The browser is not configured correctly.

Action

Verify that the browser is configured correctly for Kerberos login. For more information, see [“Kerberos authentication with iLO” \(page 278\)](#).

iLO Credential prompt appears during Kerberos login attempt

Symptom

When a user clicks the **Zero Sign In** button, a credential prompt appears.

Cause

The browser is not configured correctly for Kerberos login.

Action

iLO Credential prompt appears during Kerberos login by name attempt

Symptom

A credential prompt appears when a user tries to log in to iLO with a user name in Kerberos SPN format and the associated domain password.

Cause

The computer account for iLO is part of a child domain and the Kerberos configuration parameters reference the parent domain.

Action

Verify that the following Kerberos parameters are configured correctly: **Kerberos Realm**, **Kerberos KDC Server Address**, and **Kerberos KDC Server Port**.

A directory connection to iLO ends prematurely

Symptom

An Active Directory session ends prematurely.

Cause

Network errors can cause iLO to conclude that a directory connection is no longer valid. If iLO cannot detect the directory, it ends the directory connection. Any attempt to continue using the terminated connection redirects the browser to the login page.

This issue might occur in the following situations:

- The network connection is terminated.
- The directory server is shut down.

Action

Log back in and continue using iLO.

If the directory server is unavailable, you must log in with a local user account.

Configured Directory user contexts do not work with iLO login

Symptom

Directory user contexts are configured, but the login options they provide do not work.

Cause

The user object in the directory or the user context is not configured correctly.

Action

Ask the network administrator to verify the following:

- The full DN of the user object exists in the directory.
This information appears after the first `CN=` in the DN.
- The remainder of the DN was added as a user context.
User contexts are not case-sensitive, and any other characters, including spaces, are part of the user context.

More information

[Directory authentication and authorization](#)

[Directory user contexts](#)

iLO directory user account does not log out after directory timeout expires

Symptom

A directory user is not logged out after being idle for the amount of time configured for the directory login timeout.

Cause

The iLO **Idle Connection Timeout** value is set to **Infinite**. With this configuration, the Remote Console periodically pings the iLO firmware to verify that the connection exists. When the Remote Console pings iLO, the iLO firmware queries the directory for user permissions. This periodic query keeps the directory connection active, and prevents a user from being logged out based on the directory timeout settings.

Action

Change the **Idle Connection Timeout** setting.

Failure generating Kerberos Keytab file for iLO Zero Sign In configuration

Symptom

When you try to generate a keytab file with `ktpass`, the process fails.

Cause

The `ktpass` command was formatted incorrectly.

Action

Try again, and ensure that the principal name is formatted correctly.

More information

[Ktpass](#)

Error when running `Setspn` for iLO Kerberos configuration

Symptom

An error occurred when running the `Setspn` command.

Action

1. Use MMC with the `ADSIEDit` snap-in, and find the computer object for iLO.

2. Set the `DNSHostName` property to the iLO DNS name. For example:

```
cn=iloname,ou=us,ou=clients,dc=example,dc=net
```

iLO Zero Sign In fails after domain controller OS reinstall

Symptom

The iLO web interface **Zero Sign In** option does not work after the domain controller OS is reinstalled.

Cause

The key version number sequence is reset when the domain controller OS is reinstalled.

Action

Generate and install a new Kerberos keytab file.

More information

[Generating a keytab file for iLO in a Windows environment](#)

Failed iLO login with Active Directory credentials

Symptom

User authentication fails when iLO is configured to use Active Directory.

Cause

There is a certificate problem:

- An SSL certificate is not installed on the Active Directory server.
- An old SSL certificate on the Active Directory server points to a previously trusted CA with the same name as the CA in the current certificate. This situation might happen if a certificate service is added and removed, and then added again.

You can verify this cause by checking the SSL Connection test results on the **Directory Tests** page.

Action

1. Open the MMC.
2. Add the certificates snap-in.
3. When prompted, select **Computer Account** for the type of certificates you want to view.
4. To return to the certificates snap-in, click **OK**.
5. Select the **Personal→Certificates** folder.
6. Right-click the folder and select **Request New Certificate**.
7. Verify that the **Type** is domain controller, and click **Next** until a certificate is issued.

Directory Server DNS Name test reports a failure

Symptom

The Directory Server DNS Name test reports the status **Failed**.

Cause

iLO cannot obtain an IP address for the directory server.

Action

Try the following actions:

1. Verify that the DNS server configured in iLO is correct.
2. Verify that the directory server FQDN is correct.
3. As a troubleshooting tool, use an IP address instead of the FQDN.
4. If the problem persists, check the DNS server records and network routing.

Ping Directory Server test reports a failure

Symptom

The Ping Directory Server test reports the status **Failed**.

Cause

iLO pinged the directory server and did not receive a response.

Action

Try the following actions:

1. Check to see if a firewall is active on the directory server.
2. Check for network routing issues.

Connect to Directory Server test reports a failure

Symptom

The Connect to Directory Server test reports the status **Failed**.

Cause

iLO failed to initiate an LDAP connection with the specified directory server.

Action

Try the following actions:

1. Verify that the configured directory server is the correct host.
2. Verify that iLO has a clear communication path to the directory server through port 636 (consider any routers or firewalls between iLO and the directory server).
3. Verify that any local firewall on the directory server is enabled to allow communications through port 636.

Connect using SSL test reports a failure

Symptom

The Connect using SSL test reports the status **Failed**.

Cause

The SSL handshake and negotiation between iLO and the directory server were unsuccessful.

Action

Try the following actions:

- Enable the directory server for SSL negotiations.
- If you are using Microsoft Active Directory, verify that Active Directory Certificate Services is installed.

Bind to Directory Server test reports a failure

Symptom

The Bind to Directory Server test reports the status **Failed**.

Cause

iLO failed to bind the connection with the specified user name or an anonymous bind.

Action

Try the following actions:

1. Verify that the directory server allows anonymous binding.
2. If you entered a user name in the test boxes, verify that the credentials are correct.
3. If you verified that the user name is correct, try using other user-name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`.
4. Verify that the specified user is allowed to log in and is enabled.

Directory Administrator Login test reports a failure

The Directory Administrator Login test reports the status **Failed**.

Symptom

The Directory Administrator Login test reports the status **Failed**.

Cause

You entered values in the optional **Directory Administrator Distinguished Name** and **Directory Administrator Password** boxes, and login to the directory server failed.

Action

Verify that the directory administrator credentials were entered correctly.

User Authentication test reports a failure

Symptom

The User Authentication test reports the status **Failed**.

Cause

Authentication failed with the provided user name and password.

Action

Try the following actions:

1. Verify that the user credentials were entered correctly.
2. Try using other user-name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`.
3. Verify that the specified user is allowed to log in and is enabled.
4. Check to see if access restrictions are configured for the specified user account.

User Authorization test reports a failure

Symptom

The User Authorization test reports the status **Failed**.

Cause

Authorization failed with the provided user name and password.

Action

Try the following actions:

1. Verify that the specified user name is part of the specified directory group.
2. Check to see if access restrictions are configured for the specified user account.

Directory User Contexts test reports a failure

Symptom

The Directory User Contexts test reports the status **Failed**.

Cause

When iLO used the provided **Directory Administrator Distinguished Name** to search for a specified user context, the container was not found in the directory.

Action

Verify that the search contexts were entered correctly.

LOM Object Exists test reports a failure

Symptom

The LOM Object Exists test reports the status **Failed**.

Cause

iLO failed to locate the directory object specified by the **LOM Object Distinguished Name** configured on the **Security→Directory** page.

Action

Try the following actions:

1. Verify that the LDAP FQDN of the LOM object is correct.
2. Try to update the HPE Extended Schema and snap-ins in the directory server by updating the HPLOMIG software.

Remote Console issues

The following sections discuss troubleshooting Remote Console issues.

① **IMPORTANT:** Pop-up blocking applications, which prevent the automatic opening of new windows, prevent the Remote Console from running. Disable any pop-up blocking programs before you start the Remote Console.

iLO Java IRC displays red X when Firefox is used to run Java IRC on Linux client

Symptom

The Java IRC displays a red X icon when you run the Java IRC on a Linux system.

Cause

Firefox is not configured to accept cookies.

Action

Configure Firefox to accept cookies. For instructions on configuring Firefox, see the Firefox documentation.

iLO Java IRC does not start

Symptom

The Java IRC fails to start when you do not accept the security warning and confirm that you want to run the application.

Cause

You cannot run the Java IRC without accepting the security warning and confirming that you want to run the application.

Action

1. Click the **Clear** button in the **Java Console** window.
2. To close the **Java Console** window, click the **Close** button.
3. Reset iLO.
For instructions, see “[iLO diagnostics](#)” (page 193).
4. Clear the browser cache.
5. Close the browser and open a new browser window.
6. Log in to iLO, start the Java IRC, and then accept the certificate.

Cursor cannot reach iLO Remote Console window corners

Symptom

The mouse cursor cannot be moved to the corners of the Remote Console window.

Action

Right-click and drag the mouse cursor outside the Remote Console window, and then drag it back inside.

iLO Remote Console text window not updated correctly

Symptom

When you use the Remote Console to display text windows that scroll at a high rate of speed, the text window might not be updated correctly.

Cause

This issue might occur when video updates happen faster than the iLO firmware can detect and display them. Typically, only the upper left corner of the text window is updated while the rest of the text window remains static.

Action

After the text window stops scrolling, click **Refresh** to update the Remote Console window.

Mouse or keyboard not working in iLO remote console

Symptom

The mouse or keyboard does not work in the .NET IRC or Java IRC.

Solution 1

Action

1. Close the .NET IRC or Java IRC.
2. Navigate to the **Power Management**→**Power Settings** page.
3. Clear the **Enable persistent mouse and keyboard** check box, and then click **Apply**.
4. Start the .NET IRC or Java IRC again.

