Hewlett Packard
Enterprise

HPE iLO 4 2.81 User Guide

Part Number: 30-5AF37350-004
Published: September 2022
Edition: 1

HPE iLO 4 2.81 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: 30-5AF37350-004
Published: September 2022
Edition: 1

© Copyright 2012-2022 Hewlett Packard Enterprise Development LP

Notices

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.

Acknowledgments

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

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

Google™ is a trademark of Google Inc.

Google Chrome™ browser is a trademark of Google Inc.

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

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

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

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

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

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

Revision history

Part Number	Publication date	Edition	Summary of changes
30-5AF37350-004	September 2022	1	Updated iLO encryption details
30-5AF37350-003	April 2022	1	Updated iLO encryption details
684918-405a	May 2019	2	Updated troubleshooting solution for iLO firmware update does not finish .

Part Number	Publication date	Edition	Summary of changes
684918-405	April 2019	1	Added support for HTML5 Integrated Remote Console. Updated directory configuration information to support OpenLDAP directory servers. Updated default value (Disabled) for IPMI/DCMI over LAN in iLO 4 2.60 and later. Added information about viewing iLO health status on the Overview and Login pages. Added new Key Manager support. Minor updates and corrections.
684918-404a	October 2018	2	Minor updates and corrections
684918-404	October 2016	1	Updates for iLO 4 2.50

Table of contents

1 iLO

- 1.1 iLO features
- 1.2 iLO web interface
- 1.3 ROM-based configuration utilities
- 1.4 iLO mobile app
- 1.5 iLO RESTful API
- 1.6 RESTful Interface Tool
- 1.7 iLO scripting and command line
- 1.8 iLO Amplifier Pack
- 1.9 HPE InfoSight for servers

2 Setting up iLO

- 2.1 Preparing to set up iLO
  - 2.1.1 iLO network connection options
  - 2.1.2 NIC teaming with Shared Network Port configurations
    - 2.1.2.1 NIC teaming constraints
    - 2.1.2.2 Hewlett Packard Enterprise NIC teaming modes
  - 2.1.3 iLO IP address acquisition
  - 2.1.4 iLO access security
  - 2.1.5 iLO configuration tools
- 2.2 Initial setup steps: Process overview
- 2.3 Connecting iLO to the network
- 2.4 Setting up iLO by using the ROM-based setup utilities
  - 2.4.1 Configuring a static IP address with the ROM-based setup utilities
    - 2.4.1.1 Configuring a static IP address (iLO RBSU)
    - 2.4.1.2 Configuring a static IP address (iLO 4 Configuration Utility)
  - 2.4.2 Managing local user accounts with the ROM-based setup utilities
    - 2.4.2.1 Adding user accounts (iLO RBSU)
    - 2.4.2.2 Editing user accounts (iLO RBSU)
    - 2.4.2.3 Removing user accounts (iLO RBSU)
    - 2.4.2.4 Adding user accounts (iLO 4 Configuration Utility)
    - 2.4.2.5 Editing or removing user accounts (iLO 4 Configuration Utility)
- 2.5 iLO setup with the web interface
- 2.6 Logging in to iLO for the first time
  - 2.6.1 iLO default DNS name and user account
- 2.7 iLO licensed features
- 2.8 iLO drivers and utilities
  - 2.8.1 Windows driver support
  - 2.8.2 Linux driver and utility support
  - 2.8.3 VMware driver support
- 2.9 Installing the iLO drivers and utilities
  - 2.9.1 Obtaining the iLO drivers and utilities
  - 2.9.2 Driver and utility installation with the SPP

2.9.3 Loading hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux
2.9.4 Removing hp-health for SUSE Linux Enterprise Server and Red Hat Enterprise Linux
2.9.5 Installing hp-health for Ubuntu
2.9.6 Removing hp-health for Ubuntu
3 Updating iLO firmware, language, and licensing
3.1 Firmware updates
3.1.1 Online firmware update
3.1.1.1 In-band firmware update methods
3.1.1.2 Out-of-band firmware update methods
3.1.2 Offline firmware update
3.1.2.1 Offline firmware update methods
3.1.3 Supported firmware types
3.1.4 Obtaining the iLO firmware image file
3.1.5 Obtaining supported server firmware image files
3.1.5.1 Server firmware file type details
3.1.6 Updating iLO or server firmware by using the iLO web interface
3.1.7 Requirements for firmware update to take effect
3.2 Language packs
3.2.1 Installing language packs
3.2.2 Selecting a language pack
3.2.3 Configuring the default language settings
3.2.4 Configuring the current iLO web interface session language
3.2.5 Uninstalling a language pack
3.2.6 How iLO determines the session language
3.3 iLO licensing
3.3.1 License key information
3.3.2 Installing a license key by using a browser
3.3.3 Viewing license information
3.3.3.1 License details
4 Managing user accounts and directory groups
4.1 iLO user accounts
4.1.1 Adding local user accounts
4.1.2 Editing local user accounts
4.1.3 Viewing local user accounts
4.1.4 Deleting a user account
4.1.5 iLO user account options
4.1.6 iLO user privileges
4.1.7 Password guidelines
4.1.8 IPMI/DCMI users
4.2 iLO directory groups
4.2.1 Adding directory groups
4.2.2 Editing directory groups
4.2.3 Viewing directory groups
4.2.4 Deleting a directory group

4.2.5 Directory group options
4.2.6 Active Directory nested groups (schema-free configuration only)
4.2.7 Directory group privileges
5 Configuring iLO Federation
5.1 iLO Federation settings
5.2 Prerequisites for using the iLO Federation features
5.3 iLO Federation network requirements
5.4 Configuring the multicast options for one iLO system at a time
5.4.1 Multicast options
5.5 iLO Federation groups
5.5.1 iLO Federation group memberships for local iLO systems
5.5.2 iLO Federation group memberships for a set of iLO systems
5.5.3 iLO Federation group privileges
5.5.4 iLO Federation group characteristics
5.6 Managing iLO Federation group memberships (local iLO system)
5.6.1 Adding iLO Federation group memberships
5.6.2 Editing iLO Federation group memberships
5.6.3 Removing a group membership from a local iLO system
5.6.4 Viewing iLO Federation group memberships (local iLO system)
5.7 Adding iLO Federation group memberships (multiple iLO systems)
5.7.1 Adding a group based on an existing group
5.7.2 Creating a group from a filtered list of servers
5.7.3 Servers affected by a group membership change
5.8 Configuring Enclosure iLO Federation Support
5.8.1 Verifying server blade support for iLO Federation
6 Configuring the iLO security features
6.1 General security guidelines
6.2 Managing SSH keys
6.2.1 Authorizing a new SSH key by using the web interface
6.2.2 Authorizing a new SSH key by using the CLI
6.2.3 Deleting SSH keys
6.2.4 Requirements for authorizing SSH keys from an HPE SIM server
6.2.5 SSH keys
6.2.6 Supported SSH key format examples
6.3 Administering SSL certificates
6.3.1 Viewing SSL certificate information
6.3.1.1 SSL certificate details
6.3.2 Obtaining and importing an SSL certificate
6.3.2.1 Obtaining a trusted certificate from a CA
6.3.2.1.1 CSR input details
6.3.2.1.2 Certificate signing requests
6.3.2.2 Importing a trusted certificate
6.3.3 Removing a customized certificate
6.4 Directory authentication and authorization settings in iLO

6.4.1 Prerequisites for configuring authentication and directory server settings
6.4.2 Configuring Kerberos authentication settings in iLO
6.4.2.1 Kerberos settings
6.4.3 Configuring schema-free directory settings in iLO
6.4.3.1 Schema-free directory settings
6.4.4 Configuring HPE Extended Schema directory settings in iLO
6.4.4.1 HPE Extended Schema directory settings
6.4.5 Directory user contexts
6.4.6 Directory Server CA Certificate
6.4.7 Deleting a directory server CA certificate
6.4.8 Local user accounts with Kerberos authentication and directory integration
6.4.9 Running directory tests
6.4.9.1 Directory test input values
6.4.9.2 Directory test status values and controls
6.4.9.3 Directory test results
6.4.9.4 iLO directory tests
6.5 Configuring encryption settings
6.5.1 Modifying the AES/DES encryption setting
6.5.2 Connecting to iLO by using AES or 3DES encryption
6.5.3 Enabling FIPS mode
6.5.4 Configuring a FIPS-validated environment with iLO
6.5.5 Viewing encryption settings
6.5.5.1 Encryption settings
6.5.6 Disabling FIPS mode
6.5.7 iLO encryption details
6.6 HPE SSO
6.6.1 Configuring iLO for HPE SSO
6.6.2 Single Sign-On Trust Mode options
6.6.3 SSO user privileges
6.6.4 Adding trusted certificates
6.6.4.1 Trusted certificate format
6.6.4.2 Extracting the HPE SIM SSO certificate
6.6.5 Importing a direct DNS name
6.6.6 Viewing trusted certificates and records
6.6.6.1 Trusted certificate and record details
6.6.7 Removing trusted certificates and records
6.7 Configuring the Login Security Banner
6.8 Configuring remote console computer lock settings
6.8.1 Remote console computer lock options
6.9 Configuring the Integrated Remote Console Trust setting (.NET IRC)
6.9.1 Integrated Remote Console Trust setting options
6.10 iLO security with the system maintenance switch
7 Configuring iLO access settings
7.1 Configuring iLO service settings

7.1.1 Service settings
7.2 Configuring iLO access options
7.2.1 Access options
7.3 Login security
7.4 iLO login with an SSH client
8 Configuring iLO network settings
8.1 iLO network settings
8.2 Viewing the network configuration summary
8.2.1 Network configuration summary details
8.2.2 IPv4 Summary details
8.2.3 IPv6 Summary details
8.3 General network settings
8.3.1 Configuring the iLO Hostname Settings
8.3.1.1 iLO hostname and domain name limitations
8.3.2 NIC settings
8.3.2.1 Enabling the iLO Dedicated Network Port through the iLO web interface
8.3.2.1.1 Link State values
8.3.2.2 Enabling the iLO Shared Network Port through the iLO web interface
8.3.2.2.1 Shared Network Port options
8.3.2.3 iLO network port configuration options
8.3.2.4 iLO network connection considerations
8.4 Configuring IPv4 settings
8.4.1 DHCPv4 settings
8.4.2 General IPv4 settings
8.4.3 IPv4 DNS server settings
8.4.4 WINS server settings
8.4.5 Ping Gateway on Startup setting
8.5 Configuring IPv6 settings
8.5.1 DHCPv6 settings
8.5.2 IPv6 DNS server settings
8.5.3 General IPv6 settings
8.5.4 iLO features that support IPv6
8.6 Configuring iLO SNTP settings
8.6.1 SNTP options
8.6.2 iLO clock synchronization
8.6.3 DHCP NTP address selection
8.7 iLO NIC auto-selection
8.7.1 NIC auto-selection support
8.7.2 iLO startup behavior with NIC auto-selection enabled
8.7.3 Enabling iLO NIC auto-selection
8.7.4 Configuring NIC failover
8.8 Viewing iLO systems in the Windows Network folder
9 Configuring iLO management settings
9.1 iLO SNMP management

9.2 Agentless Management Service and the Insight Management Agents
9.2.1 Installing AMS or the Insight Management Agents
9.2.2 Verifying AMS installation
9.2.2.1 Verifying AMS status: iLO web interface
9.2.2.2 Verifying AMS status: Windows
9.2.2.3 Verifying AMS status: SUSE Linux Enterprise Server and Red Hat Enterprise Linux
9.2.2.4 Verifying AMS status: VMware
9.2.2.5 Verifying AMS status: Ubuntu
9.2.3 Restarting AMS
9.2.4 Nagios plug-in for Agentless Management
9.3 Configuring SNMP settings
9.3.1 SNMP options for all configurations
9.3.2 SNMP options for Agentless Management only
9.4 SNMPv3 authentication
9.4.1 Configuring SNMPv3 users
9.4.1.1 SNMPv3 user options
9.4.2 Deleting an SNMPv3 user profile
9.4.3 Configuring the SNMPv3 Engine ID
9.5 Configuring SNMP alerts
9.5.1 SNMP alert settings
9.6 Using the AMS Control Panel to configure SNMP and SNMP alerts (Windows only)
9.7 SNMP traps
9.8 REST alerts
9.9 Configuring Insight Management integration
9.9.1 Insight Management integration options
9.10 iLO AlertMail
9.10.1 Enabling AlertMail
9.10.1.1 AlertMail options
9.10.2 Disabling AlertMail
9.11 Remote syslog
9.11.1 Enabling iLO remote syslog
9.11.1.1 Remote syslog options
9.11.2 Disabling iLO Remote Syslog
10 Managing remote support
10.1 HPE embedded remote support
10.1.1 Device support
10.1.2 Data collected by HPE remote support
10.1.3 HPE Tech Care service
10.2 Prerequisites for remote support registration
10.2.1 Supported browsers for HPE embedded remote support
10.2.2 Setting up a ProLiant server for remote support registration
10.2.3 Insight Online direct connect network requirements
10.2.4 Setting up the Insight Remote Support central connect environment
10.2.5 Verifying access to Insight Online

10.3 Registering for Insight Online direct connect
10.3.1 Registering for Insight Online direct connect (step 1)
10.3.2 Registering for Insight Online direct connect (step 2)
10.3.3 Confirming registration is complete (iLO web interface)
10.3.4 Completing the optional post-registration steps
10.4 Editing the web proxy settings (Insight Online direct connect only)
10.5 Registering for Insight Remote Support central connect
10.6 Unregistering from Insight Online direct connect
10.7 Unregistering from Insight Remote Support central connect
10.8 Remote support service events
10.8.1 Service event transmission
10.8.2 Using maintenance mode
10.8.3 Sending a test service event
10.8.3.1 Viewing a test service event by using Insight Online
10.8.3.2 Viewing a test service event by using the Insight RS Console
10.8.4 Viewing the service event log
10.8.4.1 Service event log details
10.8.4.2 Supported service event types
10.8.5 Clearing the Service Event Log
10.9 Remote Support data collection
10.9.1 Sending data collection information
10.9.2 Sending Active Health System reporting information
10.9.3 Viewing data collection status in iLO
10.9.3.1 Data Collection details
10.9.4 Viewing Active Health System reporting status in iLO
10.9.4.1 Active Health System reporting details
10.9.5 Viewing data collection status in Insight Online
10.9.6 Viewing data collection status in the Insight RS Console (Insight Remote Support central connect only)
10.10 Registering a ProLiant server used as a host server for Insight Online direct connect
10.11 Changing the remote support configuration of a supported device
10.11.1 Changing a supported device from central connect to direct connect remote support
10.11.2 Changing a supported device from direct connect to central connect remote support
11 Managing iLO with the ROM-based utilities
11.1 iLO ROM-based utilities
11.2 Configuring network settings with the ROM-based utilities
11.2.1 Configuring NIC and TCP/IP settings (iLO RBSU)
11.2.2 Configuring DNS/DHCP settings (iLO RBSU)
11.2.3 Configuring advanced network settings (iLO RBSU)
11.2.4 Configuring Network Options (iLO 4 Configuration Utility)
11.2.5 Configuring Advanced Network Options (iLO 4 Configuration Utility)
11.2.6 Network Options
11.2.7 Advanced Network Options
11.3 Configuring access settings with the ROM-based utilities
11.3.1 Configuring global settings (iLO RBSU)

11.3.2 Configuring serial CLI options (iLO RBSU)
11.3.3 Configuring access settings (iLO 4 Configuration Utility)
11.4 Viewing information about iLO by using the iLO 4 Configuration Utility
11.4.1 About iLO
12 Using the iLO web interface
12.1 Browser requirements
12.2 Supported browsers
12.3 Enabling JavaScript for Internet Explorer
12.4 Logging in to the iLO web interface
12.5 Cookie sharing between browser instances and iLO
12.6 iLO web interface overview
12.6.1 iLO controls
12.7 Starting a remote management tool from the login page
12.8 Changing the language from the login page
13 Viewing iLO overview and system information
13.1 Viewing iLO overview information
13.1.1 System information details
13.1.2 System status details
13.1.3 Connection to HPE status
13.1.4 Active sessions list
13.2 Viewing health summary information
13.2.1 Redundancy status
13.2.2 Subsystem and device status
13.2.3 Subsystem and device status values
13.3 Viewing fan information
13.3.1 Fan details
13.3.2 Fans
13.4 Temperature information
13.4.1 Viewing the temperature graph
13.4.1.1 Temperature graph details
13.4.2 Viewing temperature sensor data
13.4.2.1 Temperature sensor details
13.4.3 Temperature monitoring
13.5 Viewing power information
13.5.1 Power Supply Summary details
13.5.2 Power Supplies list
13.5.3 Power Discovery Services iPDU Summary
13.5.4 Power Readings
13.5.5 Power Microcontroller
13.5.6 Smart Storage Battery details
13.5.7 Power monitoring
13.5.8 High Efficiency Mode
13.6 Viewing processor information
13.6.1 Processor details

13.7 Viewing memory information
13.7.1 Advanced Memory Protection details
13.7.2 Memory Summary
13.7.3 Memory Details
13.8 Viewing network information
13.8.1 Physical Network Adapters
13.8.2 Logical Network Adapters
13.9 Viewing the device inventory
13.9.1 Device Inventory details
13.9.2 Device status values
13.9.3 Viewing PCI slot details
13.9.3.1 PCI slot tooltip details
13.10 Viewing storage information
13.10.1 Supported storage components
13.10.2 Smart Array details
13.10.2.1 Controllers
13.10.2.2 Drive Enclosures
13.10.2.3 Logical Drives
13.10.2.4 Physical Drives
13.10.3 Direct-attached storage details
13.10.3.1 Controllers
13.10.3.2 Physical Drives
13.11 Viewing installed firmware information
13.11.1 Firmware types
13.11.2 Firmware details
13.12 Viewing software information
13.12.1 HPE Software List details
13.12.2 Running Software details
13.12.3 Installed Software details
14 Using the iLO logs
14.1 iLO Event Log
14.1.1 Viewing the event log
14.1.1.1 Event log view controls
14.1.1.2 Event log details
14.1.1.3 Event log icons
14.1.2 Saving the event log to a CSV file
14.1.3 Clearing the event log
14.2 Integrated Management Log
14.2.1 Viewing the IML
14.2.1.1 IML view controls
14.2.1.2 IML details
14.2.1.3 IML icons
14.2.2 Marking an IML entry as repaired
14.2.3 Adding a maintenance note to the IML

14.2.4 Saving the IML to a CSV file
14.2.5 Clearing the IML
14.2.6 IML troubleshooting links
15 Using the Active Health System
15.1 Active Health System
15.2 Active Health System data collection
15.3 Active Health System Log
15.4 Active Health System Log download methods
15.5 Downloading the Active Health System Log for a date range
15.6 Downloading the entire Active Health System Log
15.7 Downloading the Active Health System Log by using cURL
15.7.1 cURL command usage with iLO
15.8 Downloading the Active Health System log (iLOREST)
15.8.1 iLOREST serverlog command usage
15.9 Clearing the Active Health System Log
16 Using the iLO diagnostics, reboot, and reset features
16.1 Viewing iLO self-test results
16.1.1 Self-test details
16.2 Generating an NMI
16.3 Formatting the Embedded Flash
16.4 Configuring redundant ROM
16.5 iLO reboot (reset)
16.5.1 iLO reboot (reset) methods
16.5.2 Rebooting (resetting) iLO with the web interface
16.5.3 Rebooting (resetting) iLO with the iLO 4 Configuration Utility
16.5.4 Performing a graceful iLO reboot with the server UID button
16.5.5 Performing a hardware iLO reboot with the server UID button
16.6 Reset iLO to the factory default settings
16.6.1 Resetting iLO to the factory default settings (iLO RBSU)
16.6.2 Resetting iLO to the factory default settings (iLO 4 Configuration Utility)
17 Using the iLO Federation features
17.1 iLO Federation
17.2 Selected Group list
17.2.1 Selected Group list filters
17.2.2 Selected Group list filter criteria
17.3 Exporting iLO Federation information to a CSV file
17.4 iLO Federation Multi-System view
17.4.1 Viewing server health and model information
17.4.1.1 Server health and model details
17.4.2 Viewing servers with critical and degraded status
17.4.2.1 Critical and degraded server status details
17.5 Viewing the iLO Federation multi-system map
17.5.1 iLO peer details
17.6 iLO Federation Group Virtual Media

17.6.1 Connecting scripted media for groups
17.6.2 Viewing scripted media status for groups
17.6.2.1 Scripted media details
17.6.3 Ejecting a scripted media device
17.6.4 Servers affected by a group virtual media action
17.7 iLO Federation Group Power
17.7.1 Changing the power state for a group of servers
17.7.2 Power state options for groups
17.7.3 Servers affected by a group power state change
17.8 Configuring group power capping
17.8.1 Group power capping considerations
17.8.2 Viewing group power capping information
17.8.2.1 Power capping details
17.9 iLO Federation group firmware update
17.9.1 Updating the firmware for multiple servers
17.9.2 Viewing group firmware information
17.9.2.1 Firmware details
17.9.3 Servers affected by a group firmware update
17.10 Installing license keys (iLO Federation group)
17.10.1 Servers affected by a license installation
17.10.2 Viewing iLO Federation group license information
17.10.2.1 iLO Federation group license details
18 iLO Remote Console
18.1 Starting the integrated remote console
18.1.1 Starting the HTML5 IRC
18.1.2 Starting the HTML5 IRC from the Overview page
18.1.3 HTML5 remote console modes
18.1.4 HTML5 remote console controls
18.1.5 Starting the .NET IRC
18.1.6 Starting the .NET IRC from the Overview page
18.1.7 .NET IRC requirements
18.1.8 Starting the Java IRC (Oracle JRE)
18.1.9 Starting the Java IRC (Oracle JRE) from the Overview page
18.1.10 Starting the Java IRC (OpenJDK JRE)
18.1.11 Acquiring the remote console
18.1.12 Joining a Shared Remote Console session (.NET IRC only)
18.1.12.1 Shared remote console (.NET IRC only)
18.1.13 Viewing the remote console status bar
18.1.13.1 Remote console status bar details
18.2 Integrated remote console features
18.2.1 Keyboard actions with the IRC
18.2.1.1 Sending a keyboard action with the HTML5 IRC
18.2.1.2 Sending a keyboard action with the .NET IRC or Java IRC
18.2.1.3 Sending a remote console hot key

18.2.1.4 Changing the keyboard layout in the HTML5 IRC
18.2.2 Virtual power IRC features
18.2.2.1 Using the remote console virtual power switch with the HTML5 IRC
18.2.2.2 Using the remote console virtual power switch with the .NET IRC or Java IRC
18.2.3 Virtual power button options
18.2.4 Virtual media IRC features
18.2.4.1 Using a virtual drive (physical drive on a client PC)
18.2.4.2 Using a local IMG or ISO file with the HTML5 IRC
18.2.4.3 Using a local IMG or ISO file with the .NET IRC or Java IRC
18.2.4.4 Using a virtual drive to install an OS and provide a required driver (.NET IRC or Java IRC)
18.2.4.5 Using a URL-based image file with the HTML5 IRC
18.2.4.6 Using a URL-based image file with the .NET IRC or Java IRC
18.2.4.7 Using a virtual folder (.NET IRC only)
18.2.4.7.1 Virtual folders
18.2.4.8 Create Media Image feature (Java IRC only)
18.2.4.8.1 Creating a disk image file (Java IRC)
18.2.4.8.2 Copying data from an image file to a physical disk (Java IRC)
18.2.5 Console capture (.NET IRC)
18.2.5.1 Console capture controls
18.2.5.2 Viewing server startup and server prefailure sequences
18.2.5.3 Saving server startup and server prefailure video files
18.2.5.4 Capturing video files with the remote console
18.2.5.5 Viewing saved video files with the remote console
18.2.6 Screen captures with the IRC
18.2.6.1 Capturing the HTML5 remote console screen
18.2.6.2 Capturing the .NET IRC screen
18.3 Remote console hot keys
18.3.1 Creating remote console hot keys
18.3.2 Keys for configuring remote console computer lock keys and hot keys
18.3.3 Resetting hot keys
18.3.4 Viewing configured remote console hot keys (Java IRC)
19 Using a text-based Remote Console
19.1 iLO Virtual Serial Port
19.1.1 Configuring the iLO Virtual Serial Port in the host system RBSU
19.1.2 Configuring the iLO Virtual Serial Port in the UEFI System Utilities
19.1.3 Configuring Linux to use the iLO Virtual Serial Port
19.1.3.1 Configuring Red Hat Enterprise Linux 6 to use the iLO Virtual Serial Port
19.1.3.2 Configuring Red Hat Enterprise Linux 7 to use the iLO Virtual Serial Port
19.1.3.3 Configuring SUSE Linux Enterprise Server to use the iLO Virtual Serial Port
19.1.4 Windows EMS Console with iLO Virtual Serial Port
19.1.4.1 Configuring Windows for use with the iLO Virtual Serial Port
19.1.5 Starting an iLO Virtual Serial Port session
19.1.6 Viewing the iLO Virtual Serial Port log
19.2 Text-based Remote Console (Textcons)

19.2.1 Using the Text-based Remote Console
19.2.2 Linux with the Text-based Remote Console
19.2.3 Customizing the Text-based Remote Console
20 Using iLO virtual media
20.1 Virtual media considerations
20.2 Virtual media operating system information
20.2.1 Operating system USB requirement
20.2.2 Configuring Windows 7 for use with iLO Virtual Media
20.2.3 Operating system considerations: Virtual Floppy/USB key
20.2.3.1 Changing diskettes
20.2.4 Operating system considerations: Virtual CD/DVD-ROM
20.2.4.1 Mounting a USB virtual media CD/DVD-ROM (Linux command line)
20.3 iLO web interface Virtual Media options
20.3.1 Viewing and modifying the Virtual Media port
20.3.2 Viewing connected local media
20.3.2.1 Local media details
20.3.3 Ejecting a local virtual media device
20.3.4 Connecting scripted media
20.3.5 Viewing connected scripted media
20.3.5.1 Scripted media details
20.3.6 Ejecting scripted media
20.4 Setting up IIS for scripted virtual media
20.4.1 Configuring IIS
20.4.2 Configuring IIS for read/write access
20.4.3 Inserting virtual media with a helper application
20.4.4 Sample virtual media helper application
20.5 Boot Order
20.5.1 Configuring the server boot mode
20.5.2 Configuring the server boot order
20.5.3 Changing the one-time boot status
20.5.3.1 Changing the one-time boot status in Legacy BIOS mode
20.5.3.2 Changing the one-time boot status in UEFI mode
20.5.4 Using the additional Boot Order page options
21 Using the power management features
21.1 Server power-on
21.2 Brownout recovery
21.3 Graceful shutdown
21.4 Power efficiency
21.5 Power-on protection
21.6 Power allocation (blade servers and compute modules)
21.7 Managing the server power
21.7.1 Virtual power button options
21.8 Configuring the System Power Restore Settings
21.8.1 Auto Power-On

21.8.2 Power-On Delay
21.9 Viewing server power usage
21.9.1 Power meter graph details
21.9.2 Power meter graph display options
21.9.3 Viewing the current power state
21.9.3.1 Current power state details
21.9.4 Viewing the server power history
21.9.4.1 Power history details
21.10 Power settings
21.10.1 Configuring Power Regulator settings
21.10.1.1 Power Regulator modes
21.10.2 Configuring power caps
21.10.2.1 Power capping considerations
21.10.3 Configuring battery backup unit settings
21.10.3.1 Battery backup unit options
21.10.4 Configuring SNMP alert on breach of power threshold settings
21.10.4.1 SNMP Alert on breach of power threshold options
21.10.5 Configuring the persistent mouse and keyboard
22 Working with enclosures, frames, and chassis
22.1 Onboard Administrator
22.1.1 Viewing OA information
22.1.1.1 OA details
22.1.2 Starting the OA GUI
22.1.3 Toggling the enclosure UID LED
22.1.4 Enclosure bay IP addressing
22.1.5 Dynamic Power Capping for server blades
22.1.6 iLO virtual fan
22.1.7 iLO option
22.2 Viewing frame information
22.2.1 Frame details
22.2.2 Toggling the frame or compute module UID
22.3 Viewing chassis information
22.3.1 Power Supplies list
22.3.2 Intelligent PDU details
22.3.3 Smart Storage Battery details
23 Using the Embedded User Partition
23.1 iLO Embedded User Partition
23.2 Embedded User Partition use cases
23.3 Configuring the Embedded User Partition
23.3.1 Configuring the Embedded User Partition (UEFI System Utilities)
23.3.2 Configuring the Embedded User Partition (UEFI Shell)
23.4 Configuring the Embedded User Partition boot settings
23.4.1 Configuring the Embedded User Partition boot order setting (iLO web interface)
23.4.2 Configuring the Embedded User Partition for one-time boot (iLO web interface)

23.4.3 Configuring the Embedded User Partition boot order setting (UEFI System Utilities)
23.4.4 Configuring the Embedded User Partition for one-time boot (UEFI System Utilities)
23.4.5 Configuring the Embedded User Partition boot order setting (UEFI Shell)
23.4.6 Configuring the Embedded User Partition for one-time boot (UEFI Shell)
24 Using iLO with other software products and tools
24.1 Viewing Location Discovery Services information
24.1.1 Location Discovery Services details
24.1.2 Location Discovery Services
24.2 Opening the System Management Homepage
24.3 IPMI server management
24.3.1 Advanced IPMI tool usage on Linux
24.4 Using key managers with iLO
24.4.1 Supported key managers
24.4.2 Configuring key manager servers
24.4.2.1 Key manager server options
24.4.3 Adding key manager configuration details
24.4.3.1 Key manager configuration details
24.4.4 Testing the key manager configuration
24.4.5 Viewing key manager events
24.4.6 Clearing the key manager log
24.5 iLO and remote management tools
24.5.1 Starting a remote management tool from iLO
24.5.2 Deleting a remote manager configuration
24.5.3 Using iLO with HPE OneView
24.5.3.1 Server signatures (Synergy compute modules only)
24.6 Adding hotfixes to create an HPE OneView custom firmware bundle
24.7 Using HPE Smart Update Manager to create a custom ISO on Windows
24.8 Using iLO with HPE SIM
24.8.1 HPE SIM features
24.8.2 Establishing SSO with HPE SIM
24.8.3 iLO identification and association
24.8.3.1 Viewing iLO status in HPE SIM
24.8.3.2 iLO links in HPE SIM
24.8.3.3 Viewing iLO in HPE SIM System lists
24.8.4 Receiving SNMP alerts in HPE SIM
24.8.5 iLO and HPE SIM HTTP port matching requirement
24.8.6 Reviewing iLO license information in HPE SIM
25 Setting up Kerberos authentication and directory services
25.1 Kerberos authentication with iLO
25.1.1 Configuring Kerberos authentication: Process overview
25.1.2 Configuring the iLO hostname and domain name for Kerberos authentication
25.1.2.1 iLO hostname and domain name requirements for Kerberos authentication
25.1.3 Preparing the domain controller for Kerberos support
25.1.4 Generating a keytab file for iLO in a Windows environment

25.1.4.1 Ktpass
25.1.4.2 Setspn
25.1.5 Verifying that your environment meets the Kerberos authentication time requirement
25.1.6 Configuring supported browsers for single sign-on
25.1.6.1 Enabling single sign-on in Microsoft Internet Explorer
25.1.6.2 Enabling single sign-on in Mozilla Firefox
25.1.6.3 Single-sign on with Google Chrome
25.1.6.4 Enabling single sign-on in Microsoft Edge
25.1.6.5 Verifying the single sign-on (Zero Sign In) configuration
25.1.6.6 Verifying that login by name works
25.2 Directory integration benefits
25.3 Choosing a directory configuration to use with iLO
25.4 Schema-free directory authentication
25.4.1 Configuring iLO for schema-free directory integration: Process Overview:
25.4.2 Prerequisites for using schema-free directory integration
25.5 HPE Extended Schema directory authentication
25.5.1 Directory services support
25.5.2 Configuring the HPE Extended Schema with Active Directory: Process overview
25.5.3 Prerequisites for configuring Active Directory with the HPE Extended Schema configuration
25.5.4 Installing the iLO directory support software
25.5.4.1 Directories Support for ProLiant Management Processors install options
25.5.5 Running the Schema Extender
25.5.5.1 Schema Extender required information
25.5.6 Directory services objects
25.5.7 Management options added by the HPE Active Directory snap-ins
25.5.7.1 Setting a client IP address or DNS name restriction
25.5.8 Directory-enabled remote management (HPE Extended Schema configuration)
25.5.8.1 Roles based on organizational structure
25.5.8.2 How role access restrictions are enforced
25.5.8.3 User access restrictions
25.5.8.4 Role access restrictions
25.5.9 Configuring Active Directory and HPE Extended Schema (Example configuration)
25.5.9.1 Creating and configuring directory objects for use with iLO in Active Directory
25.5.9.1.1 Creating the iLOs organizational unit and adding LOM objects
25.5.9.1.2 Creating the Roles organizational unit and adding role objects
25.5.9.1.3 Assigning rights to the roles and associating the roles with users and devices
25.5.9.2 Configuring iLO and associating it with a Lights-Out Management object
25.6 User login using directory services
25.7 Tools for configuring multiple iLO systems at a time
25.8 Directories Support for ProLiant Management Processors (HPLOMIG)
25.9 Configuring directory authentication with HPLOMIG
25.9.1 Discovering management processors
25.9.1.1 HPLOMIG management processor search criteria
25.9.1.2 HPLOMIG management processor import list requirements