Solution 2

Action

Right-click and drag the mouse cursor outside the Remote Console window, and then drag it back inside.

Solution 3

Action

For the Java Applet only:

1. Shut down and exit your browser.
2. Open the Java Control Panel.
3. Navigate to the **Java Runtime Environment Settings** dialog box.
4. Add the following runtime parameter:
`-Dsun.java2d.d3d=false`
5. Click **OK** and close the **Java Runtime Environment Settings** window.
6. Click **Apply**, and then click **OK** to close the Java Control Panel.

NOTE: Viewing your changes before you click **Apply** might reset the **Runtime Parameters** dialog box, causing your edits to be lost.

iLO .NET IRC sends characters continuously after switching windows

Symptom

When you switch to a different window, the .NET IRC sends characters continuously.

Cause

If you press a key during a .NET IRC session, and you switch windows, the key might remain pressed in the session, causing the character to repeat continuously.

Action

Bring the remote console window to the front of your desktop by clicking the .NET IRC window.

iLO Java IRC displays incorrect floppy and USB-key device information

Symptom

When the Firefox browser is used, the Java IRC might display incorrect floppy drive and USB-key device information.

Cause

The client OS or Java software might be out of date.

Action

1. Make sure that Red Hat Enterprise Linux 5 or later is installed on the local client system.
2. Install the latest version of Java and configure it to connect through the Firefox browser.
3. Log in to the iLO web interface.
4. Insert a USB key or floppy disk on the local client system.
5. Verify that you can access the USB key or floppy disk.
6. Open a Java IRC session.
7. Select **Virtual Drives**→**Image File Removable Media**.
The **Choose Disk Image File** dialog box opens.
8. Type or select the path of the USB key or floppy disk (`/dev/disk`) inserted in the client.
You can also mount the USB key or floppy disk by label.
9. Click **OK**.

Caps Lock out of sync between iLO and Java IRC

Symptom

When you log in to the Java IRC, the **Caps Lock** setting might be out of sync between iLO and the Java IRC.

Action

To synchronize the **Caps Lock** settings, select **Keyboard**→**Caps Lock** in the Java IRC.

Num Lock out of sync between iLO and Shared Remote Console

Symptom

When you log in to a Shared Remote Console session, the **Num Lock** setting might be out of sync between iLO and some of the Remote Console sessions.

Action

To synchronize the **Num Lock** settings, select **Keyboard**→**Num Lock** in the Remote Console.

Keystrokes repeat unintentionally during iLO Remote Console session

Symptom

A keystroke repeats unintentionally during a Remote Console session.

Solution 1

Cause

A network issue might be causing network latency.

Action

Identify and fix problems that might cause network latency.

Solution 2

Cause

The remote system settings are causing a delay.

Action

Adjust the following settings on the remote machine:

- **Increase the typematic delay**—This setting controls the delay before a character repeats when you press and hold a key on the keyboard.
- **Decrease the typematic rate**—This setting controls the rate at which a character repeats when you press and hold a key on the keyboard.

NOTE: The exact name of the setting varies depending on the OS you are using. For more information about changing the typematic delay and rate, see your OS documentation.

Session leader does not receive connection request when iLO .NET IRC is in replay mode

Symptom

When a Remote Console session leader plays captured video data, a prompt is not displayed when another user requests to access or share the .NET IRC.

Cause

The request to access or share the .NET IRC timed out.

Action

Contact the other user or use the Remote Console Acquire feature to take control of the .NET IRC. For instructions, see [“Acquiring the Remote Console” \(page 218\)](#).

iLO Remote Console Keyboard LED does not work correctly

Symptom

The client keyboard LED does not reflect the state of the remote console keyboard.

Cause

The client keyboard LED does not reflect the true state of the remote console keyboard lock keys. The **Caps Lock**, **Num Lock**, and **Scroll Lock** keys are fully functional when you use the keyboard options in the Remote Console.

Action

No action needed.

iLO .NET IRC becomes inactive or disconnects

Symptom

The iLO .NET IRC becomes inactive or disconnects during periods of high activity. .NET IRC activity slows before becoming inactive. Symptoms of an inactive .NET IRC include the following:

- The .NET IRC display is not updated.
- Keyboard and mouse activity is not recorded.
- Shared Remote Console requests do not register.
- You can replay a captured video file, but the other .NET IRC features remain inactive.

Solution 1

Cause

Multiple users are logged in to iLO.

Action

Try the following:

- Reduce the number of simultaneous iLO user sessions.
- Reset iLO.

Solution 2

Cause

A connected Virtual Media session is being used to perform a continuous copy operation. The continuous copy operation takes priority and, consequently, the .NET IRC loses synchronization. Eventually, the Virtual Media connection resets multiple times and causes the USB media drive for the OS to lose synchronization with the Virtual Media client.

Action

Try the following:

- Reconnect to the .NET IRC and the Virtual Media.
- Reset iLO.

iLO .NET IRC failed to connect to server

Symptom

iLO displays the message Failed to connect to server when it attempts to establish a .NET IRC session.

Solution 1

Cause

The network response is delayed. The iLO .NET IRC client waits a specified amount of time for a connection to be established with iLO. If the client server does not receive a response in this amount of time, it displays an error message.

Action

Correct the network delay and retry the .NET IRC connection.

Solution 2

Cause

A Shared Remote Console session is requested, but the session leader delayed sending an acceptance or denial message. The iLO .NET IRC client waits a specified amount of time for a connection to be established with iLO. If the client server does not receive a response in this amount of time, it displays an error message.

Action

Contact the .NET IRC session leader and retry the request, or use the Remote Console Acquire feature. For more information, see [“Acquiring the Remote Console” \(page 218\)](#).

File not present after copy from server to iLO Virtual Media USB key

Symptom

If you copy files from a target server to an iLO virtual drive, the files are not visible in Windows Explorer on the client computer.

Cause

File changes on an iLO Virtual Media USB key cannot be viewed in Windows Explorer by the user on the client computer.

Windows Explorer keeps a cached copy of the files on the USB key. The iLO Remote Console does not notify the Windows Shell when the USB key is updated with file changes. If you refresh the Explorer window, the cached information is sent back to the USB key, so the changed information cannot be viewed.

Action

1. Connect a USB key to a Windows client computer.
2. Start the .NET IRC, and connect the USB key by selecting it in the **Virtual Drives** menu.
3. Make file changes to the connected device (copy, delete, and so on).
4. To ensure that all data is updated on the device, unmount the device from the target server.
5. Disconnect the device by using the **Virtual Devices** menu in the .NET IRC.

△ **CAUTION:** Do not use Windows Explorer to refresh the contents of the USB key.

6. Use the **Safely Remove Hardware** feature to remove the device from the client computer.
7. Remove the device from the client computer.

When you connect the USB key to any computer, the file changes will be visible in Windows Explorer.

iLO .NET IRC takes a long time to verify application requirements

Symptom

When you start the .NET IRC from the iLO web interface, the **Launching Application** dialog box appears and remains on the screen for a long time.

Action

1. Open Internet Explorer.
2. Select **Tools**→**Internet Options**.
The **Internet Options** window opens.
3. Click the **Connections** tab, and then click the **LAN settings** button.
The **Local Area Network (LAN) Settings** window opens.
4. Clear the **Automatically detect settings** check box.
5. Optional: If needed, configure the proxy server settings.
6. Close all of the browser windows.
7. Restart the browser and start the .NET IRC.

iLO .NET IRC will not start

Symptom

When you start the .NET IRC, the **Cannot Start Application** dialog box appears with the message Application cannot be started. Contact the application vendor.

Action

Clear the ClickOnce application cache by entering the following command from the Windows Command Prompt: `rundll32 %windir%\system32\dfshim.dll CleanOnlineAppCache`.

iLO .NET IRC cannot be shared

Symptom

When you try to join a shared .NET IRC session, the **Unable to connect** dialog box appears with the message Unable to connect to shared IRC. This might be due to a firewall blocking port 17990.

Action

Try the following:

- Make sure that there is a communication route between the session leader .NET IRC client and each shared .NET IRC client.
- Make sure that the firewall settings on all clients allow an inbound connection to the Remote Console port (the default port is 17990).

iLO .NET IRC will not start in Firefox

Symptom

When you launch the .NET IRC in Mozilla Firefox, the application might fail to start.

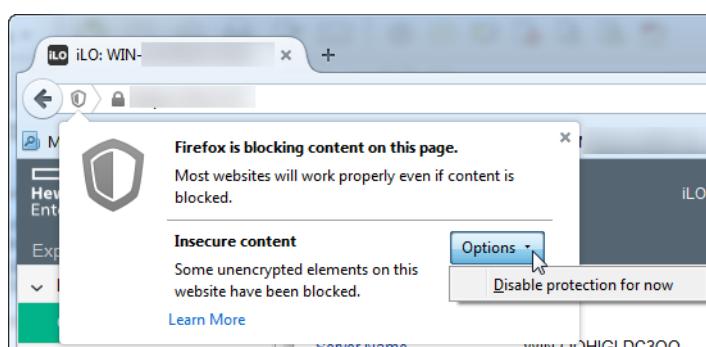
Cause

If the iLO system uses the default iLO SSL certificate (not a signed trusted certificate) the iLO web interface uses HTTP instead of HTTPS to start the .NET IRC. Since the iLO web interface uses HTTPS, and the web interface starts the IRC by using HTTP, the browser displays a warning.

Action

Try the following:

- Import an SSL certificate into iLO and enable the **IRC Requires a Trusted Certificate** in iLO setting on the **Administration**→**Security**→**Remote Console** page. This configuration is the most secure solution.
For information about importing certificates, see “[Administering SSL certificates](#)” (page 74).
For information about changing the **IRC Requires a Trusted Certificate** in iLO setting, see “[Configuring the Integrated Remote Console Trust setting \(.NET IRC\)](#)” (page 94).
- Click the shield icon in the address bar, and then select **Options**→**Disable protection for now**.



The warning might vary depending on your browser version.

- Use a different browser.
- Use the Standalone IRC, available at the following website: <http://www.hpe.com/support/hpesc>.
- Use the iLO mobile app. For more information, see <http://www.hpe.com/info/ilo/mobileapp>.

iLO .NET IRC will not start in Google Chrome

Symptom

When you launch the .NET IRC in Google Chrome, the application fails to start.

Cause

Previous versions of Google Chrome could run the .NET IRC with an NPAPI plug-in that supported ClickOnce. Google Chrome 42 and later does not support NPAPI-based plug-ins.

Action

- Use a different browser.
- Use the Java IRC.
- Use the Standalone IRC, available at the following website: <http://www.hpe.com/support/hpesc>.
- Use the iLO mobile app. For more information, see <http://www.hpe.com/info/ilo/mobileapp>.

Unable to boot to DOS using a USB key mounted with the iLO Remote Console

Symptom

An error occurs when you try to boot to a DOS-bootable USB key that is mounted by using the iLO Remote Console.

If the USB key is 2 GB or less, the following message is displayed:

```
Attempting Boot From CD-ROM
Attempting Boot From USB DriveKey (C:)

Cannot load DOS! Any key to retry
```

If the USB key is larger than 2 GB, the server does not progress beyond following message:

```
Attempting Boot From USB DriveKey (C:) Boot From Drive
Operating system load error.
SYSLINUX 3.73 2009-01-25 EBIOS Copyright (C) 1994-2008 H. Peter Anvin
FreeDOS kernel build 2036 cvs [version Aug 18 2006 compiled Aug 18 2006]
Kernel compatibility 7.10 - WATCOMC - 80386 CPU required - FAT32 support

(C) Copyright 1995-2006 Pasquale J. Villani and The FreeDOS Project.
All Rights Reserved. This is free software and comes with ABSOLUTELY NO
WARRANTY; you can redistribute it and/or modify it under the terms of the
GNU General Public License as published by the Free Software Foundation;
either version 2, or (at your option) any later version.
- InitDiskWARNING: using suspect partition Pri:1 FS 0c: with calculated values
470-113-35 instead of 469-254-63
-
```

Cause

The Remote Console does not have sufficient privileges to access the boot sector of the USB key.

Action

Try the following:

- Right-click Internet Explorer, and then select **Run as administrator**. Start the iLO web interface, launch the Remote Console, and then boot to the USB key.
- Plug the USB key directly into the server.

Text-based Remote Console issues

The following sections discuss items to be aware of when attempting to resolve text-based Remote Console issues.

Unable to view Linux installer in text-based Remote Console

Symptom

The Linux installer screen is not displayed when you install Linux from the text-based Remote Console.

Cause

The screen is in graphics mode.

Action

Do one of the following:

- For most versions of Linux, enter `linux text nofb`.
The characters that you enter do not appear.
After you enter the command, the screen changes from graphics mode to text mode, displaying the screen.
- For SUSE Linux Enterprise Server, press **F2** and the down arrow from the text console. The text mode is selected and the screen appears.

Unable to pass data through SSH terminal

Symptom

The SSH terminal does not pass keystroke data to the text-based Remote Console.

Cause

If you use an SSH terminal to access the text console, SSH might intercept keystroke data and not pass the action to the text-based Remote Console. When this behavior occurs, it looks like the keystroke did not perform its function.

Action

Disable SSH terminal shortcuts.

VSP-driven selection during the serial timeout window sends output to BIOS redirect instead of VSP

Symptom

VSP-driven selection during the serial timeout window sends output to BIOS redirect instead of VSP.

Cause

The `/etc/grub.conf` file includes an option for a serial timeout window (`terminal --timeout=10 serial console`). This option provides a window of time to select a keystroke on the VSP or on the VGA console, and then the menu is output to the corresponding device. The BIOS serial redirect intercepts VSP keystrokes during this timeout window.

Action

Do not press a key for a VSP-driven selection during the 10-second timeout or turn off BIOS redirection to the VSP.

Scrolling and text appear irregular during BIOS redirection

Symptom

During BIOS redirection, scrolling and text are not displayed correctly. When you enter commands in the ROM-based utility, text might overwrite itself on the bottom line of the terminal window.

Cause

The BIOS expects and controls a fixed 80x24 character window. When redirected to the serial port, the BIOS still expects and controls a fixed 80x24 character window. If the VSP client (SSH, HyperTerminal, or another terminal emulator) resizes the window to a size other than 80x24, scrolling becomes confused and screen output appears garbled.

Action

Configure the terminal emulator for a window size of exactly 80x24 characters.

SSH issues

Initial PuTTY input slow with iLO

Symptom

During the initial connection to iLO through a PuTTY client, input is accepted slowly for approximately 5 seconds.

Action

Try the following:

- Verify that the client configuration options are correct.
- Clear the **Disable Nagle's algorithm** check box in the low-level TCP connection options.

PuTTY client unresponsive with iLO Shared Network Port

Symptom

When you use a PuTTY client with the Shared Network Port, the PuTTY session becomes unresponsive.

Cause

A large amount of data is being transferred or you are using a Virtual Serial Port and Remote Console.

Action

Close the PuTTY client and restart the session.

Text is displayed incorrectly when using an SSH connection to iLO

Symptom

Extended text configuration beyond the 80 x 25 configuration is not displayed correctly when using SSH.

Cause

SSH access from the text-based Remote Console supports the standard 80 x 25 configuration of the text screen. This mode is compatible for the text-based Remote Console for most text-mode interfaces.

Action

Hewlett Packard Enterprise recommends configuring the text application in 80 x 25 mode or using the graphical Remote Console.

An SSH session fails to start or terminates unexpectedly

Symptom

An SSH session fails to start or terminates unexpectedly.

Solution 1

Cause

iLO is configured to use the Shared Network Port, and NIC teaming is enabled for the NIC the Shared Network Port uses. In this configuration, network communications might be blocked in the following cases:

- The selected NIC teaming mode causes the switch that iLO is connected with to ignore traffic from the server NIC/port that iLO is configured to share.
- The selected NIC teaming mode sends all traffic destined for iLO to a NIC/port other than the one that iLO is configured to share.

Action

Ensure that your Shared Network Port configuration follows the NIC teaming guidelines. For more information, see [“NIC teaming with Shared Network Port configurations” \(page 24\)](#).

Remote Support issues

SSL Bio Error during Insight RS registration

Symptom

The following error occurs when you try to register a server for Insight Remote Support central connect: SSL Bio Error.

Action

1. Navigate to the **Information**→**Diagnostics** page in the iLO web interface.
2. Click **Reset iLO**.

Clicking **Reset iLO** does not make any configuration changes, but it terminates any active connections to iLO and completes any firmware updates in progress. The Configure iLO Settings privilege is required to reset iLO on the **Diagnostics** page.

3. When the reset is finished, log in to the iLO web interface and retry the registration procedure.

Server not identified by server name in Insight Online or Insight RS

Symptom

A server is not identified as <server name> in Insight Online or Insight RS. Instead, it is identified in Insight Online as <product name>_<serial number> and in Insight RS as <serial number>.

Cause

The server was registered for remote support before iLO discovered the server name.

Action

1. Do one of the following:
 - Verify that AMS is enabled and the operating system is running.
 - Update the **Server Name** on the **Administration**→**Access Settings** page in the iLO web interface.
 - For Windows systems only: Start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.
2. For Insight Remote Support central connect only: Depending on your configuration, do one of the following:
 - For configurations with iLO firmware 1.30 or later, no additional action is required. iLO automatically detects the server name and forwards it to Insight RS and Insight Online.
 - ProLiant Gen8 servers only: For configurations with iLO firmware versions earlier than 1.30, the server name is updated automatically the next time data collection information is transmitted. Data collection occurs every 30 days and can be initiated immediately from the **Remote Support**→**Data Collections** page in the iLO web interface.
3. If you had an active Insight Online session when you performed [Step 1](#), click the refresh button (**C**) to update the Insight Online view with the server information.

More information

[Sending data collection information](#)

Server OS name and version not listed in Insight RS or Insight Online

Symptom

The server OS name and version are not listed in Insight RS or Insight Online.

Cause

The server was registered for remote support when the OS and AMS were not running (for example, during an Intelligent Provisioning registration). In this situation, iLO cannot determine which OS is installed.

Action

To update the OS information, iLO must acquire the OS information from AMS.

1. Verify the following:
 - For ProLiant Gen8 servers: iLO firmware 1.20 or later (Insight Remote Support central connect) or 1.40 or later (Insight Online direct connect) is installed.
 - For ProLiant Gen9 servers: iLO firmware 2.00 or later is installed.
 - AMS is enabled and the OS is running.
 - For Insight Remote Support central connect only: A supported version of Insight RS is installed on the host server. For more information, see <http://www.hpe.com/support/InsightRS-Support-Matrix>.
 - For Insight Remote Support central connect only: The RIBCL credentials for the server have been entered in the Insight RS Console and are associated with the ProLiant server.
2. Initiate the data collection process from the **Remote Support→Data Collections** page in the iLO web interface. For instructions, see “[Sending data collection information](#)” (page 139). The OS name and version are forwarded to Insight RS and Insight Online during the data collection process.
3. If you had an active Insight Online session when you performed [Step 2](#), click the refresh button (C) to update the Insight Online view.
If AMS is installed and the OS was running during the most recent data collection transmission, the OS name and version are listed on the Insight Online **Device Configuration Details** page.

Connection error during Insight Online direct connect registration

Symptom

The following error occurs when you try to register a server for Insight Online direct connect:
Cannot connect to remote host.