25.9.2 (Optional) Upgrading firmware on management processors (HPLOMIG)
25.9.3 Selecting directory configuration options
25.9.3.1 Management processor selection methods
25.9.3.2 Directory access methods and settings
25.9.4 Naming management processors (HPE Extended Schema only)
25.9.5 Configuring directories when HPE Extended Schema is selected
25.9.5.1 Configure directory window options
25.9.6 Configuring management processors (Schema-free configuration only)
25.9.6.1 Management processor settings
25.9.7 Setting up management processors for directories
25.9.8 Importing an LDAP CA Certificate
25.9.9 (Optional) Running directory tests with HPLOMIG
25.10 Directory services schema
25.10.1 HPE Management Core LDAP OID classes and attributes
25.10.2 Core class definitions
25.10.3 Core attribute definitions
25.10.4 Lights-Out Management specific LDAP OID classes and attributes
25.10.5 Lights-Out Management attributes
25.10.6 Lights-Out Management class definitions
25.10.7 Lights-Out Management attribute definitions
26 Using the iLO mobile app
26.1 iLO mobile app features
26.2 iLO mobile app limitations
26.3 Using the iLO mobile app on an Android device
26.3.1 Adding an iLO system to the mobile app
26.3.2 Adding an iLO system to the mobile app by scanning a QR code
26.3.3 Editing the list of iLO systems
26.3.4 Deleting an iLO system from the list
26.3.5 Viewing the list of iLO systems
26.3.6 Starting the remote console
26.3.7 Remote console usage
26.3.8 Mobile app keyboard usage
26.3.9 Supported remote console gestures
26.3.10 Launching a script stored on a web server
26.3.11 Starting the iLO web interface
26.3.12 Clearing the iLO mobile app history
26.4 Using the iLO mobile app on an iOS device
26.4.1 Adding an iLO system to the mobile app
26.4.2 Adding an iLO system to the mobile app by scanning a QR code
26.4.3 Editing the list of iLO systems
26.4.4 Deleting iLO systems from the list
26.4.5 Viewing the list of iLO systems
26.4.6 Starting the remote console
26.4.7 Remote console usage

26.4.8 Mobile app keyboard usage
26.4.9 Supported remote console gestures
26.4.10 Launching a script stored on a web server
26.4.11 Starting the iLO web interface
26.4.12 Clearing the iLO mobile app history
26.5 iLO mobile app feedback
27 Troubleshooting
27.1 Using the iLO Virtual Serial Port with Windbg
27.2 Using the ProLiant Preboot Health Summary
27.2.1 Preboot Health Summary details
27.3 Event log entries
27.4 Incorrect time stamp on iLO Event Log entries
27.5 Login and iLO access issues
27.5.1 iLO firmware login name and password not accepted
27.5.2 iLO management port not accessible by name
27.5.3 iLO RBSU unavailable after iLO and server reset
27.5.4 Unable to access the iLO login page
27.5.5 Unable to return to iLO login page after iLO reset
27.5.6 Unable to connect to iLO after changing network settings
27.5.7 An iLO connection error occurs after an iLO firmware update
27.5.8 Unable to connect to iLO processor through NIC
27.5.9 Unable to log in to iLO after installing iLO certificate
27.5.10 Unable to connect to iLO IP address
27.5.11 iLO TCP/IP communication fails
27.5.12 Secure Connection Failed error when using Firefox to connect to iLO
27.5.13 Security warning when navigating to iLO web interface with Internet Explorer
27.5.14 Certificate error when navigating to iLO web interface with Edge
27.5.15 Security warning when navigating to iLO web interface with Chrome
27.5.16 Security warning when navigating to iLO web interface with Firefox
27.5.17 iLO login page displays a Website Certified by an Unknown Authority message
27.5.18 iLO inaccessible on a server managed by HPE OneView
27.5.19 Unable connect to an iLO system with the iOS mobile app
27.5.20 iLO responds to pings intermittently or does not respond
27.5.21 Running an XML script with iLO fails
27.5.22 A certificate warning is displayed when you try to open the iLO online help in Microsoft Edge (legacy)
27.6 Directory issues
27.6.1 Logging in to iLO with Kerberos authentication fails
27.6.2 iLO credential prompt appears during Kerberos login attempt
27.6.3 iLO credential prompt appears during Kerberos login by name attempt
27.6.4 A directory connection to iLO ends prematurely
27.6.5 Configured directory user contexts do not work with iLO login
27.6.6 A directory user account does not log out after the directory timeout expires
27.6.7 Failure generating Kerberos keytab file for iLO Zero Sign In configuration
27.6.8 Error when running Setspn for iLO Kerberos configuration

27.6.9 OpenLDAP authentication fails when configured with nested groups or posixgroups
27.6.10 iLO Zero Sign In fails after domain controller OS reinstall
27.6.11 Failed iLO login with Active Directory credentials
27.6.12 Directory Server DNS Name test reports a failure
27.6.13 Ping Directory Server test reports a failure
27.6.14 Connect to Directory Server test reports a failure
27.6.15 Connect using SSL test reports a failure
27.6.16 Bind to Directory Server test reports a failure
27.6.17 Directory Administrator Login test reports a failure
27.6.18 User Authentication test reports a failure
27.6.19 User Authorization test reports a failure
27.6.20 Directory User Contexts test reports a failure
27.6.21 LOM Object Exists test reports a failure
27.7 Remote Console issues
27.7.1 Caps Lock out of sync between Remote Console and client keyboard
27.7.2 Num Lock out of sync between Remote Console and client keyboard
27.7.3 Session leader does not receive connection request when .NET IRC is in replay mode
27.7.4 Keystrokes repeat unintentionally during Remote Console session
27.7.5 Cursor cannot reach Remote Console window corners
27.7.6 Remote Console text window not updated correctly
27.7.7 Remote Console keyboard LED does not work correctly
27.7.8 File not present after copy from server to virtual media USB key
27.7.9 Unable to boot to DOS using a USB key mounted with the Remote Console
27.7.10 Remote Console hot key does not work in the HTML5 IRC
27.7.11 Pressing CTRL+ALT+DEL in the Remote Console affects only the client OS
27.7.12 Keyboard input has unexpected effects when using HTML5 IRC
27.7.13 .NET IRC sends characters continuously after switching windows
27.7.14 .NET IRC becomes inactive or disconnects
27.7.15 .NET IRC failed to connect to server
27.7.16 .NET IRC takes a long time to verify application requirements (Internet Explorer)
27.7.17 .NET IRC displays a dialog box that says the application cannot be started (Internet Explorer)
27.7.18 .NET IRC displays a dialog box that says the application cannot be started (new Microsoft Edge)
27.7.19 .NET IRC displays a dialog box that says the application is improperly formatted
27.7.20 .NET IRC displays a security warning dialog box
27.7.21 .NET IRC cannot be shared
27.7.22 The .NET IRC will not start in the legacy version of Microsoft Edge
27.7.23 The .NET IRC will not start in the new Microsoft Edge
27.7.24 Mouse or keyboard does not work in the Integrated Remote Console
27.7.25 Java IRC displays red X when Firefox is used to run Java IRC on Linux client
27.8 SSH issues
27.8.1 Initial PuTTY input slow with iLO
27.8.2 PuTTY client unresponsive with iLO Shared Network Port
27.8.3 Text is displayed incorrectly when using an SSH connection to iLO
27.8.4 An SSH session fails to start or terminates unexpectedly

27.9 Text-based Remote Console issues
27.9.1 Unable to view Linux installer in text-based Remote Console
27.9.2 Unable to pass data through SSH terminal
27.9.3 VSP-driven selection during the serial timeout window sends output to BIOS redirect instead of VSP
27.9.4 Scrolling and text appear irregular during BIOS redirection
27.10 Remote Support issues
27.10.1 SSL Bio Error during Insight RS registration
27.10.2 Server not identified by server name in Insight Online or Insight RS
27.10.3 Server OS name and version not listed in Insight RS or Insight Online
27.10.4 Connection error during Insight Online direct connect registration
27.10.5 iLO session ends unexpectedly during iLO Insight Online direct connect registration
27.10.6 Server health status is red in Insight RS or Insight Online
27.11 iLO Federation issues
27.11.1 Query errors occur on iLO Federation pages
27.11.2 A timeout error is displayed on the iLO Multi-System Map page
27.11.3 iLO Multi-System Map page displays a 502 error
27.11.4 iLO Multi-System Map page displays a 403 error
27.11.5 iLO peers are not displayed on iLO Federation pages
27.11.6 iLO peers are displayed with IPv6 addresses on IPv4 networks
27.12 Firmware issues
27.12.1 Unsuccessful iLO firmware update
27.12.2 iLO firmware update error
27.12.3 iLO firmware update does not finish
27.12.4 iLO network Failed Flash Recovery
27.13 License key installation errors
27.14 Unable to access Virtual Media or graphical Remote Console
27.15 Unable to get SNMP information in HPE SIM
27.16 Unable to receive HPE SIM alarms (SNMP traps) from iLO
27.17 Server name present after System Erase Utility is executed
27.18 AMS is installed but unavailable in iLO
27.19 OS installation from a Virtual Media device fails on a server that uses the iLO Shared Network Port
28 Websites
29 Support and other resources
29.1 Accessing Hewlett Packard Enterprise Support
29.2 Accessing updates
29.3 Remote support
29.4 Customer self repair
29.5 Warranty information
29.6 Regulatory information
29.7 Documentation feedback

iLO

HPE iLO 4 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. iLO management is a powerful tool that provides multiple ways to configure, update, monitor, and repair servers remotely. iLO (Standard) comes preconfigured on Hewlett Packard Enterprise servers without any additional cost or license.

Features that enhance server administrator productivity are licensed. For more information, see the HPE iLO Licensing Guide.

iLO features

iLO includes the following standard and licensed features. To view the license requirements for these features, see the iLO licensing guide.

- **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 or upload the log to the Active Health System Viewer.
- **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.
- **Deployment and provisioning**—Use Virtual Power and Virtual Media for tasks such as the automation of deployment and provisioning.
- **Embedded remote support**—Register a supported server for HPE remote support.
- **iLO Federation management**—Use the iLO Federation features to discover and manage multiple servers at a time.
- **Integrated Management Log**—View server events and configure notifications through SNMP alerts, remote syslogs, and email alerts.
- **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.
- **Power consumption and power settings**—Monitor the server power consumption, configure server power settings, and configure power capping on supported servers.
- **Power management**—Securely and remotely control the power state of the managed server.
- **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.
- **User access**—Use local or directory-based user accounts to log in to iLO.
- **Virtual Media**—Remotely mount high performance Virtual Media devices to the server.

iLO web interface

You can use the iLO web interface to access iLO through a supported browser to monitor and configure managed servers.

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.

iLO mobile app

The iLO mobile app provides access to supported servers from a mobile device. The mobile app interacts directly with the iLO processor, providing total control of the server as long as it 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.

iLO RESTful API

iLO 4 2.00 and later includes the iLO RESTful API. The iLO RESTful API is a management interface you can use with server management tools to perform server configuration, inventory, and monitoring tasks. Use a REST client, such as the RESTful Interface Tool, to send HTTPS operations (`GET`, `PUT`, `POST`, `PATCH`, and `DELETE`) to the iLO web server.

iLO 4 2.30 and later is Redfish 1.0-conformant while remaining backward compatible with previous versions of the iLO RESTful API.

You can use the iLO RESTful API to access iLO Standard features. To access licensed features, install an iLO license.

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

RESTful Interface Tool

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

For more information, see the following website: **https://www.hpe.com/info/resttool**.

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 Amplifier Pack

The iLO Amplifier Pack is an advanced server inventory and firmware and driver update solution. It uses iLO Advanced functionality to enable rapid discovery, detailed inventory reporting, and firmware and driver updates. The iLO Amplifier Pack performs rapid server discovery and inventory for thousands of supported servers for the purpose of updating firmware and drivers at scale.

For more information about iLO Amplifier Pack, see the following website: **https://www.hpe.com/servers/iloamplifierpack**.

HPE InfoSight for servers

The HPE InfoSight portal is a secure web interface hosted by HPE that allows you to monitor supported devices through a graphical interface.

HPE InfoSight for servers:

- Combines the machine learning and predictive analytics of HPE InfoSight with the health and performance monitoring of Active Health System (AHS) and HPE iLO to optimize performance and predict and prevent problems
- Provides automatic collection and analysis of the sensor and telemetry data from AHS to derive insights from the behaviors of the install base to provide recommendations to resolve problems and improve performance

For more information on getting started and using HPE InfoSight for servers, go to: **https://www.hpe.com/info/infosight-servers-docs**.

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:

Procedure

1. How will 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?

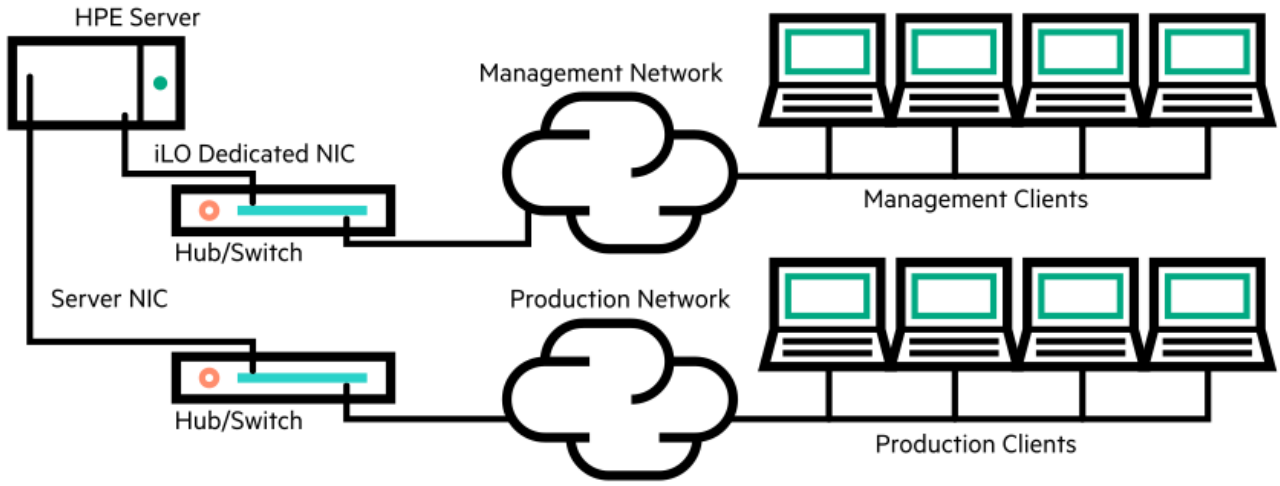
iLO network connection options

You can connect iLO 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

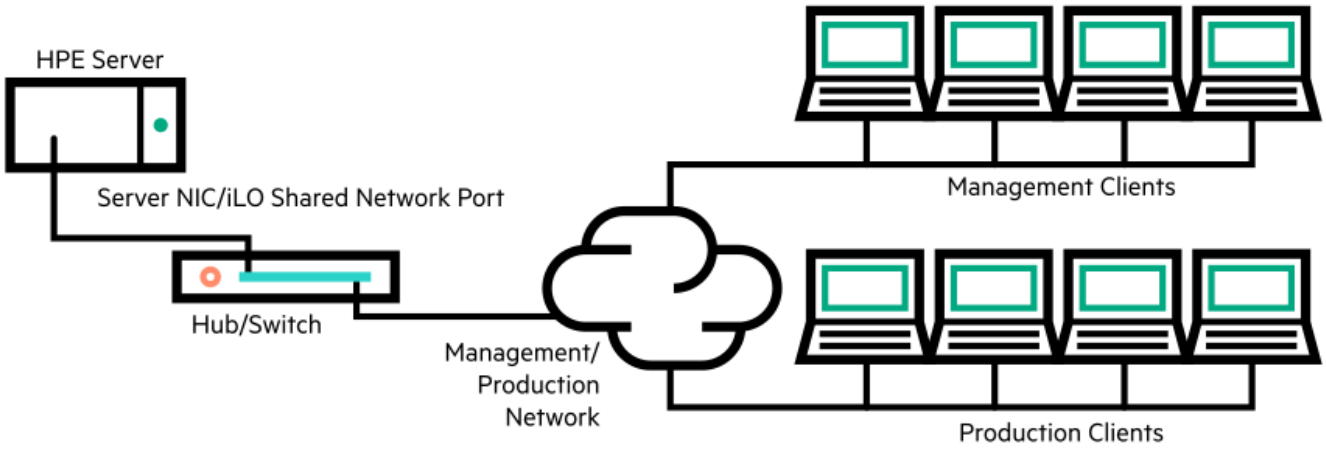
In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO from anywhere on the network. Using a Shared Network Port configuration 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 server startup, and when the operating system NIC drivers are loading and unloading, there are brief periods of time (2–8 seconds) when you cannot access iLO from the network. After these short periods, iLO communication is restored and iLO will respond to network traffic.

  When this situation occurs, the Remote Console and connected iLO Virtual Media devices might be disconnected.
- Network controller firmware updates or resets can also cause iLO to be unreachable over the network for a brief period of time.
- The iLO Shared Network Port connection cannot operate at a speed greater than 100 Mbps. Network-intensive tasks such as data transfer through iLO virtual media might be slower than the same tasks performed in a configuration that uses the iLO Dedicated Network Port.

Figure 2: Shared network connection


HPE Server
Server NIC/iLO Shared Network Port
Hub/Switch
Management/
Production
Network
Management Clients
Production Clients

NIC teaming with Shared Network Port configurations

NIC teaming is a feature you can use to improve server NIC performance and reliability.

NIC teaming constraints

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.

Network Fault Tolerance

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

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

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 switch assisted load balancing, see the switch vendor documentation.

For additional information, see the **ProLiant Network Adapter Teaming support document**.

For information about selecting a NIC teaming mode when your server uses another implementation of NIC teaming, see NIC teaming constraints and the 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.

Dynamic IP 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.

Static IP address

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.

Login security with local accounts is managed through the iLO Access Settings and user privileges.

Directory services

To support more than 12 users, configure iLO to use a directory service to authenticate and authorize access. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise.

If you plan to use directory services, consider enabling at least one local administrator account for alternative access.

A directory provides a central point of administration for iLO devices and users, and the directory can enforce a strong password policy.

iLO configuration tools

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

ROM-based setup

Use iLO RBSU or the iLO 4 Configuration Utility when the system environment does not use DHCP, DNS, or WINS.

iLO web interface

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

To start Intelligent Provisioning, press F10 during POST. For information about the iLO settings you can configure, see the Intelligent Provisioning user guide.

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**—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 iLO 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 command-line 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 through 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 the HPE OneView user guide.

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.

Procedure

1. Review the General security guidelines for setting up and using iLO.
2. Connect iLO to the network.
3. If you are not using dynamic IP addressing, use the ROM-based setup utilities to configure a static IP address.
4. If you will use the local accounts feature, use the ROM-based setup utilities to configure user accounts.
5. Optional: Install an iLO license.
6. 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.

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**.

For more information about the iLO ROM-based utilities and their features, see iLO ROM-based utilities.

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)

Procedure

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 boxes.
   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)

Procedure

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)

Procedure

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.

Editing user accounts (iLO RBSU)

Procedure

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.

Removing user accounts (iLO RBSU)

Procedure

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)

Procedure

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.

Editing or removing user accounts (iLO 4 Configuration Utility)

Procedure

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 5, 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.

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

Procedure

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.

> **TIP:**
>
> After you log in to iLO for the first time, Hewlett Packard Enterprise recommends changing the password for the default user account.

iLO default DNS name and user account

The iLO firmware is configured with a default user name, password, and DNS name. The default 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 string
- **DNS name**—ILOXXXXXXXXXXX, where the **X** characters represent the server serial number.

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 user credentials (on the serial label pull tab) to log in after the reset.

iLO licensed features

iLO (Standard) is preconfigured on Hewlett Packard Enterprise servers without an additional cost or license. Features that enhance productivity are licensed. For more information, see the iLO licensing guide at the following website: **http://www.hpe.com/info/ilo-docs**.

To activate iLO licensed features, install an iLO license.

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.

Windows driver support

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

iLO 4 Channel Interface Driver for Windows

This driver (`hpqilo3chif.sys`) allows software to communicate with iLO. The driver is used by the ProLiant Monitor service, Insight Management Agents and WBEM Providers, Agentless Management Service, and other utilities. Install this driver in all configurations.

iLO 4 Management Controller Driver Package for Windows

This package includes the ProLiant Monitor service and the `hpqilo3core.sys` driver to support Automatic Server Recovery.

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.

  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: `ilo`.

This driver manages Agentless Management Service, 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

Procedure

- **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.

  You can download some of the components separately at the Hewlett Packard Enterprise Support Center website: **http://www.hpe.com/support/ilo4**.

- **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.

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

Procedure

To load `hp-health`, enter the following command: `rpm -ivh hp-health-<d.vv.v-pp.Linux_version.arch>.rpm`.

In this command, `<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

Procedure

To remove `hp-health`, enter the following command: `rpm -e hp-health`.

Installing hp-health for Ubuntu

Procedure

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: **http://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

Procedure

To remove `hp-health`, enter the following command: `apt-get remove hp-health`.

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 iLO 4 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.

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.

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.

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.

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.

iLO RESTful API

Use the iLO RESTful API and a REST client such as the RESTful Interface Tool to update firmware.

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.

HPLOMIG (also called Directories Support for ProLiant Management Processors)

You do not need to use directory integration to take advantage of the HPLOMIG firmware update capabilities. HPLOMIG 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.

LOCFG.PL

Use a Perl sample to send RIBCL scripts to iLO over the network.

Offline firmware update

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

Offline firmware update methods

SPP

Download the SPP and use it to install or update firmware.

SUM

Use SUM to perform firmware, driver, and software maintenance on supported servers and other nodes.

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.

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

You can download the iLO firmware image file and use it to update a single server or multiple servers in a group.

The BIN file from the iLO Online Flash Component is required for updating the iLO firmware with the Flash Firmware or Group Firmware Update features.

Procedure

1. Navigate to the following website: **http://www.hpe.com/support/hpesc**.
2. To locate and download the iLO Online Flash Component file, follow the onscreen instructions.

   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:
     - `#./<firmware_file_name>.scexe -unpack=/tmp/`
     - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

   The name of the iLO firmware image file is similar to `iLO 4_<yyy>.bin`, where `<yyy>` represents the firmware version.

Obtaining supported server firmware image files

Procedure

1. Navigate to the following website: **http://www.hpe.com/support/hpesc**.
2. To locate and download an Online ROM Flash Component file, follow the onscreen instructions.
3. If you downloaded a Windows component:
   a. Double-click the downloaded file, and then click the Extract button.
   b. Select a location for the extracted files, and then click OK.
4. If you downloaded a Linux component:

   Depending on the file format, enter one of the following commands:

   - `#./<firmware_file_name>.scexe -unpack=/tmp/`
   - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

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

Procedure

1. Obtain an iLO firmware or server firmware file.
2. Navigate to the Administration > Firmware page.
3. Depending on the browser you use, click Browse or Choose File, and then specify the location of the firmware image file.
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.

   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.
8. Optional: To confirm that the new firmware is active, check the version on the System Information > Firmware page.

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 and the Integrated Remote Console.

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, version 2.20 or later) replaces the installed language pack.
- iLO 4 2.20 or later requires version 2.20 or later of the iLO language packs.
- 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 Integrated Remote Console uses 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

Procedure

1. Download a language pack from the following website: **http://www.hpe.com/support/ilo4**.
2. To extract the contents, double-click the downloaded file.

   The language pack file name is similar to the following: `lang_<language>_<version>.lpk`.
3. Navigate to the Administration > Access Settings > Language page.
4. Depending on the browser you use, click Browse or Choose File.
5. Select the language pack, and then click Open.
6. Click Install.

   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.

   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:

Procedure

- Navigate to the login page, and then select a language in the Language menu.
- Click the Language menu at the bottom of any iLO web interface page, and then select a language.
- Select a language on the Administration > Access Settings > Language page.

Configuring the default language settings

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

Prerequisites

- Configure iLO Settings privilege
- The language pack for the language you want to use is installed.
- The language you want to use is installed in the browser and it is set to take priority over the other installed browser languages.

Procedure

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 iLO web interface session language

Procedure

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

Procedure

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.

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.
- An iLO Advanced license is automatically included with Synergy compute modules. You cannot add or remove a license on Synergy compute modules.
- Use the Licensing and Group Licensing pages to view and install licenses for ProLiant servers, and to view license information for Synergy compute modules.
- If you lose a license key, follow the lost license key instructions.
- A free iLO evaluation license key is available for download from the following website: **http://www.hpe.com/info/tryilo**.

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.

Procedure

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

   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.

Viewing license information

Procedure

Navigate to the Administration > Licensing page.

License details

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

  For security, only the last five digits of the license key are displayed.

iLO user accounts

iLO enables you to manage user accounts stored locally in secure memory.

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, configure iLO to use a directory service to authenticate and authorize its users.

Adding local user accounts

Prerequisites

Administer User Accounts privilege

Procedure

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 available user privileges, click the select all check box.
5. To save the new user, click Add User.

Editing local user accounts

Prerequisites

Administer User Accounts privilege

Procedure

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:
   - Login Name
   - User 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
6. To select all available user privileges, click the select all check box.
7. To save the user account changes, click Update User.

Viewing local user accounts

Procedure

1. Navigate to the Administration > User Administration page.

   The Local Users table shows the login name, user name, and assigned privileges of each configured user.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

Deleting a user account

Prerequisites

Administer User Accounts privilege

Procedure

1. Navigate to the Administration > User Administration page.
2. Select the check box next to one or more user accounts that you want to delete.
3. Click Delete.
4. When prompted to confirm the request, click OK.

iLO user account options

- 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.

iLO user privileges

- Remote Console Access—Enables a user to access the host system Remote Console, including video, keyboard, and mouse control.
- Virtual Media—Enables a user to use the Virtual Media feature on the host system.
- 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.
- 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.

Password guidelines

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

- When working with passwords:
  - Do not write down or record passwords.
  - Do not share passwords with others.
  - Do not use passwords that are made up of words found in a dictionary.
  - Do not use passwords that contain obvious words. Examples include the company name, product name, user name, or login name.
  - Change passwords regularly.
  - Keep the iLO default credentials in a safe place.
- Use strong passwords with at least three of the following characteristics:
  - At least one uppercase ASCII character
  - At least one lowercase ASCII character
  - At least one ASCII digit
  - At least one other type of character (for example, a symbol, special character, or punctuation).
- The minimum length for a user account password is set on the Access Settings page. Depending on the configured Minimum Password Length value, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. Hewlett Packard Enterprise recommends using a Minimum Password Length of eight or more characters. The default value is eight characters.

  IMPORTANT:

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

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, 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.

iLO directory groups

iLO directory groups are used with Kerberos authentication and schema-free directory integration. iLO supports up to six directory groups.

Adding directory groups

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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.

Editing directory groups

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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.

Viewing directory groups

Procedure

1. Navigate to the Administration > User Administration page.

   The Directory Groups table shows the group DN, group SID, and the assigned privileges for each group.

2. (Optional) To view a privilege name, move the cursor over a privilege icon.

Deleting a directory group

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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.

Directory group options

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 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.

Active Directory nested groups (schema-free configuration 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.

Directory group privileges

- 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.

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 you navigate to one of the iLO Federation pages, 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 group is retrieved.

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

Prerequisites for using the iLO Federation features

Procedure

- 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.
- If the switches in your network include the option to enable or disable multicast traffic, ensure that it is enabled. 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.
- If you want to use server blades in a BladeSystem c-Class enclosure with iLO Federation, the Enable Enclosure iLO Federation Support setting must be enabled in the Onboard Administrator web interface. This setting is enabled by default.

Configuring the multicast options for one iLO system at a time

Use the following procedure to configure the multicast options for the systems you will add to iLO Federation groups. If you use the default values, configuration is not required.

You can use the iLO RESTful API or RIBCL scripts to view and configure multicast options for multiple iLO systems.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > iLO Federation page.
2. Enable or disable the iLO Federation Management option.
3. Enable or disable the Multicast Discovery option.
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

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.

The possible values are:

- 30, 60, or 120 seconds
- 5, 10, 15, or 30 minutes
- Disabled

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. Valid values are from 1 to 255. The default value is 5.

iLO Federation groups

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.

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 the servers in the group.

You can add group memberships for multiple iLO systems on the 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.

iLO Federation group privileges

When an iLO system is 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.

iLO Federation group characteristics

- 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.
- Each 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 the iLO RESTful API to configure group memberships.

  For more information, see the iLO RESTful API documentation at the following website: **https://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.

Managing iLO Federation group memberships (local iLO system)

Adding iLO Federation group memberships

Prerequisites

- Configure iLO Settings privilege
- The Minimum Password Length setting on the Access Settings page is set to 31 or fewer characters.

Procedure

1. Navigate to the Administration > iLO Federation page.
2. Click Join Group.
3. Enter a Group Name.

   This value can be 1 to 31 characters long.
4. Enter the Group Key and Group Key Confirm values.

   The group key (password) can be from the configured minimum password length to 31 characters long.
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. Click Join Group.

   If you entered the name and key of an existing group, the local iLO system is added to that group.

   If you entered the name and key of a group that does not exist, the group is created and the local iLO system is added to it.

Editing iLO Federation group memberships

Prerequisites

- Configure iLO Settings privilege
- If you want to edit the group key, the Minimum Password Length setting on the Access Settings page is set to 31 or fewer characters.

Procedure

1. Navigate to the Administration > iLO Federation page.
2. Select a group membership, and then click Edit.
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.
7. If you updated the group name or group key, update them on the other systems in the affected group.

Removing a group membership from a local iLO system

Prerequisites

Configure iLO Settings privilege

Procedure

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.

Viewing iLO Federation group memberships (local iLO system)

Procedure

1. 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.

2. Optional: To view a privilege name, move the cursor over a privilege icon.

Adding iLO Federation group memberships (multiple iLO systems)

Adding a group based on an existing group

Use this procedure to create a group with the same members as an existing group. For example, you could create a group with the same systems as the DEFAULT group, but with different privileges.

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- At least one iLO Federation group exists.

Procedure

1. Navigate to the iLO Federation > Group Configuration page.
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.
3. Enter a Group Name.

   This value can be 1 to 31 characters long.

   If you enter the name of a group that exists, iLO prompts you to enter a unique group name.
4. Enter the Group Key and Group Key Confirm values.

   The group key (password) can be from the configured minimum password length to 31 characters long.
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 is not assigned 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. 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.

Creating a group from a filtered list of servers

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

When you create a group from a filtered list of servers, the group includes only the servers in the Affected Systems list during the group creation process. Servers that meet the filter criteria later, after the group is created, are not added to the group.

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- At least one iLO Federation group exists.

Procedure

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 active filters are listed at the top of the page.
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 a Group Name.

   This value can be 1 to 31 characters long.

   If you enter the name of a group that exists, iLO prompts you to enter a unique group name.
5. Enter the Group Key and Group Key Confirm values.

   The group key (password) can be from the configured minimum password length to 31 characters long.
6. 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.
7. (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 is not assigned 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.
8. 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.

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 Prev (if available) to view more servers in the list.

Configuring Enclosure iLO Federation Support

If you want to use iLO Federation with server blades in a BladeSystem c-Class enclosure, the Enable Enclosure iLO Federation Support option 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. The Enable Enclosure iLO Federation Support option is enabled by default.

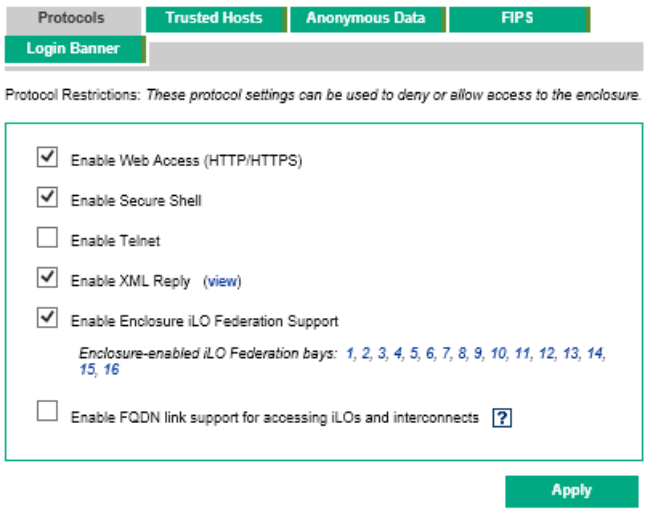
Prerequisites

Onboard Administrator 4.11 or later is installed.

Procedure

1. Log in to the Onboard Administrator web interface (https://<OA hostname or IP address>).
2. Select Enclosure Information > Enclosure Settings > Network Access in the navigation tree.

   The Protocols tab is displayed.
3. Select the Enable Enclosure iLO Federation Support check box, and then click Apply.