Cause

The DNS settings are not configured correctly in iLO.

Action

Verify that the DNS information is configured correctly in iLO.

For instructions, see “[iLO network settings](#)” (page 96).

iLO session ends unexpectedly during iLO Insight Online direct connect registration

Symptom

The iLO web interface session ends unexpectedly with the error Session Expired when you try to register a server for Insight Online direct connect.

Cause

The DNS settings are not configured correctly in iLO.

Action

Verify that the DNS settings are configured correctly.

Server health status is red in Insight RS or Insight Online

Symptom

A server that is registered for remote support is displayed with red status in Insight RS or Insight Online.

Cause

The server warranty expired.

Action

You must have a valid contract or warranty to receive remote support.

You can continue to use the iLO features to monitor and manage your server, even after the warranty expires.

iLO Federation issues

Query errors occur on iLO Federation pages

Symptom

When you open an iLO Federation page, iLO peers and associated data might be missing from the page, and the following error is displayed:

Errors occurred during query, returned data may be incomplete or inconsistent.

Cause

This error might occur when a network communication error, configuration problem, or failed iLO system prevents the retrieval of data from all systems in an iLO Federation group.

Action

Try the following:

- Wait for twice the configured **Multicast Announcement Interval**, and then refresh the iLO Federation page. If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire.
- Check the **Multi-System Map** page for errors. This page can help you identify communication problems between iLO peers.
- If you are using server blades in a BladeSystem enclosure, verify that **Enclosure iLO Federation Support** is configured on the **Enclosure Settings**→**Network Access**→**Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This configuration is required to allow peer-to-peer communication between the server blades in an enclosure.
- Verify that the switches in the network are configured to allow communication between iLO peers.
- If you changed the network routes, subnet mask, IP address, or HTTP port for an iLO peer, verify that the peer has a communication path to the local iLO system.
- Ensure that a communication path exists between the local iLO system and the peer with the error. An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

More information

[Viewing the iLO Federation Multi-System Map](#)

[iLO Multi-System Map page displays a 502 error](#)
[A timeout error is displayed on the iLO Multi-System Map page](#)
[iLO Multi-System Map page displays a 403 error](#)
[Configuring Enclosure iLO Federation Support](#)
[iLO Federation network requirements](#)
[iLO network settings](#)
[iLO access settings](#)

A timeout error is displayed on the iLO Multi-System Map page

Symptom

The **Multi-System Map** page displays a `Timed Out` error for a peer of the local iLO system.

Cause

This error might occur in the following situations:

- A peer of the local iLO system has a peer that has failed.
- An intermediate firewall is preventing communication between the local iLO system and a peer.
- Network configuration changes are preventing communication between the local iLO system and a peer.
- The enclosure that contains the peer is not configured for iLO Federation support.

Action

Try one of the following:

- Remove or repair the failed peer.
- Verify that the network is configured to allow communication between the iLO peers.
- Verify that the enclosure that contains an iLO server blade peer is configured for iLO Federation support on the **Enclosure Settings**→**Network Access**→**Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This configuration is required to allow peer-to-peer communication between the server blades in an enclosure.

More information

[Configuring Enclosure iLO Federation Support](#)
[iLO Federation network requirements](#)

iLO Multi-System Map page displays a 502 error

Symptom

The **Multi-System Map** page shows a 502 error.

Cause

The listed peer rejected a request from the local iLO system.

Action

Ensure that a communication path exists between the local iLO system and the peer with the error. An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

iLO Multi-System Map page displays a 403 error

Symptom

The **Multi-System Map** page shows a 403 Forbidden/Authorization error.

Cause

The group key on the local iLO system does not match the group key on a peer iLO system.

Action

Ensure that the group key matches for all iLO systems that are members of the selected group.

iLO peers are not displayed on iLO Federation pages

Symptom

iLO peers (systems in the same group as the local iLO system) are not displayed on iLO Federation pages.

Action

Try the following:

- Ensure that the group key matches for all iLO systems that are members of the selected group.
- Wait for twice the configured multicast interval, and then refresh the iLO Federation page. If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire.
- If you are using server blades in an enclosure, verify that **Enclosure iLO Federation Support** is configured on the **Enclosure Settings**→**Network Access**→**Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This configuration is required to allow peer-to-peer communication between the server blades in an enclosure.
- Verify that the switches in the network are configured to allow communication between iLO peers.
- Ensure that a communication path exists between the local iLO system and the peer with the error. An intermediate firewall or a change to the iLO network configuration and HTTP port setting might block communication between the local iLO system and the peer.

More information

[Configuring Enclosure iLO Federation Support](#)
[iLO Federation network requirements](#)

iLO peers are displayed with IPv6 addresses on IPv4 networks

Symptom

iLO peers on an IPv4 network are displayed with IPv6 addresses on iLO Federation pages.

Action

If the network is configured to use IPv4 only, verify that the **iLO Client Applications use IPv6 first** check box is not selected on the **Network**→**iLO Dedicated Network Port**→**IPv6** page.

More information

[Configuring IPv6 settings](#)

Firmware update issues

Unsuccessful iLO firmware update

Symptom

The following issues occur when you try to update the iLO firmware:

- iLO firmware is not responding.
- iLO did not accept the firmware update request.
- An iLO firmware update stopped before the update was complete.

Solution 1

Cause

A communication or network issue occurred.

Action

1. Attempt to connect to iLO through the web browser. If you cannot connect, there is a communication issue.
2. Attempt to ping iLO. If you are successful, the network is working.
3. Try the firmware update again.

Solution 2

Action

Try a different firmware update method.

For more information, see [“Firmware updates” \(page 35\)](#).

iLO firmware update error

Symptom

The following error is displayed during a firmware update:

The last firmware update attempt was not successful. Ready for the next update.

Cause

An incorrect file was used to update the iLO firmware.

Action

To reset the flash process, click **Clear Error**, and then try the firmware update again with the correct firmware file. If you do not clear the error, the same error might occur even when you use the correct firmware file.

iLO firmware update does not finish

Symptom

An iLO firmware update remains at 1% complete and does not finish.

Action

1. Install the HPONCFG on the server.

You can download HPONCFG from the following website: <http://www.hpe.com/support/hpesc>.

2. Open a command window.
3. Change to the directory that contains HPONCFG.
4. Enter the following command:
 - Windows: hponcfg /reset
 - Linux: hponcfg -r

The user credentials are not required when you use HPONCFG from the server OS.

5. Retry the iLO firmware update.

For information about using HPONCFG, see the iLO scripting and CLI guide.

iLO network Failed Flash Recovery

Most firmware upgrades finish successfully. In the unlikely event of server power loss during an iLO firmware upgrade, iLO might be recoverable when power is restored.

When the computer is booting, the kernel performs image validation on the main image. If the image is corrupted or incomplete, the kernel enters Failed Flash Recovery. Failed Flash Recovery activates an FTP server within iLO. The FTP server enables you to send an image to iLO for programming. The FTP server does not provide any other services.

A network client can connect to the FTP server. The user name for the connection is **test**, and the password is **flash**. To send a firmware image to iLO, use the FTP client **PUT** command. After receiving the image, iLO validates the image. If the image is a complete, signed, and valid firmware image, the kernel begins programming the FLASH partition.

After the image is programmed into the FLASH partition, reset iLO by issuing the **RESET** command to the iLO FTP server.

Example:

```
F:\ilo>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Recovery server ready.
User (192.168.1.2:(none)): ftp
331 Password required.
Password:
231 Logged in.
ftp> put iLO.bin
200 Ok.
150 ready for file
226-Checking file
226-File acceptable
226-Flashing 3% complete
226-Flashing 4% complete
226-Flashing 6% complete
.
.
.
226-Flashing 97% complete
226-Flashing 99% complete
226-Flashing 100% complete
226-Flashing completed
226 Closing file
ftp: 8388608 bytes sent in 1.38Seconds 6100.81 Kbytes/sec.
ftp> quote reset
221 Goodbye (reset).
Connection closed by remote host.
ftp> quit
```

License key installation errors

Symptom

You see a License Key Error or a License Installation Failed message.

Solution 1

Cause

The key is not an iLO license key.

Action

Obtain an iLO license key, and then try again.

Solution 2

Cause

An evaluation key was submitted when a regular license was previously installed.

Action

None. iLO does not support installing an evaluation key when a regular key was previously installed.

Solution 3

Cause

The iLO date and time settings are incorrect.

Action

Check the iLO date and time settings, and then try again.

Solution 4

Cause

The license key entered is incorrect.

Action

Check for errors in the license key, and then try again.

Unable to access Virtual Media or graphical Remote Console

Symptom

The Virtual Media and graphical Remote Console features are unavailable.

Cause

You enable the iLO Virtual Media and graphical Remote Console features by installing an optional iLO license. If a license is not installed, a message informs you that these features are not available without a license.

Action

Install an iLO license.

For details about purchasing licenses, and for a list of licensed features, see the following website:
<http://www.hpe.com/info/ilo/licensing>.

Unable to get SNMP information in HPE SIM

Symptom

HPE SIM does not receive SNMP information that passes through iLO.

Solution 1

Cause

The iLO device drivers are not installed.

The agents running on the managed server provide SNMP information to HPE SIM. For the agents to pass information through iLO, the iLO device drivers must be installed.

Action

Install the iLO device drivers.

For instructions, see “[iLO drivers and utilities](#)” (page 32).

Solution 2

Cause

iLO and the management PC are not on the same subnet.

Action

1. Ping iLO from the management PC to verify that iLO and the management PC are on the same subnet.
2. If the ping is unsuccessful, correct the network configuration.

Unable to receive HPE SIM alarms (SNMP traps) from iLO

Symptom

HPE SIM does not receive SNMP traps from iLO.