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

Verifying server blade support for iLO Federation

Procedure

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

Configuring the iLO security features

General security guidelines

When you set up and use iLO, consider the following guidelines for maximizing security:

- Set up iLO on a dedicated management network.
- Do not connect iLO directly to the Internet.

  IMPORTANT:

  Change the iLO user account passwords immediately if iLO has been connected directly to the Internet.

- Install an SSL certificate that is signed by a Certificate Authority (CA).

  You can perform this task on the SSL Certificate Information page.

- Change the password for your user accounts, including the default user account.

  You can perform this task on the User Administration page.

  IMPORTANT:

  Follow the iLO user account password guidelines when you create and update user accounts.

- Instead of creating accounts with all privileges, create multiple accounts with fewer privileges.
- Keep your iLO and server firmware up-to-date.
- Use an authentication service (for example, Active Directory or OpenLDAP), preferably with two-factor authentication.
- Disable ports and protocols that you do not use (for example, SNMP Access or IPMI/DCMI over LAN Access).

  You can perform this task on the Access Settings page.

- Use HTTPS for the Integrated Remote Console.

  To configure this option, enable the IRC requires a trusted certificate in iLO setting on the Remote Console Security tab.

- Configure the Integrated Remote Console to automatically lock the server OS console.

  To configure this option, configure the Remote Console Computer Lock setting on the Remote Console Security tab.

- Configure a higher security state on the Encryption Settings page.
- Configure iLO to require login credentials when users access the iLO RBSU or the iLO 4 Configuration Utility in the UEFI System Utilities.

  You can perform this task on the Access Settings page.

- Configure iLO to log authentication failures.

  You can perform this task on the Access Settings page.

- Configure iLO to avoid access over an HTTP connection.

  To configure this behavior, install a trusted SSL certificate that is signed by a Certificate Authority (CA) and enable the IRC requires a trusted certificate in iLO setting.

  You can complete these configuration steps on the SSL Certificate Information page and the Remote Console page Security tab respectively.

  In this configuration, when you access the iLO web interface, iLO returns an HTTP Strict Transport Security (HSTS) flag in the response header, which enables the browser to automatically redirect any HTTP request to HTTPS.

Managing SSH keys

Authorizing a new SSH key by using the web interface

Prerequisites

Administer User Accounts privilege

Procedure

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

   Each user account can have only one key assigned.
7. Click Authorize New Key.
8. Paste the public key into the Public Key Import Data box.
9. Click Import Public Key.

   The Authorized SSH Keys table is updated to show the hash of the SSH public key associated with the user account.

Authorizing a new SSH key by using the CLI

Prerequisites

Administer User Accounts privilege

Procedure

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 `/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.

   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
   ```

Deleting SSH keys

Use the following procedure to delete SSH keys from one or more user accounts.

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

Prerequisites

Administer User Accounts privilege

Procedure

1. Navigate to the Administration > Security page.
2. On the Secure Shell Key page, select the check box to the left of the user for which you want to delete an SSH key.
3. Click Delete Selected Key(s).

   The selected SSH keys are removed from iLO.

Requirements for 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 in iLO before you use `mxagentconfig` to authorize a key.
- The user name and password entered in `mxagentconfig` must correspond to a user account with the Configure iLO Settings privilege. The user can be a directory user or a local user.
- The key is authorized in iLO and corresponds to the user name specified in the `mxagentconfig` command.

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

SSH keys

When you add an SSH key to iLO, the iLO firmware associates the key with a local user account.

Supported SSH key formats

- RFC 4716
- OpenSSH key format
- iLO legacy format

Working with SSH keys

- The supported SSH key formats are supported with the iLO web interface and the CLI.
- 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 can import SSH keys with a maximum length of 1,366 bytes. If the key length exceeds 1,366 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 iLO RESTful API to enter the public key, the user name is provided with the public key in the POST body.
- 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 a user is removed after an SSH key is authorized for that user, the SSH key is removed.

Supported SSH key format examples

RFC 4716

```
---- BEGIN SSH2 PUBLIC KEY ---- CRLF
Comment: "Administrator"CRLF
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZCRLF
ZtzF0VInP5x2VFVYmTvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
3wI3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8CRLF
/UAAAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0PcCRLF
j477YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcCRLF
jFteBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHCRLF
g8ZJazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8CRLF
hX/Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYCRLF
aiFDLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtCRLF
STV CRLF
---- END SSH2 PUBLIC KEY ---- CRLF
```

OpenSSH key format

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avN
Sz0DNQuU7gTPfjj/8cXyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0d
VOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5Qx
qkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIyNjcQODeYYqOvVU45AkSkLBMGjpF
05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxDOvNWAAAAg
Ff6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekB
a9QI91H1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLw
AOTSmQEOW Administrator CRLF
```

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----- CRLF
ssh-dss
AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx91V22XvonwijdFiOM/0Vv
uzVhM9oKdGMC7sCGQrFV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwr
ApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQDofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0
KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0jKzzVxmsanO+pjju7lrE3xUxojev
lokTERSCMxLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzGfi5pKAAAA
IEAl7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53Wl1pUARJg1s
s8Ruy7YBv8Z1urWWAF3fYy7R/SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYo
mYwnDC4m1IT4= ASmith CRLF
-----END SSH KEY-----CRLF
```

Administering SSL certificates

The Secure Sockets Layer (SSL) protocol is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. An SSL certificate is a small computer file that digitally combines a cryptographic key (the server public key) with the server name. Only the server itself has the corresponding private key, allowing for authenticated two-way communication between a user and the server.

A certificate must be signed to be valid. If it is signed by a Certificate Authority (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.

IMPORTANT:

Using a self-signed certificate is less secure than importing a trusted certificate. Hewlett Packard Enterprise recommends importing a trusted certificate to protect the iLO user account credentials.

Viewing SSL certificate information

Procedure

Navigate to the Administration > Security > SSL Certificate page.

SSL certificate details

- Issued To—The entity to which the certificate was issued.

  When you view the iLO self-signed certificate, this value displays information related to the Hewlett Packard Enterprise Houston office.

- Issued By—The CA that issued the certificate.

  When you view the iLO self-signed certificate, this value displays information related to the Hewlett Packard Enterprise Houston office.

- Valid From—The first date that the certificate is valid.
- Valid Until—The date that the certificate expires.
- Serial Number—The serial number assigned to the certificate. This value is generated by iLO for the self-signed certificate, and by the CA for a trusted 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

Procedure

1. Obtain a trusted certificate from a Certificate Authority (CA).
2. Import the trusted certificate into iLO.

Obtaining a trusted certificate from a CA

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Security > SSL Certificate page.
2. Click Customize Certificate.
3. Enter values for the following:
   - Country (C)
   - State (ST)
   - City or Locality (L)
   - Organization Name (O)
   - Organizational Unit (OU)
   - Common Name (CN)
4. (Optional) To include the iLO IP addresses in the CSR, select the include iLO IP Address(es) check box.

   NOTE:

   Many certificate authorities (CAs) cannot accept this input. Do not select this option if you are not sure that the CA you are using can accept this input.

   When this option is enabled, the iLO IP addresses will be included in the CSR Subject Alternative Name (SAN) extension.
5. Click Generate CSR.

   A message notifies you that a CSR is being generated and that the process might take up to 10 minutes.
6. After a few minutes (up to 10), click Generate CSR again.

   The CSR is displayed.
7. Select and copy the CSR text.
8. Open a browser window and navigate to a third-party CA.
9. Follow the onscreen instructions and submit the CSR to the CA.
   - When prompted to select a certificate purpose, make sure that you select the option for a server certificate.
   - When you submit the CSR to the CA, your environment might require the specification of Subject Alternative Names. If necessary, enter the iLO DNS name.

   The CA generates a certificate. The certificate signing hash is determined by the CA.
10. After you obtain the certificate, make sure that:
    - The CN matches the iLO FQDN. This value is listed as the iLO Hostname on the Overview page.
    - The certificate is a Base64-encoded X.509 certificate.
    - The first and last lines are included in the certificate.

CSR input details

When you create a CSR, enter the following details:

- 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.

  To enable iLO to enter the FQDN in the CSR, configure the Domain Name on the Network General Settings page.
- Include iLO IP Address(es)—Select this check box to include the iLO IP addresses in the CSR.

> **NOTE:**
>
> Many CAs cannot accept this input. Do not select this option if you are not sure that the CA you are using can accept this input.

Certificate signing requests

A CSR contains a public and private key pair that validates communications between the client browser and iLO. iLO generates a 2048-bit RSA key. 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.

Importing a trusted certificate

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Security > SSL Certificate page.
2. Click Customize Certificate.
3. Click Import Certificate.
4. 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).
5. Reset iLO.

Removing a customized certificate

Use this feature to remove a custom SSL certificate and regenerate the iLO self-signed certificate.

You might want to remove a custom certificate for the following reasons:

- The certificate expired.
- The certificate contains invalid information.
- There are security concerns related to the certificate.
- An experienced support organization recommended that you remove a custom certificate.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Security > SSL Certificate page.
2. Click Remove.

   iLO prompts you to confirm that you want to delete the existing certificate, reset iLO, and generate a new self-signed certificate.
3. Click OK.

   iLO removes the custom SSL certificate, resets, and generates a new self-signed certificate.

   It might take several minutes for iLO to generate the new certificate.

Directory authentication and authorization settings in iLO

The iLO firmware supports Kerberos authentication with Microsoft Active Directory. It also supports directory integration with an Active Directory or OpenLDAP directory server.

When you configure directory integration, you choose between the schema-free and HPE Extended Schema configurations. The HPE Extended Schema is supported only with Active Directory. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port.

You can enable the directory server certificate validation feature by importing a CA certificate. This feature ensures that iLO connects to the correct directory server during LDAP authentication.

Configuring the authentication and directory server settings in iLO is one step in the process of configuring iLO to use a directory or Kerberos authentication. Additional steps are required to set up your environment to use these features.

Prerequisites for configuring authentication and directory server settings

Procedure

1. Verify that your iLO user account has the Configure iLO Settings privilege.
2. Install a license that supports this feature.
3. Configure your environment to support Kerberos authentication or directory integration.

Configuring Kerberos authentication settings in iLO

Prerequisites

- Your environment meets the prerequisites for using this feature.
- The Kerberos keytab file you created during the environment setup tasks is available.

Procedure

1. Navigate to the Administration > Security > Directory page.
2. Select the Kerberos Authentication check box.
3. Select the Local User Accounts check box 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 or Choose File (depending on the browser you use), and then follow the onscreen instructions.
8. Click Apply Settings.
9. Click Administer Groups to configure directory groups.

Kerberos settings

- Kerberos Authentication—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 127 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 127 characters. Each realm must have at least one Key Distribution Center (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

Prerequisites

Your environment meets the prerequisites for using this feature.

Procedure

1. Navigate to the Administration > Security > Directory page.
2. Select Use Directory Default Schema from the LDAP Directory Authentication menu.
3. Select the Local User Accounts check box if you want to use local user accounts at the same time as directory integration.
4. OpenLDAP users only: Select the Generic LDAP check box.

   This setting is available only if Use Directory Default Schema is selected.
5. Enter the FQDN or IP address of a directory server in the Directory Server Address box.
6. Enter the directory server port number in the Directory Server LDAP Port box.
7. Enter valid search contexts in one or more of the Directory User Context boxes.
8. Optional: Import a new CA certificate.
   a. Click Import in the Certificate Status box.
   b. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
9. Optional: Replace an existing CA certificate.
   a. Click View in the Certificate Status text box.
   b. Click New in the Certificate Details window.
   c. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
10. Click Apply Settings.
11. To test the communication between the directory server and iLO, click Test Settings.
12. Optional: To configure directory groups, click Administer Groups to navigate to the User Administration page.

Schema-free directory settings

- Use Directory Default Schema—Selects directory authentication and authorization by using user accounts in the directory. User accounts and group memberships are used to authenticate and authorize users.

  This configuration supports Active Directory and OpenLDAP.

- Generic LDAP—Specifies that this configuration uses the OpenLDAP supported BIND method.

- 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. There is a 1904 character limit for the sum of all the directory user contexts.

- Certificate Status—Specifies whether a directory server CA certificate is loaded.

  If the status is Loaded, click View to display the CA certificate details. If no CA certificate is loaded, the status Not Loaded is displayed. iLO supports SSL certificates up to 4 KB in size.

Configuring HPE Extended Schema directory settings in iLO

Prerequisites

Your environment meets the prerequisites for using this feature.

Procedure

1. Navigate to the Administration > Security > Directory page.
2. Select Use Extended Schema from the LDAP Directory Authentication menu.
3. Select the Local User Accounts check box 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. Optional: Import a new CA certificate.
   a. Click Import in the Certificate Status text box.
   b. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
9. Optional: Replace an existing CA certificate.
   a. Click View in the Certificate Status text box.
   b. Click New in the Certificate Details window.
   c. Paste the Base64-encoded X.509 certificate data into the Import Certificate window, and then click Import.
10. Click Apply Settings.
11. To test the communication between the directory server and iLO, click Test Settings.

HPE Extended Schema directory settings

- Use 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. This configuration supports Active Directory.
- LOM Object Distinguished Name—Specifies where this iLO instance is listed in the directory tree (for example, `cn=Mail Server iLO,ou=Management Devices,o=ab`).

  User search contexts are not applied to the LOM object DN when iLO accesses the directory server.
- 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. There is a 1904 character limit for the sum of all the directory user contexts.
- Certificate Status—Specifies whether a directory server CA certificate is loaded.

  If the status is Loaded, click View to display the CA certificate details. If no CA certificate is loaded, the status Not Loaded is displayed. iLO supports SSL certificates up to 4 KB in size.

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.
- **Example 4 (OpenLDAP user)**—If a user has the DN `UID=user,ou=people,o=ab`, and you enter the search context
  `ou=people,o=ab`
  , the user can log in as
  `user`
  instead of entering the DN.
  To use this format, you must enable Generic LDAP on the Security - Directory page.

Directory Server CA Certificate

During LDAP authentication, iLO validates the directory server certificate if the CA certificate is already imported. For successful certificate validation, make sure that you import the correct CA certificate. If certificate validation fails, iLO login is denied and an event is logged. If no CA certificate is imported, the directory server certificate validation step is skipped.

To verify SSL communication between the directory server and iLO, click Test Settings.

Deleting a directory server CA certificate

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Security > Directory page.
2. Click View in the Certificate Status text box.
3. Click Delete in the Certificate Details window.

   iLO prompts you to confirm the request.
4. Click OK.

   iLO notifies you that the certificate was deleted.

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 a 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.

Procedure

1. Navigate to the Administration > Security > Directory page.
2. At the bottom of the Directory page, click Test Settings.

   iLO displays the results of a series of simple tests designed to validate the directory settings. 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.
3. 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.

   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.
4. In the Directory Test Controls section, enter a test user name and password in the Test User Name and Test User Password boxes.
5. 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.

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. iLO does not store these credentials.

Directory test status values and controls

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. To identify the problem, check the onscreen log.
  - Warning—One or more of the directory tests reported a Warning status.
- Test—The name of each test.
- 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.
  - A test failure prevents further progress.
  - The tests are stopped.

  Possible 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 such as the directory server certificate subject and the roles that were evaluated.

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.

LDAP server certificate validation errors are reported in the results for this test.

Bind to Directory Server

This test binds the connection with the user name specified in the test controls. 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. Providing these values is 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.

User login is the only way that you can test contexts that begin with the @ symbol.

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.

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

This test is run even if LDAP Directory Authentication is disabled.

Configuring encryption settings

Modifying the AES/DES encryption setting

Prerequisites

Configure iLO Settings privilege

Procedure

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.
4. If you changed the Enforce AES/3DES Encryption setting to Enabled, close all open browsers.

   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
```

Enabling FIPS mode

Use this procedure to configure iLO to operate in FIPS mode. To configure iLO in a FIPS-validated environment, see Configuring a FIPS-validated environment with iLO.

Prerequisites

- Configure iLO Settings privilege
- The server is not an HPE Synergy Gen9 Compute Module. This feature is not supported on HPE Synergy Gen9 Compute Modules.

Procedure

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. 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. Disable the IPMI/DCMI over LAN Access and SNMP Access options 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.

   To verify that the configuration is FIPS-compliant, check your configuration against the Security Policy document that was part of the iLO FIPS validation process.

   The validated Security Policy document is available on the **NIST website**. To access iLO 4 FIPS information, enter certificate number 2574 on the validated modules search page.

8. Optional: Restore the iLO configuration by using HPONCFG.

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

9. Optional: Configure the Login Security Banner to inform iLO users that a system is using FIPS mode.

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.

It is important to decide if a FIPS-validated version of iLO is required for your environment, or if running iLO with FIPS mode enabled will suffice. Because of the lengthy validation process, a FIPS-validated version of iLO might have been superseded by a nonvalidated version with new features and security enhancements. In this situation, a FIPS-validated version of iLO might be less secure than the latest version.

Configuring a FIPS-validated environment is not supported on HPE Synergy Gen9 Compute Modules.

Procedure

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**. To access iLO 4 FIPS information, enter certificate number 2574 on the validated modules search page.

Viewing encryption settings

Procedure

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.

  This option is not supported on HPE Synergy Gen9 Compute Modules.

- 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.

Disabling FIPS mode

Procedure

To disable FIPS mode for iLO (for example, if a server is decommissioned), set iLO to the factory default settings.

CAUTION:

When you reset iLO to the factory default settings, all potentially sensitive data is erased, including all logs and settings.

Events related to the reset are not logged to the Event Log and Integrated Management Log because this step clears all the data in the logs.

iLO encryption details

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

iLO supports the following ciphers when FIPS Mode 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)
- 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)

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 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 MAC.

When FIPS Mode 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.

iLO 4 version 2.11 is FIPS validated.

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.

HPE SSO

HPE SSO enables you to browse directly from HPE SSO-compliant applications to iLO, bypassing an intermediate login step.

To use this feature:

- You must have a supported version of an application that is HPE SSO-compliant.
- 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.

Configuring iLO for HPE SSO

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Security > HPE SSO page.
2. Configure the Single Sign-On Trust Mode setting.

   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.

   When a system is registered as a trusted server, SSO might be refused because of the current trust mode or certificate status. For example, SSO would be refused when:

   - A server is registered as a trusted server, a certificate is not imported, and the trust mode is set to Trust by Certificate.
   - A server certificate is imported but the certificate has expired.

   The list of trusted servers is not used when SSO is disabled. iLO does not enforce SSO server certificate revocation.

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 HPE SSO-compliant applications by matching a certificate previously imported to iLO.
- Trust by Name—Enables SSO connections from HPE SSO-compliant applications 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 application that is HPE SSO-compliant, 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 the Single Sign-On Settings section. iLO directory settings do not apply.

The default privilege settings follow:

- User—Login only
- Operator—Login, Remote Console, Virtual Power and Reset, and Virtual Media
- Administrator—Login, Remote Console, Virtual Power and Reset, Virtual Media, Configure iLO Settings, 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 allocated storage is used, no more imports are accepted.

For information about how to extract a certificate from an HPE SSO-compliant application, see your HPE SSO-compliant application documentation.

Prerequisites

Configure iLO Settings privilege

Procedure

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.

     Install iLO 4 1.20 or later to support the larger certificates used with recent versions of HPE SIM. HPE SIM 7.3.2 and 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.

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 SSO certificate

You can use the following methods to extract HPE SIM SSO certificates. For more information, see the HPE SIM documentation.

Prerequisites

HPE SIM 7.4 or later

Procedure

- Enter one of the following links in a web browser:

  ```
  http://<HPE SIM name or network address>:280/GetCertificate?certtype=sso
  ```

  ```
  https://<HPE SIM name or network address>:50000/GetCertificate?certtype=sso
  ```

  All request parameters are case-sensitive. If you capitalize the lowercase `certtype` parameter, the parameter will not be read, and HPE SIM will return the default HPE SIM certificate instead of a trusted certificate.

- Export the certificate from HPE SIM.

  To complete this step, select Options > Security > Certificates > HPE Systems Insight Manager Single Sign-On Server Certificate , and then click Export.

Importing a direct DNS name

Prerequisites

Configure iLO Settings privilege

Procedure

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

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.

Procedure

Navigate to the Administration > Security > HPE SSO page.

Trusted certificate and record details

Status

The status of the certificate or record. The possible status values follow:

- The certificate or record is valid.
- There is a problem with the certificate or record. Possible reasons follow:
  - The record contains a DNS name, and the trust mode is set to Trust by Certificate (only certificates are valid).
  - A certificate is configured, and the trust mode is set to Trust by Name (only directly imported IP addresses or DNS names are valid).
  - Trust None (SSO disabled) is selected.
- The certificate or record is not valid. Possible reasons follow:
  - The certificate is out-of-date. Check the certificate details for more information.
  - The iLO clock is not set or is set incorrectly. The iLO clock must be in the certificate 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

Procedure

1. Navigate to the Administration > Security > HPE SSO page.
2. Select one or more trusted certificates or records in the Manage Trusted Certificates and Records table.
3. Click Delete.

   iLO prompts you to confirm that you want to delete the selected certificates or records.

   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. The security banner is also displayed when you connect to iLO through an SSH connection. For example, you could enter a message with contact information for the owner of the server.

Prerequisites

Configure iLO Settings privilege

Procedure

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.

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

   Do not add blank spaces or blank lines to the security message. Blank spaces and blank lines contribute to the byte count, and they are not displayed in the security banner on the login page.

   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 you out when a remote console session ends or the network link to iLO is lost. If you open a remote console window when this feature is enabled, the OS is locked when you close the window.

Prerequisites

Configure iLO Settings privilege

Procedure

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

Remote console computer lock options

- Windows—Configures 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—Configures 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 automatically sent to the server OS when a remote console session ends or the iLO network link is lost.
- Disabled (default)—Disables the remote console computer lock feature. When a remote console session ends or the iLO network link is lost, the OS on the managed server is not locked.

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

Procedure

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.

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 of the server system board. Disabling iLO security allows login access with all privileges, without a user ID and password.

The system maintenance switch is 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. For more information about using the system maintenance switch, see the server maintenance and service guide.

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 the ROM-based configuration utility is disabled.
- The boot block must be updated.

  Hewlett Packard Enterprise does not anticipate that you will have a reason 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.
- iLO is unreachable over the network because the iLO NICs are turned off or the iLO network configuration is incorrect. It is not possible or convenient to use the ROM-based configuration utility to correct the configuration.

  Disabling iLO security resets the iLO network configuration to the factory default settings.
  - On most servers, this action enables DHCP and the iLO Dedicated Network Port.
  - On servers where the iLO Dedicated Network Port is an optional add-on card, this action enables DHCP and the Shared Network Port.
- Only one user name is configured, and the password is forgotten.
- You want to erase the configuration information stored on the battery-powered SRAM memory device.

  When iLO starts, it backs up the configuration information stored in the battery-powered SRAM memory device to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored. When iLO security is disabled, the SRAM data is not restored automatically.

Effects of disabling iLO security

- All security authorization verifications are disabled.
- If the host server is reset, the ROM-based 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 server power is cycled.
- 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 alert is sent when iLO starts after the iLO security configuration change.

Configuring iLO access settings

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.

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

Configuring iLO 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, an iLO reset is required to activate the changes.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Access Settings page.

   The Access Settings tab is displayed.

2. Update the service settings as needed.

3. Click Apply.

   iLO prompts you to confirm that you want to apply the changes and reset iLO.

4. To apply the changes and reset iLO now, click OK.

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

Service settings

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 SNMPv3 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 Disabled.

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

When this value is set 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

Procedure

1. Navigate to the Administration > Access Settings page.

   The Access Settings tab is displayed.

2. Update the access options as needed.

3. Click Apply.

   If a reset is required, iLO prompts you to confirm that you want to apply the changes and reset iLO.

   If a reset is not required, iLO completes the change and refreshes the page.

4. If a reset prompt was displayed, click OK to end your browser connection and initiate a reset.

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

Access options

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 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)

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.

- 19200
- 38400—iLO RBSU and the iLO 4 Configuration Utility do not support this value.
- 57600
- 115200

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. You can view activity by using the CLI command `vsp log`. The Virtual Serial Port buffer size is 128 KB.
- Disabled (default)—Virtual Serial Port activity is not logged.

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.

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 4 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.

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 Access Settings page.
- iLO saves a detailed log entry for failed login attempts. You can configure the Authentication Failure Logging frequency on the Access Settings page.

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.

Configuring iLO network settings

iLO network settings

To access iLO network settings, you select the active network interface card, and then view or edit the configuration on the following pages:

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

If you select the inactive NIC, iLO notifies you that it is not configured to use that NIC.

Viewing the network configuration summary

Procedure

Select Network > iLO Dedicated Network Port or Network > Shared Network Port.

Network configuration summary details

- NIC In Use—The name of the active iLO network interface (iLO Dedicated Network Port or iLO 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.

If the Shared Network Port is enabled, you cannot modify the Link State or Duplex Option. In Shared Network Port configurations, link settings must be managed in the operating system.

IPv4 Summary details

- 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.

IPv6 Summary details

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

- 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—The address type.
  - 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.

General network settings

Use the iLO Dedicated Network Port or Shared Network Port Network General Settings page to configure the iLO Hostname and NIC settings.

Configuring the iLO Hostname Settings

Prerequisites

Configure iLO Settings privilege

Procedure

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. This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

   You can enter up to 49 characters.
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 Settings and IPv6 Settings pages.

   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 Settings page.
5. To save the changes, 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.

    iLO allows up to 49 characters in the hostname, but using a shorter name can help you to avoid interoperability issues with other software products in your environment.
  - 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.

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

Procedure

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

   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.

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 (supported servers only).
- 1000BaseT, Half-duplex—Forces a 1 Gb connection that uses half duplex (supported servers only).

  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

Prerequisites

Configure iLO Settings privilege

Procedure

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.
7. To use a VLAN, select the Enable VLAN check box.
8. If you enabled VLAN, enter a VLAN Tag.
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.

Shared Network Port options

Port

The Shared Network Port number.

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.

Enable VLAN

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.

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.

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—Depending on your configuration, the following Shared Network Port options are available:
  - 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 through 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 through a common RJ-45 connector.

  There are some drawbacks to using a Shared Network Port option:

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

    When this situation occurs, the Remote Console and connected iLO Virtual Media devices might be disconnected.
  - Network controller firmware updates or resets can also cause iLO to be unreachable over the network for a brief period.
  - The iLO Shared Network Port connection cannot operate at a speed greater than 100 Mbps. Network-intensive tasks such as data transfer through iLO virtual media might be slower than the same tasks performed in a configuration that uses the iLO Dedicated Network Port.

For information about the NICs your server supports, see the server specifications at the following website: **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 network connection.
- By default, the iLO Shared Network Port uses port 1 on the server network interface card. 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 support port selection, iLO 4 2.00 and later allows you to select a different port. If you select a port other than port 1 in a Shared Network Port configuration, and your server does not support that configuration, iLO switches to port 1 at startup.
- Access to iLO through IPv6 is not supported when the Shared Network Port is enabled.
- On servers without 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 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, you must manage these settings in the operating system.
- If the Shared Network Port is enabled and you use NIC teaming, review the NIC teaming documentation.

Configuring IPv4 settings

Use the following procedure to configure the IPv4 settings. When you configure these settings, do not enter special use IPv4 addresses such as 192.0.2.0/24. These addresses are not supported. For more information, see the documentation for RFC5735 on the IETF website.

Prerequisites

Configure iLO Settings privilege

Procedure

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.

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 Use DHCPv4 Supplied WINS Servers, 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.

IPv4 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. 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.

Prerequisites

Configure iLO Settings privilege

Procedure

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.

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 when 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 enabled, Enable DHCPv6 in Stateless Mode (Other) is enabled by default because it is implicit in the DHCPv6 Stateful messages that are required between iLO and the DHCPv6 server.

IPv6 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.

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 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, the Enable DHCPv4 option is enabled on the IPv4 tab.
- If you will use a DHCPv6-provided NTP service configuration, the Enable DHCPv6 in Stateless Mode (Other) option 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.

Procedure

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, enable Use DHCPv4 Supplied Time Settings, Use DHCPv6 Supplied Time Settings, or both.
   - 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.

   For blade servers, this setting is called Propagate NTP or OA Time to Host.

   For nonblade servers, this setting is called Propagate NTP Time to Host.
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.

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.

NTP time propagation setting

The name of this setting differs depending on the server type.

- Propagate NTP Time to Host (nonblade servers)—Determines whether the server time is synchronized with the iLO time during the first POST after AC power is applied or iLO is reset to the default settings.
- 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.

  When this setting 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 that you can select in iLO is Atlantic/Reykjavik GMT. If you select this time zone, the 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 (UTC).

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)
- Frame Link Module (Synergy compute modules)

Primary and secondary NTP server addresses can be configured manually or through 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.

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.

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.
- 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

Procedure

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_nicautosel` 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 HPE iLO 4 Scripting and Command Line Guide .

3. Arrange the server cabling, and then reset iLO.

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

Configuring NIC failover

Prerequisites

NIC auto-selection is enabled.

Use one of the following options to configure NIC failover. For detailed information, see the HPE iLO 4 Scripting and Command Line Guide.

Procedure

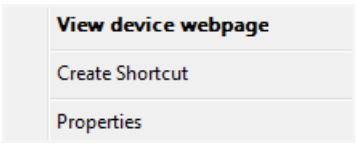
- Use the CLI command `oemhp_nicfailover` to configure NIC failover.
- Add the `ILO_NIC_FAIL_OVER` tag to your `MOD_NETWORK_SETTINGS` script, and run the script.

Viewing iLO systems in the Windows Network folder

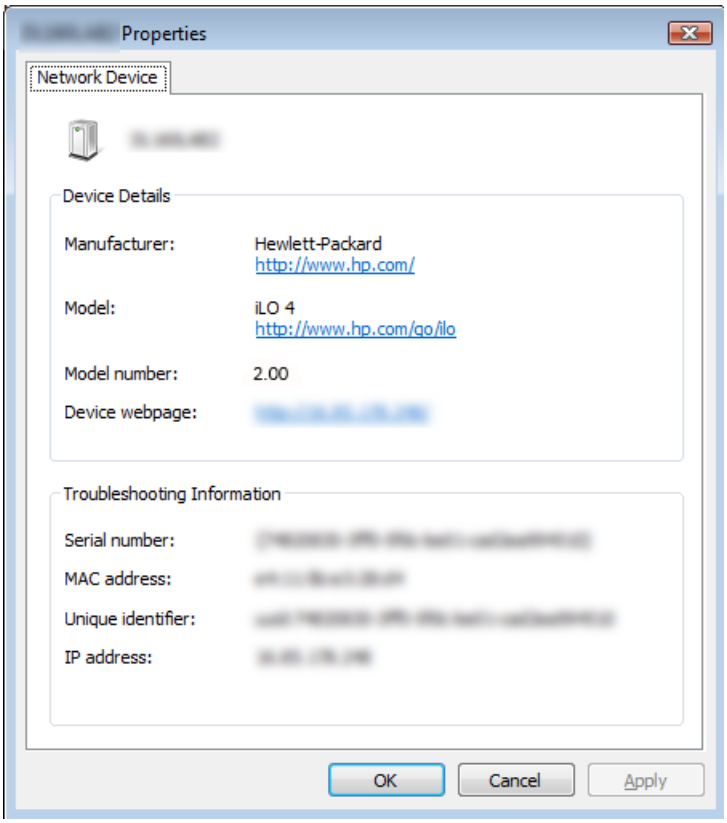
If UPnP is configured, iLO systems on the same network as a Windows system are displayed in the Windows Network folder.

Procedure

- To start the web interface for an iLO system, right-click the icon 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 manufacturer and version information. To start the iLO web interface, click the Device webpage link.
  - Troubleshooting Information—The serial number, MAC address, UUID, and IP address.

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 the Agentless Management Service 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.

Depending on the SNMP configuration you choose, additional software might be required. For more information, see Agentless Management Service and the Insight Management Agents.

For more information about Agentless Management, see the HPE Agentless Management and the transition from OS-based agents document at the following website: **http://www.hpe.com/info/ilo-docs**.

Table 1: Information provided by Agentless Management and Insight Management Agents lists the information collected by the available server configurations.

Table 1: 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	• Fans • Temperatures • Power supplies • Memory • CPU	• Fans • Temperatures • Power supplies • Memory • CPU	• Fans • Temperatures • Power supplies • Memory • CPU
Storage	• Smart Array [3] • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array • Smart Storage battery monitoring (supported servers only)	• Smart Array [3] • 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 drives [4]	• Smart Array • SMART Drive Monitoring (connected to Smart Array, Smart HBA, and AHCI) • SAS/SATA HBA/RAID • Fibre Channel/iSCSI • Tape • External storage
Network	• MAC addresses for embedded NICs • Physical link connectivity and link up/link down traps for NICs that have NC-SI over MCTP [5] • Fibre Channel adapters that support Hewlett Packard Enterprise vendor-defined MCTP commands [6]	• MAC and IP address for standup and embedded NICs • Link up/link down traps [7], [5] • NIC teaming information • Supported Fibre Channel adapters	• MAC and IP addresses for standup and embedded NICs • Link up/link down traps [5] • NIC teaming information • VLAN information

Component	Agentless Management without AMS	Agentless Management with AMS	Insight Management Agents
Other	• iLO data • Firmware inventory • Device inventory	• iLO data • Firmware inventory • Device inventory • OS information (host SNMP MIB) [7] • Driver/service inventory • Logging events to OS logs [8]	• iLO data • OS information (host SNMP MIB) • Performance data • User-configurable thresholds • Logging events to OS logs • Clustering information
Prefailure warranty alerts	• Memory • Drives (physical and logical)	• Memory • Drives (physical and logical)	• 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] SNMP traps are suppressed for All Links Down and Link Up/Link Down events that occur during POST. Alerting is suppressed during POST, but monitoring is still active. Alerts for detected status changes are sent when POST is complete.