Action

1. Log in to iLO with a user account that has the Configure iLO Settings privilege.
2. Configure the alert types and SNMP trap parameters on the **Administration**→**Management** page.

Server name still present after System Erase Utility is executed

Symptom

The server name is displayed on the **iLO Overview** page after the System Erase Utility is used.

Cause

The server name, as shown on the **iLO Overview** page, is the installed host operating system name. If the Insight Management Agents are installed on the server, the agents will obtain the host name and update it on the iLO web interface page.

Action

To remove the server name after the redeployment of a server, do one of the following:

- To update the server name, load the Insight Management Agents.
- Set iLO to the factory default settings by using iLO RBSU or the iLO 4 Configuration Utility.

△ CAUTION: This procedure clears all iLO configuration information, not just the **Server Name**.

For more information, see “[Resetting iLO to the factory default settings \(iLO RBSU\)](#)” (page 197) and “[Resetting iLO to the factory default settings \(iLO 4 Configuration Utility\)](#)” (page 197).

- Change the server name on the **Administration**→**Access Settings**→**Access Options** page in the iLO web interface.

AMS is installed but unavailable in iLO

Symptom

AMS is installed on a server, but it is listed as **Not available** in the iLO web interface

Solution 1

Action

Verify that AMS is installed.

For more information, see “[Verifying the AMS installation](#)” (page 114).

Solution 2

Action

Restart AMS.

For more information, see “[Restarting AMS](#)” (page 115).

Solution 3

Action

Reset iLO.

For more information, see “[iLO diagnostics](#)” (page 193).

26 Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
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

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, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - Software Depot website:
www.hpe.com/support/softwaredepot
- 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:
www.hpe.com/support/AccessToSupportMaterials

① **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Lost license key recovery

If an iLO license key is lost, send a replacement request and your proof of purchase to one of the following email addresses:

- Americas: licensing.ams@hpe.com
- Europe, Middle East, and Africa: licensing.emea@hpe.com
- Asia-Pacific and Japan: licensing.apj@hpe.com

Websites

Website	Link
iLO 4	http://www.hpe.com/info/ilo/docs
iLO licensing	http://www.hpe.com/info/ilo/licensing
iLO mobile app	http://www.hpe.com/info/ilo/mobileapp
ProLiant Gen8 servers	http://www.hpe.com/info/proliantgen8/docs
ProLiant Gen9 servers	http://www.hpe.com/support/proliantgen9/docs
UEFI System Utilities	http://www.hpe.com/info/ProLiantUEFI/docs
Intelligent Provisioning	http://www.hpe.com/info/intelligentprovisioning/docs/
Remote Support	http://www.hpe.com/info/insightremotesupport/docs
SUM	http://www.hpe.com/info/hpsum/documentation
SPP	http://www.hpe.com/info/spp/documentation
OA	http://www.hpe.com/support/oa/docs
iLO RESTful API and RESTful Interface Tool	http://www.hpe.com/info/restfulinterface/docs
HPE SIM	http://www.hpe.com/info/insightmanagement/sim/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:
www.hpe.com/support/selfrepair

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 will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:
www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

A iLO license options

HPE iLO standard and licensed features

Table 8 (page 362) lists the features that are included with each iLO license.

Table 8 HPE iLO standard and licensed features

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Essentials	iLO Scale-Out	iLO Advanced	iLO Advanced for BladeSystem
Platform support	Ships free with all servers that have iLO in them (except BL)	Ships free with all BL servers that have iLO in them	ProLiant Gen9 100 Series and lower, ProLiant Gen8 e-series servers, and ProLiant MicroServer Gen8	ProLiant Gen9 SL, BL, XL, DL 100 and 10 series, and ProLiant Gen8 DL 160, SL, XL, and BL servers ¹	All servers that have iLO in them (except BL)	All ProLiant BladeSystem servers that have iLO in them
Embedded Health System	X	X	X	X	X	X
Virtual Power Buttons	X	X	X	X	X	X
IPMI Over LAN/DCMI	X	X	X	X	X	X
Web-Based GUI	X	X	X	X	X	X
SSH Command Line Interface	X	X	X	X	X	X
RIBCL	X	X	X	X	X	X
Virtual Serial Port	X	X	X	X	X	X
IPv6	X	X	X	X	X	X
Active Health System	X	X	X	X	X	X
Embedded Remote Support	X	X	X	X	X	X
Agentless Management	X	X	X	X	X	X
Integrated Remote Console (IRC/Virtual KVM—Supports text and graphics)	Pre-OS only	X	X	Pre-OS only	X	X
iLO Federation Discovery	X	X	X	X	X	X
iLO Federation Discovery Group License Activation	X	X	X	X	X	X

Table 8 HPE iLO standard and licensed features (continued)

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Essentials	iLO Scale-Out	iLO Advanced	iLO Advanced for BladeSystem
Platform support	Ships free with all servers that have iLO in them (except BL)	Ships free with all BL servers that have iLO in them	ProLiant Gen9 100 Series and lower, ProLiant Gen8 e-series servers, and ProLiant MicroServer Gen8	ProLiant Gen9 SL, BL, XL, DL 100 and 10 series, and ProLiant Gen8 DL 160, SL, XL, and BL servers ¹	All servers that have iLO in them (except BL)	All ProLiant BladeSystem servers that have iLO in them
Global Team Collaboration via Integrated Remote Console					X	X
Integrated Remote Console Record and Playback					X	X
Virtual Media via Integrated Remote Console		X	X		X	X
Scripted Virtual Media					X	X
Text-based Remote Console via SSH (Textcons) ²				X	X	X
Directory Service Authentication					X	X
Kerberos Authentication					X	X
Email-Based Alerting			X	X	X	X
Remote Syslog				X	X	X
Advanced Power Management (Power History Graphs, Dynamic Power Capping)				X	X	X
Virtual Serial Port Record and Playback				X	X	X
Discovery Services					X	X

Table 8 HPE iLO standard and licensed features (continued)

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Essentials	iLO Scale-Out	iLO Advanced	iLO Advanced for BladeSystem
Platform support	Ships free with all servers that have iLO in them (except BL)	Ships free with all BL servers that have iLO in them	ProLiant Gen9 100 Series and lower, ProLiant Gen8 e-series servers, and ProLiant MicroServer Gen8	ProLiant Gen9 SL, BL, XL, DL 100 and 10 series, and ProLiant Gen8 DL 160, SL, XL, and BL servers ¹	All servers that have iLO in them (except BL)	All ProLiant BladeSystem servers that have iLO in them
Smart Array Secure Encryption				X	X	X
iLO Federation Management				X	X	X

¹ When an iLO Scale-Out license is applied to a blade server, it does not remove features that are available with the iLO Standard for BladeSystem license.

² This feature is supported only on servers that are configured to use the Legacy BIOS boot mode. It is not supported on servers that are configured to use UEFI mode.

B Directory services schema

This appendix describes the classes and attributes that are used to store Lights-Out management authorization data in the directory service.

HPE Management Core LDAP OID classes and attributes

Changes made to the schema during the schema setup process include changes to the following:

- Core classes
- Core attributes

Core classes

Class name	Assigned OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Core attributes

Attribute name	Assigned OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core class definitions

The following tables define the HPE Management core classes.

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Description	This class defines target objects, providing the basis for Hewlett Packard Enterprise products that use directory-enabled management.
Class type	Structural
SuperClasses	user
Attributes	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership - 1.3.6.1.4.1.232.1001.1.1.2.2
Remarks	None

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	This class defines role objects, providing the basis for Hewlett Packard Enterprise products that use directory-enabled management.
Class type	Structural
SuperClasses	group
Attributes	hpqRoleIPRestrictions - 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault - 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction - 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership - 1.3.6.1.4.1.232.1001.1.1.2.3
Remarks	None

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	This class defines policy objects, providing the basis for Hewlett Packard Enterprise products that use directory-enabled management.
Class Type	Structural
SuperClasses	top
Attributes	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1
Remarks	None

Core attribute definitions

The following tables define the HPE Management core class attributes.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	Distinguished name of the policy that controls the general configuration of this target
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Single valued
Remarks	None

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	Provides a list of hpqRole objects that belong to this object
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Multivalued
Remarks	None

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	Provides a list of hpqTarget objects that belong to this object
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Multivalued
Remarks	None

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	A Boolean that represents access by unspecified clients and that partially specifies rights restrictions under an IP network address constraint
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	If this attribute is <code>TRUE</code> , IP restrictions will be satisfied for unexceptional network clients. If this attribute is <code>FALSE</code> , IP restrictions will be unsatisfied for unexceptional network clients.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	Provides a list of IP addresses, DNS names, domains, address ranges, and subnets that partially specify right restrictions under an IP network address constraint
Syntax	Octet String - 1.3.6.1.4.1.1466.115.121.1.40
Options	Multivalued
Remarks	<p>This attribute is used only on role objects.</p> <p>IP restrictions are satisfied when the address matches and general access is denied. They are unsatisfied when the address matches and general access is allowed.</p> <p>Values are an identifier byte followed by a type-specific number of bytes that specify a network address.</p> <ul style="list-style-type: none"> For IP subnets, the identifier is <code><0x01></code>, followed by the IP network address in network order, followed by the IP network subnet mask in network order. For example, the IP subnet 127.0.0.1/255.0.0 would be represented as <code><0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00></code>. For IP ranges, the identifier is <code><0x02></code>, followed by the lower bound IP address, followed by the upper bound IP address. Both are inclusive and in network order. For example, the IP range 10.0.0.1 to 10.0.10.255 would be represented as <code><0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF></code>. For DNS names or domains, the identifier is <code><0x03></code>, followed by the ASCII encoded DNS name. DNS names can be prefixed with an <code>*</code> (ASCII <code>0x2A</code>), to indicate they must match all names that end with the specified string. For example, the DNS domain <code>*.acme.com</code> is represented as <code><0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D></code>. General access is allowed.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	A 7-day time grid, with 30-minute resolution, which specifies rights restrictions under a time constraint
Syntax	Octet String {42} - 1.3.6.1.4.1.1466.115.121.1.40
Options	Single valued
Remarks	<p>This attribute is used only on role objects.</p> <p>Time restrictions are satisfied when the bit that corresponds to the current local time of the device is 1 and unsatisfied when the bit is 0.</p> <ul style="list-style-type: none">• The least significant bit of the first byte corresponds to Sunday, from midnight to 12:30 a.m.• Each more significant bit and sequential byte corresponds to the next consecutive half-hour blocks within the week.• The most significant (eighth) bit of the 42nd byte corresponds to Saturday at 11:30 p.m. to Sunday at midnight.