[6] Supported with iLO 4 2.50 and later.

[7] The data supplied by Agentless Management is not as extensive as the data supplied by the SNMP agents.

[8] 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.

Agentless Management Service and the Insight Management Agents

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

- 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.
- The Insight Management Agents are not supported on Synergy compute modules.

Installing AMS or the Insight Management Agents

Procedure

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 (**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 AMS installation

Verifying AMS status: iLO web interface

Procedure

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

Procedure

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 Linux Enterprise Server and Red Hat Enterprise Linux

Procedure

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

Procedure

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`.

      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

Procedure

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

Procedure

- **Windows**—Navigate to the Windows Services page and restart AMS.
- **SUSE Linux Enterprise Server and Red Hat Enterprise Linux** —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

Procedure

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:
   - System Location
   - System Contact
   - System Role
   - System Role Detail
   - Read Community

   These values are unavailable when SNMP Pass-thru is selected.
4. Enter the following information:
   - Trap Community
   - SNMP Alert Destination(s)
   - SNMP Port
5. To save the configuration, click Apply.

SNMP options for all configurations

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 Access Settings page.

SNMP options for Agentless Management 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 SNMPv3 security features enable secure data collection from iLO 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 SNMP agent level (iLO) and the SNMP manager level (client system). Messages exchanged between the SNMP 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
- iLO is configured to use Agentless Management.

Procedure

1. Navigate to the Administration > Management page.

   The SNMP Settings tab is displayed.

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

   If user profiles are not configured, the Security Name column displays each profile with the value unset.

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

3. Enter the following values:
   - Security Name
   - Authentication Protocol
   - Authentication Passphrase
   - Privacy Protocol
   - Privacy Passphrase
4. To save the user profile, click Apply.

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.

Deleting an SNMPv3 user profile

Prerequisites

- Configure iLO Settings privilege
- iLO is configured to use Agentless Management.

Procedure

1. Navigate to the Administration > Management page.
2. Scroll to the SNMPv3 Users section.
3. Select a user profile in the SNMPv3 Users section, and then click Delete.
4. When prompted to confirm the request, click OK.

Configuring the SNMPv3 Engine ID

The SNMPv3 Engine ID sets the unique identifier of an SNMP engine belonging to an SNMP agent entity.

Prerequisites

- Configure iLO Settings privilege
- iLO is configured to use Agentless Management.

Procedure

1. Navigate to the Administration > Management page.
2. Enter a value in the SNMPv3 Engine ID box.

   This value must be a hexadecimal string of 6 to 48 characters, not counting the preceding 0x, and must be an even number of characters (for example, `0x01020304abcdef`). If you do not configure this setting, the value is system-generated.
3. Click Apply.

Configuring SNMP alerts

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Administration > Management page.
2. 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 configured SNMP Alert Destination(s), 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. After the alert is generated, check the HPE SIM console for receipt of the alert.
6. To save the configuration, click Apply.

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

The host name is an OS construct and it does not remain persistent with the server when 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. 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 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)

Procedure

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 configured Trap Destination(s), click Send Test Trap.

   Test alerts are used to verify the network connectivity of iLO with the Trap Destination(s) addresses. After the alert is generated, check the alert destination for receipt of the alert.
5. To save the configuration, click Apply.

SNMP traps

The following table lists the SNMP traps supported by iLO 4 and supported ProLiant servers and Synergy compute modules.

To cross reference an SNMP trap with REST alert information, see REST alerts.

Trap number	SNMP trap name	Description
0	Cold Start Trap	SNMP was initialized, the system completed POST, or AMS started.
4	Authentication Failure Trap	SNMP detected an authentication failure.
1006	cpqSeCpuStatusChange	An uncorrectable machine check exception was detected in a processor.
1010	cpqSeUSBStorageDeviceReadErrorOccurred	A read error occurred on an attached USB storage device.
1011	cpqSeUSBStorageDeviceWriteErrorOccurred	A write error occurred on an attached USB storage device.
1012	cpqSeUSBStorageDeviceRedundancyLost	USB storage device redundancy was lost.
1013	cpqSeUSBStorageDeviceRedundancyRestored	USB storage device redundancy was restored.
1014	cpqSeUSBStorageDeviceSyncFailed	The sync operation to restore USB storage device redundancy failed.
3033	cpqDa6CntlrStatusChange	Smart Array controller status change detected.
3034	cpqDa6LogDrvStatusChange	Smart Array logical drive status change detected.
3038	cpqDa6AccelStatusChange	Smart Array cache module status change detected.
3039	cpqDa6AccelBadDataTrap	The Smart Array cache module lost backup power.
3040	cpqDa6AccelBatteryFailed	The Smart Array cache module backup power failed.
3046	cpqDa7PhyDrvStatusChange	Smart Array physical drive status change detected.
3047	cpqDa7SpareStatusChange	Smart Array spare drive status change detected.
3049	cpqDaPhyDrvSSDWearStatusChange	Smart Array physical drive SSD wear status change detected.
5022	cpqSasPhyDrvStatusChange	AMS detected a change in the status of an SAS or SATA physical drive.
6026	cpqHe3ThermalConfirmation	The server was shut down due to a thermal anomaly and is now operational.
6027	cpqHe3PostError	One or more POST errors occurred.
6032	cpqHe3FltTolPowerRedundancyLost	The fault-tolerant power supplies lost redundancy for the specified chassis.
6033	cpqHe3FltTolPowerSupplyInserted	A fault-tolerant power supply was inserted.
6034	cpqHe3FltTolPowerSupplyRemoved	A fault-tolerant power supply was removed.

Trap number	SNMP trap name	Description
6035	cpqHe3FltTolFanDegraded	The fault-tolerant fan condition was set to Degraded.
6036	cpqHe3FltTolFanFailed	The fault-tolerant fan condition was set to Failed.
6037	cpqHe3FltTolFanRedundancyLost	The fault-tolerant fans lost redundancy.
6038	cpqHe3FltTolFanInserted	A fault-tolerant fan was inserted.
6039	cpqHe3FltTolFanRemoved	A fault-tolerant fan was removed.
6041	cpqHe3TemperatureDegraded	The temperature status was set to Degraded, and the temperature is outside the normal operating range. Depending on the system configuration, this system might be shut down.
6042	cpqHe3TemperatureOk	The temperature status was set to OK.
6048	cpqHe4FltTolPowerSupplyOk	The fault-tolerant power supply condition was set to OK.
6049	cpqHe4FltTolPowerSupplyDegraded	The fault-tolerant power supply condition was set to Degraded.
6050	cpqHe4FltTolPowerSupplyFailed	The fault-tolerant power supply condition was set to Failed.
6051	cpqHeResilientMemMirroredMemoryEngaged	The Advanced Memory Protection subsystem detected a memory fault. Mirrored Memory was activated.
6054	cpqHe3FltTolPowerRedundancyRestore	The fault-tolerant power supplies returned to a redundant state.
6055	cpqHe3FltTolFanRedundancyRestored	The fault-tolerant fans returned to a redundant state.
6064	cpqHe5CorrMemReplaceMemModule	Memory errors were corrected. Replace the memory module.
6069	cpqHe4FltTolPowerSupplyACpowerloss	The fault-tolerant power supply in the specified chassis and bay reported AC power loss.
6070	cpqHeSysBatteryFailed	The HPE Smart Storage Battery failed.
6071	cpqHeSysBatteryRemoved	The HPE Smart Storage Battery was removed.
6072	cpqHeSysPwrAllocationNotOptimized	iLO could not determine the power requirements. The server power allocation is not optimized.
6073	cpqHeSysPwrOnDenied	The server could not power on because the hardware cannot be identified.
6074	cpqHePowerFailureError	A device power failure was detected.
6075	cpqHeInterlockFailureError	A device is missing or improperly seated on the system board.
8029	cpqSs6FanStatusChange	The storage enclosure fan status changed.
8030	cpqSs6TempStatusChange	The storage enclosure temperature status changed.

Trap number	SNMP trap name	Description
8031	cpqSs6PwrSupplyStatusChange	The storage enclosure power status changed.
8032	cpqSsConnectionStatusChange	The storage enclosure status changed.
9001	cpqSm2ServerReset	The server power was reset.
9003	cpqSm2UnauthorizedLoginAttempts	The maximum unauthorized login attempt threshold was exceeded.
9005	cpqSm2SelfTestError	iLO detected a self-test error.
9012	cpqSm2SecurityOverrideEngaged	iLO detected that the security override jumper was toggled to the engaged position.
9013	cpqSm2SecurityOverrideDisengaged	iLO detected that the security override jumper was toggled to the disengaged position.
9017	cpqSm2ServerPowerOn	The server was powered on.
9018	cpqSm2ServerPowerOff	The server was powered off.
9019	cpqSm2ServerPowerOnFailure	A power-on request occurred, but the server could not be powered on because of a failure condition.
9020	cpqSm2IrsCommFailure	Communication with Insight Remote Support or Insight Online failed.
11003	cpqHo2GenericTrap	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.
11018	cpqHo2PowerThresholdTrap	A power threshold was exceeded.
11020	cpqHoMibHealthStatusArrayChangeTrap	A server health status change occurred.
14004	cpqIdeAtaDiskStatusChange	AMS detected an ATA disk drive status change.
16028	cpqFca3HostCntlrStatusChange	AMS detected a Fibre Channel host controller status change.
18011	cpqNic3ConnectivityRestored	Connectivity was restored to a logical network adapter.
18012	cpqNic3ConnectivityLost	The status of a logical network adapter changed to Failed.
18013	cpqNic3RedundancyIncreased	AMS detected that a previously failed physical adapter in a connected logical adapter group returned to OK status.
18014	cpqNic3RedundancyReduced	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.
18015	cpqNicAllLinksDown	All links are down on a network adapter.

For more information about these SNMP traps, see the following files in the Insight Management MIB update kit for HPE SIM:

- `cpqida.mib`

- `cpqhost.mib`
- `cpqhlth.mib`
- `cpqsm2.mib`
- `cpqide.mib`
- `cpqscsi.mib`
- `cpqnic.mib`
- `cpqstsys.mib`
- `cpqstdeq.mib`

REST alerts

The following table lists the REST alerts supported by iLO 4 and supported ProLiant servers and Synergy compute modules. To cross reference a REST alert with SNMP trap information, see SNMP traps.

Trap ID	REST Alert ID	REST Severity
0	N/A	N/A
4	SNMPAuthenticationFailure	OK
1006	N/A	N/A
1010	N/A	N/A
1011	N/A	N/A
1012	N/A	N/A
1013	N/A	N/A
1014	N/A	N/A
3033	DrvArrControllerFailed	Critical
	DrvArrControllerOK	OK
3034	DrvArrLogDrvFailed	Critical
	DrvArrLogDrvUnconfigured	Warning
	DrvArrLogDrvRecovering	Critical
	DrvArrLogDrvReadyRebuild	Critical
	DrvArrLogDrvRebuilding	Warning
	DrvArrLogDrvWrongDrive	Critical
	DrvArrLogDrvBadConnect	Critical
	DrvArrLogDrvOverheating	OK
	DrvArrLogDrvShutdown	Warning
	DrvArrLogDrvExpanding	Critical
	DrvArrLogDrvNotAvailable	Ok
	DrvArrLogDrvQueuedForExpansion	Warning
	DrvArrLogDrvMultiPathAccessDegraded	Warning
	DrvArrLogDrvErasing	Warning
	DrvArrLogDrvPredictiveSpareRebuildReady	Warning
	DrvArrLogDrvRapidParityInitializationInProgress	OK
	DrvArrLogDrvRapidParityInitializationPending	OK
	DrvArrLogDrvNoAccessEncryptedMissingKey	Warning
	DrvArrLogDrvUnencryptedToEncryptedTransformationInProgress	Warning
	DrvArrLogDrvRekeyInProgress	Critical
	DrvArrLogDrvNoAccessEncryptedWithControllerEncryptionNotEnabled	Warning
	DrvArrLogDrvUnencryptedToEncryptedTransformationNotStarted	OK
	DrvArrLogDrvNewLogDrvKeyRekeyRequestReceived	Warning
	DrvArrLogDrvOK	Critical

Trap ID	REST Alert ID	REST Severity
3038	DrvArrayAccBoardInvalid	Warning
	DrvArrayAccBoardEnabled	OK
	DrvArrayAccBoardTempDisabled_BadConfiguration	Critical
	DrvArrayAccBoardTempDisabled_LowBatteryPower	Critical
	DrvArrayAccBoardTempDisabled_DisableCommandIssued	Warning
	DrvArrayAccBoardTempDisabled_NoResourcesAvailable	Warning
	DrvArrayAccBoardTempDisabled_BoardNotConnected	Critical
	DrvArrayAccBoardPermDisabled_BadMirrorData	Warning
	DrvArrayAccBoardPermDisabled_ReadFailure	Warning
	DrvArrayAccBoardPermDisabled_WriteFailure	Warning
	DrvArrayAccBoardPermDisabled_ConfigCommand	Warning
	DrvArrayAccBoardTempDisabled_ExpandInProgress	OK
	DrvArrayAccBoardTempDisabled_RedundantLowBattery	OK
	DrvArrayAccBoardTempDisabled_RedundantSizeMismatch	OK
	DrvArrayAccBoardTempDisabled_RedundantCacheFailure	Warning
	DrvArrayAccBoardPermDisabled_ExcessiveECCErrors	Critical
	DrvArrayAccBoardTempDisabled_RAID_ADG_EnablerModuleMissing	Critical
	DrvArrayAccBoardPermDisabled_PostECCErrors	OK
	DrvArrayAccBoardPermDisabled_BackupPowerSourceHotRemoved	Critical
	DrvArrayAccBoardPermDisabled_CapacitorChargeLow	Critical
	DrvArrayAccBoardPermDisabled_NotEnoughBatteries	Warning
	DrvArrayAccBoardPermDisabled_NotSupportedByFirmware	Warning
	DrvArrayAccBoardPermDisabled_BatteryNotSupported	Critical
	DrvArrayAccBoardPermDisabled_NoCapacitorAttached	Critical
	DrvArrayAccBoardPermDisabled_FlashBackedBackupFailed	Warning
	DrvArrayAccBoardPermDisabled_FlashBackedRestoreFailed	Critical
	DrvArrayAccBoardPermDisabled_FlashBackedHardwareFailure	Critical
	DrvArrayAccBoardPermDisabled_CapacitorFailedToCharge	Critical
	DrvArrayAccBoardPermDisabled_IncompatibleCacheModule	Critical
	DrvArrayAccBoardPermDisabled_ChargerCircuitFailure	Critical
	DrvArrayAccBoardTempDisabled_MegaCellNotCabled	Critical
	DrvArrAcceleratorFlashMemoryNotAttached	Warning
3039	DrvArrayAccBoardBadData	Critical
3040	DrvArrayAccBoardBatteryFailed	Critical

Trap ID	REST Alert ID	REST Severity
3046	DrvArrPhysDrvFailed	Critical
	DrvArrPhysDrvPredictiveFailure	Warning
	DrvArrPhysDrvWearOut	Warning
	DrvArrPhysDrvNotAuthenticated	Warning
	DrvArrPhysDrvErasing	Warning
	DrvArrPhysDrvEraseDone	Warning
	DrvArrPhysDrvEraseQueued	Warning
	DrvArrPhysDrvOK	OK
3047	DrvArrSpareDriveFailed	Critical
	DrvArrSpareDriveInactive	OK
	DrvArrSpareDriveBuilding	Critical
	DrvArrSpareDriveActive	OK
3049	DrvArrSolidStateDiskWearOK	OK
	DrvArrSolidStateDiskFiftySixDayThresholdPassed	Warning
	DrvArrSolidStateDiskFivePercentThresholdPassed	Warning
	DrvArrSolidStateDiskTwoPercentThresholdPassed	Warning
	DrvArrSolidStateDiskWearOut	Critical
5022	N/A	N/A
6026	ServerOperational	Warning
6027	POSTErrorsOccurred	Warning
6032	PowerRedundancyLost	Warning
6033	PowerSupplyInserted	OK
6034	PowerSupplyRemoved	Warning
6035	FanDegraded	Critical
6036	FanFailed	Critical
6037	FanRedundancyLost	Warning
6038	FanInserted	OK
6039	FanRemoved	Warning
6041	ThermalStatusDegradedSysShutdown	Critical
	ThermalStatusDegradedSysContinue	Critical
6042	ThermalStatusOK	OK
6048	PowerSupplyOK	OK
6049	PowerSupplyDegraded	Critical
6050	PowerSupplyFailed	Critical
6051	MirroredMemoryEngaged	Warning
6054	PowerRedundancyRestored	OK