Lights-Out Management specific LDAP OID classes and attributes

The following schema attributes and classes might depend on attributes or classes defined in the HPE Management core classes and attributes.

Lights-Out Management classes

Class name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management attributes

Class name	Assigned OID
hpqLOMRRightLogin	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.6
hpqLOMRRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.1

Lights-Out Management class definitions

The following table defines the Lights-Out Management core class.

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	This class defines the rights and settings used with HPE Lights-Out Management products.
Class Type	Auxiliary

SuperClasses	None
Attributes	hpqLOMRightConfigureSettings - 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin - 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin - 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole - 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset - 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia - 1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

Lights-Out Management attribute definitions

The following tables define the Lights-Out Management core class attributes.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Login right for HPE Lights-Out Management products
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	Meaningful only on role objects. If TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Remote Console right for Lights-Out Management products. Meaningful only on role objects.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Virtual Media right for HPE Lights-Out Management products
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Remote Server Reset and Power Button right for HPE Lights-Out Management products

Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Local User Database Administration right for HPE Lights-Out Management products.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Configure Devices Settings right for HPE Lights-Out Management products.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is TRUE, members of the role are granted the right.

Glossary

3DES	Triple DES, the Data Encryption Standard cipher algorithm.
ABEND	Abnormal end.
ACPI	Advanced Configuration and Power Interface.
AES	Advanced Encryption Standard.
ALOM	Advanced Lights Out Manager.
AMP	Advanced Memory Protection.
AMS	Agentless Management Service.
API	Application Programming Interface.
ARP	Address Resolution Protocol.
ASR	Automatic Server Recovery.
BIOS	Basic Input/Output System.
BMC	Baseboard management controller.
CA	Certificate authority.
CLP	Command Line Protocol.
CN	Common Name.
COM port	Communication port.
cookie	A small, unscriptable text file placed on your hard drive by a website to preserve specific settings. When you return to the site, your system opens the cookie with the previously saved settings so they can be passed along to the site. Cookies are also used to store session data temporarily.
CR	Certificate request.
CSR	Certificate Signing Request.
CSV	Comma-separated value.
DCMI	Data Center Manageability Interface.
DD	A Unix program used to convert and copy a file.
DDNS	Dynamic Domain Name System.
DDR	Double data rate.
DER	Distinguished Encoding Rules.
DHCP	Dynamic Host Configuration Protocol.
DHE	Diffie–Hellman key exchange.
DIMM	Dual in-line memory module. A small circuit board holding memory chips.
DLL	Dynamic-link library.
DMTF	Distributed Management Task Force.
DN	Distinguished Name.
DNS	Domain Name System.
DSA	Digital Signature Algorithm.
DVO	Digital Video Out.
ECC	Error-correcting code.
EDO	Extended Data Out.
EMS	Emergency Management Services.
ESKM	Enterprise Secure Key Manager is a pre-configured security server that provides a unified service for creating, protecting, and delivering cryptographic keys to data encryption devices and applications across the distributed enterprise IT infrastructure. You can use ESKM to configure HPE Smart Array drive encryption.
FAT	File Allocation Table.

FIPS	Federal Information Processing Standard.
FQDN	Fully Qualified Domain Name.
FSMO	Flexible Single Master Operations.
GMT	Greenwich Mean Time.
GRUB	Grand Unified Bootloader.
HEM	High Efficiency Mode.
HPE SIM	HPE Systems Insight Manager.
HPLOMIG	Lights-Out Migration Utility, also called Directories Support for Management Processors.
HPONCFG	HPE Lights-Out Online Configuration Utility.
HPQLOCFG	HPE Lights-Out Configuration Utility
ICMP	Internet Control Message Protocol.
IDE	Integrated Drive Electronics.
IETF	Internet Engineering Task Force.
IIS	Internet Information Services.
iLO	Integrated Lights-Out.
IML	Integrated Management Log.
IPDU	Intelligent Power Distribution Unit.
IPMI	Intelligent Platform Management Interface.
IRC	Integrated Remote Console.
ISO	International Organization for Standardization.
Java IRC	Java version of the Integrated Remote Console.
JRE	Java Runtime Environment.
JSON	JavaScript Object Notation.
KCS	Keyboard Controller Style.
KDC	Key Distribution Center.
KDE	K Desktop Environment (for Linux).
KVM	Keyboard, video, and mouse.
LDAP	Lightweight Directory Access Protocol.
LDIFDE	A utility that allows you to import and export information to and from Active Directory.
LILO	Linux Loader.
LOM	Lights-Out Management.
MAC	Media Access Control.
MD5	Message-Digest algorithm 5.
MIB	Management Information Base. A database of managed objects accessed by network management protocols. An SNMP MIB is a set of parameters that an SNMP management station can query or set in the SNMP agent of a network device (for example, a router).
MIME	Multipurpose Internet Mail Extensions.
MLD	Multicast Listener Discovery.
MMC	Microsoft Management Console.
MSA	Mail Submission Agent.
MTA	Mail Transfer Agent.
NAND	A partition of non-volatile flash memory that is embedded on the system board of supported HPE servers. The NAND flash is used for files such as Active Health System data and the Intelligent Provisioning software.
NIC	Network interface card. A device that handles communication between a device and other devices on a network.

NMI	Non-maskable interrupt.
NTLM	NT LAN Manager.
NTP	Network Time Protocol.
NVMe	Non-Volatile Memory Express.
OA	Onboard Administrator.
OU	Active Directory Organizational Units.
PAL	Programmable Array Logic.
PDS	Power Discovery Services.
PIM	Protocol-Independent Multicast.
PKCS	Public-key cryptography standards.
POST	Power-on self test.
PuTTY	A terminal emulator that can act as a client for the SSH, Telnet, rlogin, and raw TCP protocols and as a serial console client.
RBSU	ROM-Based Setup Utility.
RDRAM	Rambus Dynamic Random Access Memory.
REST	Representational State Transfer.
RIBCL	Remote Insight Board Command Language.
RIMM	Rambus In-line Memory Module.
RPM	RPM Package Manager.
RSA	An algorithm for public-key cryptography.
SAID	Service Agreement Identifier.
SAS	Serial Attached SCSI.
SATA disk	Serial ATA (SATA) disk. The evolution of the ATA (IDE) interface that changes the physical architecture from parallel to serial and from primary-secondary (master-slave) to point-to-point. Unlike parallel ATA interfaces that connect two drives; one configured as primary (master), the other as secondary (slave), each SATA drive is connected to its own interface.
SD	Secure Digital.
SHA	Secure Hash Algorithm.
SID	Security Identifier.
SLAAC	Stateless address autoconfiguration.
SLES	SUSE Linux Enterprise Server.
SMASH	Systems Management Architecture for Server Hardware.
SMS	System Management Software.
SNMP	Simple Network Management Protocol.
SNTP	Simple Network Time Protocol.
SPN	Service principal name.
SPP	Service Pack for ProLiant.
SSD	Solid-state drive.
SSH	Secure Shell.
SSL	Secure Sockets Layer.
SSO	Single Sign-On.
SUM	Software Update Manager.
TLS	Transport layer security.
TM	Trusted Module.
TPM	Trusted Platform Module.
UDP	User Datagram Protocol.

UEFI	Unified Extensible Firmware Interface.
UHCI	Universal Host Controller Interface.
UID	Unit identification.
UPN	User principal name.
UPnP	Universal Plug and Play.
UPS	Uninterruptible Power Supply.
USB	Universal serial bus. A serial bus standard used to interface devices.
USM	User-based Security Model.
UTC	Coordinated Universal Time.
UTP	Unshielded twisted pair.
UUID	Universally unique identifier.
VSP	Virtual Serial Port.
WBEM	Web-Based Enterprise Management.
WINS	Windows Internet Name Service.

Index

Symbols

.NET IRC see Remote Console

A

access options

- Authentication Failure Logging, 67
- iLO Functionality, 144
- iLO ROM-Based Setup Utility, 144
- Require Login for iLO RBSU, 144
- Serial Command Line Interface Speed, 144
- Serial Command Line Interface Status, 144
- Show iLO IP during POST, 144

access settings

- configuring, 61

accessing

- updates, 359

accessing iLO

- troubleshooting, 323

Active Directory see directory integration

- directory objects, 295
- directory services, 294
- directory services objects, 291
- installation prerequisites, 288
- installing, 295

Snap-in installation and initialization for Active Directory, 295

Active Health System

- clearing the log, 191
- data collection, 129
- downloading the log, 190
- overview, 189

Active Health System reporting

- schedule, 140

active iLO sessions

- viewing, 152

AES/3DES

- configuring, 87
- connecting to iLO, 87
- overview, 84
- viewing, 86

Agentless Management

- configuring, 116
- overview, 112

Agentless Management Service, 349

- control panel, 114, 121
- downloading, 114
- guidelines, 114
- installing, 114
- Linux, 114
- restarting, 115
- troubleshooting, 358
- Ubuntu, 114
- verifying installation, 114
- VMware, 114
- Windows, 114

AlertMail

disabling, 126

enabling, 125

overview, 125

alerts

- AlertMail, 125
- Remote Syslog, 126
- SNMP, 119
- SNMP alert destinations, 116
- troubleshooting, 357

AMS

Proactive Care requirement, 130

Authentication Failure Logging

- using with SSH clients, 67

Authentication Passphrase

- SNMPv3, 118

Authentication Protocol

- SNMPv3, 118

Automatic Group Power Capping

- using with iLO Federation, 207

B

battery backup

- configuring iLO behavior, 254

blocked ports

- troubleshooting, 326

boot mode

- changing, 242

boot order

- changing, 242

brown-out recovery, 245

browser support

- web interface, 146

C

certificates see SSL certificates

chassis information, 259

- power supplies, 259

- smart storage battery, 261

CLI

- access setting, 144

- serial port speed, 144

collections see data collection

compatibility, directory migration, 304

configuring

- Enclosure iLO Federation Support, 59

- iLO Federation, 51, 53

- iLO Federation group memberships, 55–56

- multicast options, 52

connecting to iLO

- troubleshooting, 324–326

Console Capture, 220

contacting Hewlett Packard Enterprise, 359

control panel, 114

- Agentless Management Service, 114, 121

cookie behavior

- troubleshooting, 147

customer self repair, 360

D
data collection
Active Health System, 129
privacy, 129
Remote Support, 129
schedule
iLO, 139
sending
iLO, 139
system configuration, 129
Dedicated Network Port
enabling with iLO web interface, 99
DHCP
IPv4 settings, 102
IPv6 settings, 103
diagnostics, 193
iLO self-test results, 193
NMI, 194
Directories Support for ProLiant Management Processors
configuring directories with HPE Extended Schema, 310
Configuring directories with schema-free integration, 315
naming management processors, 309
Selecting a directory access method, 307
Setting up management processors for directories, 316
updating iLO firmware, 306
directory groups
deleting, 50
viewing, 47
directory integration
Active Directory, 78
benefits, 283
Kerberos, 278
migration, 303
overview, 284
setting up schema free directories, 285
troubleshooting, 330, 332
troubleshooting logout, 333
troubleshooting user contexts, 332
directory settings
authentication, 78–79
configuring, 78–79
directory server settings, 78–79
directory test controls, 82
Kerberos, 78
test results, 82
verifying, 81
directory tests
results, 82
running, 81
test controls, 82
Directory-enabled remote management
configuring, 297
overview, 297
requirements, 297
DNS name
default value, 31
DNS servers
IPv4, 102
IPv6, 103
documentation
providing feedback on, 361
domain name
configuring, 98
downloading
Active Health System Log, 190
drivers see iLO drivers

E
Embedded User Partition, 262
configuring, 263, 266
using, 262
Emergency Management Services
Windows EMS Console, 227
enclosure
fan control, 257
temperature, 257
viewing, 258
Enclosure iLO Federation Support
configuring, 59
verifying, 60
encryption
AES/3DES, 84
configuring, 87–88
connecting to iLO, 87
FIPS mode, 84
overview, 84
viewing, 86
Enterprise Secure Key Manager, 270
event log
clearing, 184
overview, 182
troubleshooting, 322

F
factory default settings
restoring, 197
fans
iLO Virtual Fan, 257
viewing, 154
features, 19
iLO Federation, 199
Federation see iLO Federation
FIPS mode
disabling, 88
enabling, 87
overview, 84
viewing, 86
Firefox
troubleshooting with Remote Console, 337
firmware, 35
see also iLO firmware
updating with iLO Federation, 210
viewing installed firmware, 178

G
gateway IP address

IPv4, 102
Global iLO 4 Settings *see* access options
graceful shutdown
 power, 245
groups *see* selected group list
iLO Federation, 53

H

health status
 viewing, 151
health summary
 device status, 153
 redundancy, 153
 status values, 154
 subsystem status, 153
 viewing, 153
hostname
 configuring, 98
hot keys
 Remote Console, 222
HPE Extended Schema configuration
 requirements, 288
HPE Extended Schema directory integration
 configuring, 287
HPE Insight Control software
 integration, 270
HPE schema directory integration
 overview, 287
 requirements, 290
HPLOMIG *see* Directories Support for ProLiant Management Processors
HPONCFG, 354

I

iLO
 certificate error, 327
 firmware update error, 354
 Remote Support prerequisites, 130
 sending a test event, 137
 sending Active Health System information, 140
 sending data collection information, 139
 updating firmware, 210
iLO 4 Configuration Utility, 357
 about iLO, 145
 access settings, 144
 advanced network options, 143
 network settings, 28, 142–143
 overview, 21
 rebooting iLO, 196
 resetting active connections, 196
 restoring factory default settings, 197
 setting up iLO, 27
iLO connection error
 troubleshooting, 325
iLO controls
 web interface, 148
iLO Dedicated Network Port *see* network
 link state, 99
iLO drivers
 downloading, 32
 installing, 32
 Linux, 33
 VMware, 33
 Windows, 32
iLO Federation
 adding group memberships, 55–56
 affected servers, 207
 firmware update, 212
 group membership, 59
 license installation, 214
 Virtual Media, 205
 Virtual Power, 207
Automatic Group Power Capping, 207
changing server power state, 205
configuring, 51
configuring multicast options, 52
critical and degraded systems, 201
editing group memberships, 56
features, 199
groups, 53
managing group memberships, 56
Multi-System Map, 202
network requirements, 51
power management, 205
removing group memberships, 56
server blade requirement, 59
updating firmware, 210
viewing group memberships, 54
viewing license status, 213
viewing license type, 213
viewing server health, 201
viewing server models, 201
Virtual Media, 203

iLO Federation Management
 troubleshooting, 351

iLO firmware
 downloading, 36, 210
 offline update, 36
 online update
 in-band update, 35
 out-of-band update, 35
 troubleshooting firmware updates, 354
 updating, 35, 37, 306

iLO Functionality
 configuring, 144

iLO login
 troubleshooting, 322

iLO mobile app
 overview, 21

iLO RBSU, 357
 access setting, 144
 configuring local user accounts, 144
 configuring user accounts, 29
 Global iLO 4 Settings, 144
 login requirement, 144
 network settings, 27
 overview, 21
 security, 68

setting up iLO, 27
troubleshooting, 323

iLO security
system maintenance switch, 69

iLO Shared Network Port see network

iLO web interface see web interface

Insight Management Agents
downloading, 114
installing, 114
integration, 124
overview, 112
using, 268

Integrated Management Log, 186
clearing, 188
maintenance note, 187
overview, 184
saving, 187
viewing, 185

integration
Systems Insight Manager, 275

IP address
configuring a static IP address, 27–28
IPv4, 102
IPv6, 103
viewing during POST, 144

IPMI tool usage
Advanced, 270

IPMI/DCMI
server management, 269
user privileges, 47

IPv4, 96
see also network
configuring, 102
DHCP, 102
DNS servers, 102
gateway address, 102
IP address, 102
ping gateway on startup, 102
static routes, 102
subnet mask, 102–103
WINS servers, 102

IPv6, 96
see also network
configuring, 103
DHCP, 103
DNS servers, 103
gateway address, 103
static routes, 103

J

Java IRC see Remote Console

K

Kerberos
configuring iLO
command line, 281
scripting, 281
web interface, 281
directory integration, 278

keytab file, 279
login by name, 283
single sign-on, 282–283
time requirement, 281
two-factor authentication, 278
Zero Sign In, 282–283

Kerberos authentication, 78
configuring iLO settings, 78

kernel debugging
troubleshooting, 319

key manager software
Enterprise Secure Key Manager, 270

keyboard
configuring persistent mouse and keyboard, 255

L

language packs, 149
configuring the current language, 41
configuring the default language, 41
installing, 39
overview, 38
selecting, 40
uninstalling, 41

legacy BIOS
changing the boot mode, 242
changing the boot order, 242
changing the one-time boot status, 243

licensing
installation, 42
license types, 42
options, 362
recovering lost license keys, 360
viewing in Systems Insight Manager, 277

Linux
Agentless Management Service, 114
configuring the Virtual Serial Port, 226
iLO drivers, 33
Text-based Remote Console, 230

login, 147
default user account, 31
security, 70
security banner, 92
troubleshooting, 324–325

logs
event log, 182
Remote Syslog, 126

lost license key
recovering, 360

M

maintenance note
Integrated Management Log, 187

memory information
viewing, 164

Microsoft ClickOnce
requirement, 94

Microsoft software
directory services for Active Directory, 294

migration utilities, 303

mobile app
 overview, 21
mouse
 configuring persistent mouse and keyboard, 255
multicast options
 configuring, 52

N

network, 98
 configuration summary, 96
 configuring a VLAN, 100
 configuring IPv4 settings, 102
 configuring IPv6 settings, 103
 configuring NIC settings, 99
 connecting iLO, 27
 enabling the Dedicated Network Port with iLO web interface, 99
 enabling the Shared Network Port with iLO web interface, 100
 IPv4 summary, 96
 IPv6 Summary, 96
 link state, 99
 name service limitations, 98
 namespace issues, 98
 SNTP, 108
 troubleshooting, 324–326
network failed flash recovery, 355
network requirements
 iLO Federation, 51
NIC auto-selection, 108, 110
NIC failover, 110
NIC information
 viewing, 169
NIC settings
 configuring, 99
 NIC auto-selection, 108, 110
 NIC failover, 110
NMI
 generating, 194

O

Onboard Administrator
 configuring iLO Federation support, 59
iLO option, 257
 using with iLO, 256
one-time boot status
 changing, 243
Option ROM Measuring
 viewing status, 210
overview, 19

P

password
 security, 46
ping gateway on startup
 IPv4, 102
port matching
 Systems Insight Manager, 277
ports, 326

Systems Insight Manager, 277
power
 Automatic Group Power Capping, 207
 brown-out recovery, 245
 configuring persistent mouse and keyboard, 255
 configuring threshold alerts, 254
 Dynamic Power Capping for server blades, 257
 efficiency, 246
 graceful shutdown, 245
 group power, 205
 managing server power, 247
 power capping, 253
 Power Regulator, 252
 server, 245
 system power restore setting, 248
 usage, 249
 viewing the current power state, 250
 viewing the server power history, 251
power capping
 configuring, 253
power information
 viewing, 158
Power Regulator
 configuring, 252
Power Regulator for ProLiant
 Dynamic Power Capping for server blades, 257
power settings
 configuring, 252
power switch
 Remote Console, 218
Preboot Health Summary, 320
prerequisites
 Remote Support, 130
Privacy Passphrase
 SNMPv3, 118
Privacy Protocol
 SNMPv3, 118
Proactive Care
 requirements, 130
processor information
 viewing, 163
proxy server
 using with iLO, 326

R

RBSU see iLO RBSU see system RBSU
rebooting
 iLO processor, 193
rebooting iLO, 195
 iLO 4 Configuration Utility, 196
 UID button, 196
Remote Console
 .NET IRC requirements, 216
 acquiring, 218
 computer lock settings, 93
 configuring trust settings (.NET IRC), 94
 Console Capture, 220
 creating hot keys, 222
 Inactive .NET IRC, 341

power switch, 218
sharing, 219
starting, 217
text-based, 224
troubleshooting, 337–338, 345, 356
using .NET IRC and Java IRC, 215
using Virtual Media, 219
remote management tool
 deleting the configuration, 274
 starting, 149, 273
 viewing, 273
Remote Support
 configuring web proxy settings, 132
 data collection, 129
 direct connect registration, 132
 editing the web proxy settings, 134
 iLO connection error, 350
 iLO session ends during registration, 350
 overview, 128
 prerequisites, 130
 server identification, 349
 service events, 129
 SSL Bio Error during registration, 348
 system configuration, 129
 troubleshooting server and operating system name, 349
remote support, 360
Remote Syslog
 configuring, 126
 disabling, 127
 enabling, 126
Require Login for iLO RBSU
 configuring, 144
requirements
 HPE Extended Schema configuration, 288
 HPE schema directory integration, 290
 Virtual Media, 232
Reset to Factory Defaults, 357
resetting
 iLO processor, 193
resetting iLO *see* rebooting iLO
RESTful API
 overview, 21
RESTful Interface Tool
 overview, 21
restoring
 factory default settings, 197

S

schema documentation, 365
Core attribute definitions, 366
Core class definitions, 365
Lights-Out Management attributes, LDAP, 368–369
Lights-Out Management classes, LDAP, 368
Lights-Out Management specific LDAP OID classes and attributes, 368
schema free directories
 configuring, 287
iLO web interface, 286
 nested groups, 287
 RIBCL scripts, 286
 setting up, 285
scripting and command line
 overview, 21
SD-Card
 status, 151
security
 configuring, 68
 guidelines, 68
 iLO RBSU, 68
 login, 70
 login security banner, 92
 passwords, 46
 TM support, 69
 TPM support, 69
 user account privileges, 70
 user accounts, 70
Security Name
 SNMPv3, 118
selected group list, 199
 filter criteria, 200
 filtering, 200
Serial Command Line Interface Speed
 configuring, 144
Serial Command Line Interface Status
 configuring, 144
serial label pull tab, 31
server
 managing power, 247
 managing with IPMI, 269
 powering on, 245
server blades
 verifying iLO Federation capability, 60
server firmware
 downloading, 37, 210
 updating, 37
Server Name
 clearing, 357
servers
 Automatic Group Power Capping, 207
 connecting Virtual Media, 203
 ejecting Virtual Media, 204
 group power, 205
 health status, 201
 license status, 213
 license type, 213
 updating firmware, 210
 viewing connected Virtual Media, 204
service events
 Remote Support, 129
 sending a test event
 iLO, 137
setting up iLO
 network connection, 27
 overview, 27
 preparation, 23
 static IP address, 27–28
 user accounts, 29, 70

using iLO 4 Configuration Utility, 27
using iLO RBSU, 27
web interface, 31

Shared Network Port
enabling with iLO web interface, 100

FlexibleLOM, 99
LOM, 99

Show iLO IP during POST
configuring, 144

single sign-on
configuring, 89
Kerberos, 282–283
privileges, 89
removing trusted certificates, 92
trust mode, 89
trusted certificates, 90
viewing trusted certificates, 91

smart storage battery, 163, 261

SNMP, 119
see also SNMP alerts
configuring, 116
configuring alerts, 119, 121
configuring SNMPv3 users, 118
overview, 112
Receiving alerts in Systems Insight Manager, 276
trap definitions, 121

SNMP alerts
Cold Start Trap Broadcast, 119
Forward Insight Manager Agent SNMP Alerts, 119
iLO SNMP Alerts, 119
sending test alerts, 119
SNMPv1 Traps, 119
Trap Source Identifier, 119

SNMP Pass-thru
configuring, 116

SNMPv3
Authentication Passphrase, 118
Authentication Protocol, 118
configuring the engine ID, 119
Privacy Passphrase, 118
Privacy Protocol, 118
Security Name, 118

SNTP
configuring, 108

software
HPE software, 180
installed software, 181
running software, 180
viewing, 179

SSH
authentication failure logging, 67
authorizing keys, 71–72
authorizing keys from Systems Insight Manager, 73
deleting keys, 73
key administration, 71
key requirements, 73
troubleshooting, 347

SSL
certificates, 74

importing certificates, 75
troubleshooting certificates, 325
viewing certificates, 74

SSL certificates
importing, 75
obtaining, 75

SSO
configuring with Systems Insight Manager, 275

static routes
IPv4, 102
IPv6, 103

status information
viewing, 151

subnet mask
IPv4, 102

support
Hewlett Packard Enterprise, 359

system information
viewing, 150, 152

system maintenance switch
overview, 69

System Management Homepage, 124

system RBSU
configuring the Virtual Serial Port, 224

Systems Insight Manager
authorizing SSH keys, 73
configuring single sign-on, 275
iLO identification, 276
iLO license, 277
iLO links, 276
integrating with iLO, 275
overview, 275
port matching, 277
single sign-on, 91
SNMP alerts, 276
troubleshooting, 357
viewing iLO, 276
viewing iLO status, 276

T

temperature information
temperature graph, 155
viewing, 155

Text-based Remote Console, 230
customizing, 229
Linux sessions, 230
overview, 224
Textcons, 228
troubleshooting, 346

Textcons see Text-based Remote Console

time zone
SNTP, 108

TM
using, 69

TPM
using, 69

Troubleshooting
Preboot health summary, 320
troubleshooting, 202

Agentless Management Service, 358
blocked ports, 326
booting to DOS, 345
certificate error, 327
cookies, 147
directory integration, 330, 332
directory logout, 333
event log, 322
event log entry time stamps, 322
iLO access, 323
iLO Federation
 403 error, 353
 502 error, 352
 iLO peer IP addresses, 353
 peers not displayed, 353
 query errors, 351
 timeout error, 352
iLO Federation Management, 351
iLO firmware update, 354
iLO RBSU, 323
iLOconnection error, 325
Inactive .NET IRC, 341
IRC failed to connect to server error message, 342
kernel debugging, 319
ktpass utility, 333
login, 322, 324–325
network failed flash recovery, 355
Remote Console, 337–338, 345, 356
Remote Support, 348–350
SSH, 347
Systems Insight Manager alarms, 357
text-based Remote Console, 346
unable to connect to iLO, 324–326
Virtual Media, 343, 345, 356
trust settings
 Remote Console, 94
Trusted Module
 status, 151
Trusted Platform Module
 status, 151
two-factor authentication
 Kerberos, 278

U

Ubuntu
 Agentless Management Service, 114

UEFI
 changing the boot mode, 242
 changing the boot order, 242
 changing the one-time boot status, 243

UEFI Shell
 Embedded User Partition, 263, 266

UEFI System Utilities
 configuring the Virtual Serial Port, 225
 Embedded User Partition, 263

UID button
 rebooting iLO, 196

updates
 accessing, 359

user accounts
 adding, 29–30, 45
 default user account, 31
 deleting, 50
 directory authentication, 78
 editing, 31, 45
 enabling local accounts, 78–79, 144
 IPMI/DCMI, 47
 overview, 44
 privileges, 44, 70
 removing, 31
 security, 70
 viewing, 44
User-based Security Model
 SNMPv3, 118

V

virtual fan, 257

Virtual Media
 changing the port, 234
 connecting to groups, 203
 disconnecting from groups, 204
 IIS, scripted media, 239
 local media, 235
 OS information, 232
 overview, 231
 scripted media, 235
 scripting, IIS requirements, 239
 troubleshooting, 343, 345, 356
 using from web interface, 234
 using with iLO Federation, 203
 using with Remote Console, 219

Virtual Power button
 using with iLO Federation, 205
 viewing affected servers, 207

Virtual Serial Port
 configuring with system RBSU, 224
 configuring with UEFI System Utilities, 225
 Linux configuration, 226
 overview, 224
 Windows configuration, 227

VLAN
 configuring, 100

VMware
 Agentless Management Service, 114
 iLO drivers, 33

W

web interface
 browser support, 146
 enabling the Dedicated Network Port, 99
 enabling the Shared Network Port, 100
 iLO controls, 148
 overview, 19
 using, 146

websites
 customer self repair, 360

Windows
 Agentless Management Service, 114

enabling EMS Console, 227
iLO drivers, 32
WINS servers
 IPv4, 102

Z

Zero Sign In
 Kerberos, 282–283