Trap ID	REST Alert ID	REST Severity
6055	FanRedundancyRestored	OK
6064	CorrectableOrUncorrectableMemoryErrors	Warning
6069	PowerSupplyACPowerLoss	Critical
6070	SystemBatteryFailed	Warning
6071	SystemBatteryRemoved	Warning
6072	SystemPowerAllocationNotOptimized	Critical
6073	SystemPowerOnDenied	Critical
6074	PowerFailureErrorTempAboveCritical	Critical
	PowerFailureErrorInputPowerLoss	Critical
	PowerFailureErrorBadFuse	Critical
	PowerFailureStandby	Critical
	PowerFailureRuntime	Critical
	PowerFailurePowerOn	Critical
	PowerFailureUnknown	Critical
	PowerFailureCpuThermalTrip	Critical
6075	InterlockFailureErrorStandby	Critical
	InterlockFailureErrorRuntime	Critical
	InterlockFailureErrorPowerOn	Critical
	InterlockFailureErrorUnknown	Critical
8029	StorageSystemFanFailed	Critical
	StorageSystemNoFan	Warning
	StorageSystemFanDegraded	Critical
	StorageSystemFanOK	OK
8030	StorageSystemTemperatureFailed	Critical
	StorageSystemTemperatureDegraded	Critical
	StorageSystemTemperatureOK	Warning
	StorageSystemNoTemperature	OK
8031	StorageSystemPwrSupplyDegraded	Critical
	StorageSystemNoPwrSupply	Warning
	StorageSystemPwrSupplyOK	OK
8032	N/A	N/A
9001	ServerResetDetected	Warning
9003	UnauthorizedLoginAttempts	OK
9005	N/A	N/A
9012	SecurityOverrideEngaged	OK
9013	SecurityOverrideDisengaged	OK
9017	ServerPoweredOn	OK

Trap ID	REST Alert ID	REST Severity
9018	ServerPoweredOff	OK
9019	ServerPowerOnFailure	Critical
9020	ILOToInsightRemoteSupportCommunicationFailure	Warning
11003	N/A	N/A
11018	PowerThresholdBreach	Warning
11020	N/A	N/A
14004	N/A	N/A
16028	N/A	N/A
18011	NicConnectivityRestored	OK
18012	NicConnectivityLost	Warning
18013	N/A	N/A
18014	N/A	N/A

Configuring Insight Management integration

Prerequisites

Configure iLO Settings privilege

Procedure

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.
4. Select the Level of Data Returned.
5. Optional: Click View XML Reply to view the response sent to HPE SIM when it uses the provided address to request iLO management processor identification.
6. To save the changes, click Apply.

Insight Management integration options

HPE SMH FQDN/IP Address

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.

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.

  When the iLO health status is Degraded, iLO displays the health status and a description of the issue on the Login page. The iLO health status is based on the combined results of the iLO diagnostic self-tests. Self-test failures that could compromise security are not displayed in the description.

- Disabled (No Response to Request)—Prevents iLO from responding to HPE SIM requests.

View XML Reply

Displays the response sent to HPE SIM when it uses the provided address to request iLO management processor identification.

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

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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. To save the changes, click Apply.
5. Optional: To send a test message to the configured email addresses, click Send Test AlertMail.

   This button is available only when AlertMail is enabled.

   The test AlertMail is initiated.
6. Optional: If you sent a test message, check the iLO Event Log to confirm that it was sent successfully.

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 Mail Submission Agent. This server cooperates with the Mail Transfer Agent to deliver the email. This string can be up to 63 characters.

Disabling AlertMail

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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.

The remote syslog format adheres to RFC5242. The syslog must start with the iLO time stamp followed by the iLO Hostname, the subsystem name (that generated the log), and the log text. For example:

```
2020-08-26T15:26:43Z  ILO7CE712P2K6  DriveArray  Smart Array - Drive is failed: Port Box 0 Bay 0
ACTION:1. Be sure all cables are connected properly and securely. 2. Be sure all drives are
fully seated. 3 Replace the defective cables, drive, or both.
```

Enabling iLO remote syslog

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The remote syslog server is configured to use UDP.

Procedure

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. To save the changes, click Apply.
5. (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.

Remote syslog options

- Remote Syslog Port—The port number through which the syslog server is listening. Only one port number can be entered in this box. When you enter multiple remote syslog servers, they must use the same port. The default value is 514.
- Remote Syslog Server—The IP address, FQDN, IPv6 name, or short name of the server running the syslog service. To enter multiple servers, separate the server IP address, FQDN, IPv6 name, or short name with a semicolon. You can enter up to 63 characters per server, and a total of 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, it can send its logs to the syslog server.

Disabling iLO Remote Syslog

Prerequisites

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Configure iLO Settings privilege

Procedure

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.

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.

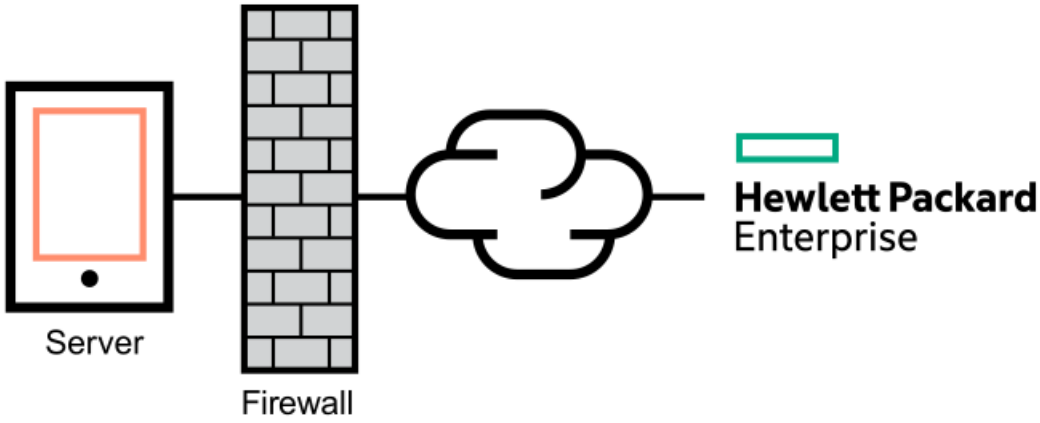
Connecting a server to Hewlett Packard Enterprise allows it to be remotely supported and to send diagnostic, configuration, telemetry, and contact information to Hewlett Packard Enterprise. No other business information is collected, and the data is managed according to the Hewlett Packard Enterprise 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

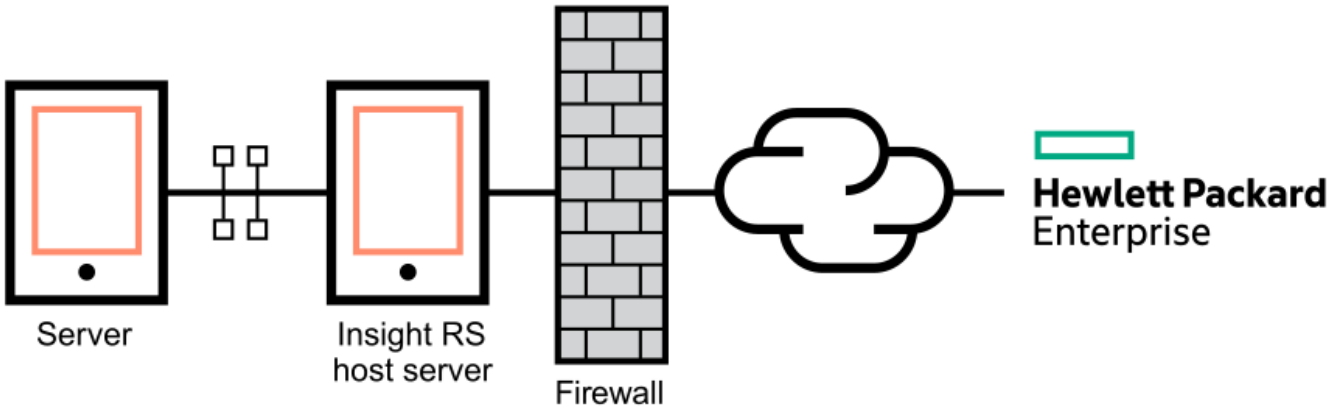
Register a server directly with Insight Online without the need to set up an Insight Remote Support centralized host server in your local environment. Insight Online will be your primary interface for remote support information.

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.



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).



Device support

Embedded remote support registration is supported for the following device types.

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.

Insight Online direct connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

Insight Remote Support central connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

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 seven days, and configuration information is sent every 30 days. The following information is included:

Registration

During server registration, iLO collects data to 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 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.

HPE Tech Care service

HPE Tech Care service customers must register their servers for remote support to receive the following Tech Care features: Tech Care 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: **https://www.hpe.com/services/techcare**.

Prerequisites for remote support registration

Procedure

1. Install a supported browser to use when you log in to the remote support solution components .
2. If you do not have an HPE Passport account, create one at the following website: **http://www.hpe.com/info/insightonline**, and make a note of your login credentials.

   In most cases, your HPE Passport user ID is the same as the email address you used during the HPE Passport registration process. If you changed your user ID in the Hewlett Packard Enterprise Support Center, be sure to log in with your user ID and not your email address.
3. Navigate to the following website and verify that the product you will register for remote support has an active Hewlett Packard Enterprise warranty or contract: **http://www.hpe.com/support/hpesc**.
4. Collect the following information. This information is used during the Insight Online direct connect registration procedure or the Insight Remote Support central connect host server configuration procedure:
   - Contact information. Hewlett Packard Enterprise uses this information when a support case is created.
   - Site information (site name, address, and time zone). Hewlett Packard Enterprise uses this information when service personnel or a part must be sent to your location.
   - Web proxy information (if a web proxy is used to access the Internet).
   - Channel Partner IDs for your authorized service provider, reseller/distributor, and installer, if you want to allow Channel Partners to view your device information. The installer is required only for Insight Remote Support central connect.

     The Partner ID is the Location ID assigned to the Channel Partner during the partner registration process. If you do not know a Channel Partner ID, contact the partner to obtain that information.
5. Set up ProLiant servers for remote support registration .

   If your servers are already set up, ensure that they meet the requirements described in the server setup instructions.
6. Obtain the iLO hostname or IP address and login credentials (login name and password).

   You can use any local or directory-based user account that has the Configure iLO Settings privilege.
7. For direct connect only: Make sure that your environment meets the Insight Online direct connect network requirements .
8. For central connect only: Set up the Insight Remote Support central connect environment .
9. Verify access to Insight Online.

Supported browsers for HPE embedded remote support

iLO

iLO 4 supports the browsers listed in Supported browsers.

Insight RS

- Microsoft Internet Explorer: 9x, 10x, 11x
- Mozilla Firefox: 49.x
- Google Chrome: 53.x

Insight Online

- Microsoft Internet Explorer: 11 or later
- Mozilla Firefox: Latest version
- Google Chrome: Latest version

Setting up a ProLiant server for remote support registration

Prerequisites

Ensure that you have the required files to set up or update a ProLiant server. Depending on your configuration, you might need the following files:

- **Service Pack for ProLiant (All supported OS except for Ubuntu)** —The SPP includes the iLO firmware, iLO 4 Channel Interface Driver, and AMS. Download the SPP from the following website: **http://www.hpe.com/servers/spp**.

  You can download the iLO 4 Channel Interface Driver, iLO firmware, and AMS separately at the following website: **http://www.hpe.com/support/ilo4**.

- **Management Component Pack (Ubuntu)**—The MCP includes AMS but it does not include the iLO firmware or the iLO driver. Download the MCP from the following website: **http://www.hpe.com/support/SDR-Linux**.

Procedure

1. Install the server hardware.
2. Connect iLO to the network.
3. Use Intelligent Provisioning to configure the server and install an OS.

   During this process, Intelligent Provisioning will prompt you to register for remote support. If you want to use iLO to register, select Register Later on the Intelligent Provisioning remote support registration page.

   For more information, see the Intelligent Provisioning user guide.
4. (Optional) Install AMS if it is not already installed.

   Hewlett Packard Enterprise recommends installing AMS.

   HPE Proactive Care services customers only: AMS installation is required to receive the following Proactive Care features: Proactive Scan Report and Firmware and Software Version Report.

   Using 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.
5. If you did 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 Access Settings page in the iLO web interface.

     To protect your privacy, do not use sensitive information in the server name. The server name is displayed in Insight Online and Insight RS.
6. On Windows servers: Install the iLO 4 Channel Interface Driver.

   If you use the Intelligent Provisioning Recommended installation method for Windows installation, the iLO 4 Channel Interface Driver for Windows is installed automatically.

   For Red Hat Enterprise Linux, SUSE Linux Enterprise Server, and Ubuntu, the driver is included in the Linux distribution.
7. Verify that 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.

   iLO 4 2.60 or later is required for Insight Remote Support direct connect registration.
8. Verify that the time zone is set in iLO.

   If the Time Zone value is incorrect, Insight Online will display incorrect time stamps for events and data collections.
9. Verify that a DNS server is configured in iLO.

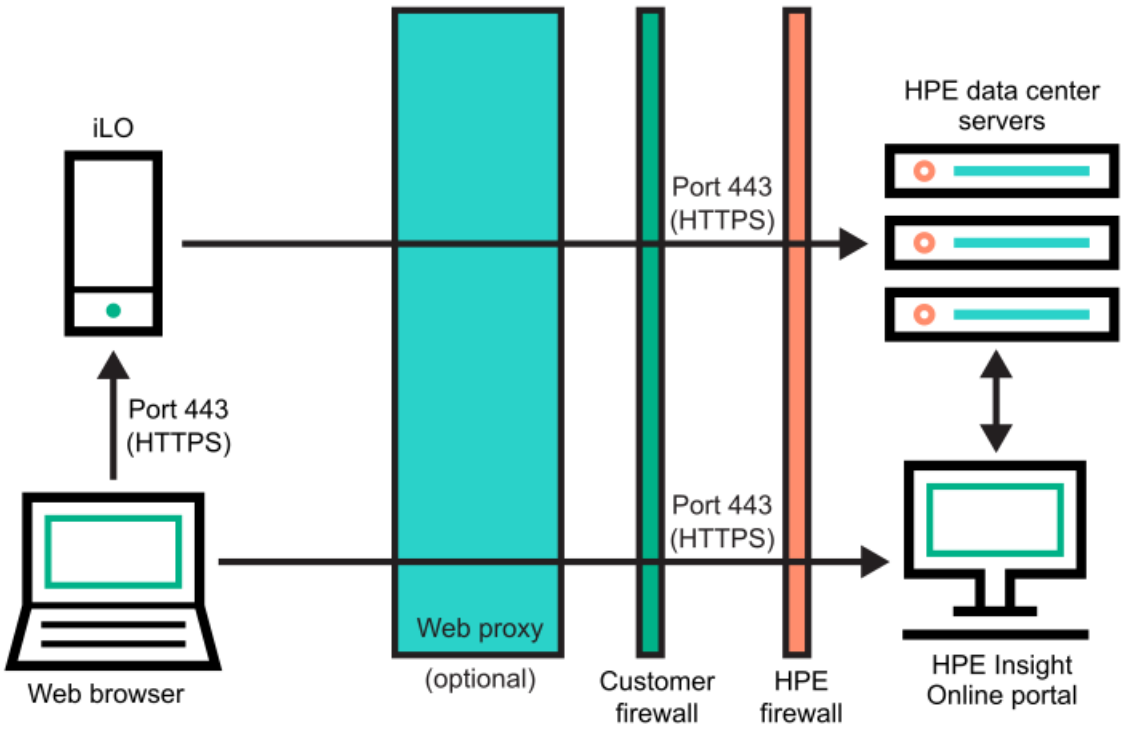
   By default, iLO is set to use DHCP to configure DNS servers and other network settings.

   The DNS server is required for communication between iLO and Insight Online.

Insight Online direct connect network requirements

Insight Online direct connect relies on communication between your environment and Hewlett Packard Enterprise to deliver support services. Ensure that your environment meets the port requirements shown in Figure 3: Network requirements for Insight Online direct connect.

Figure 3: Network requirements for Insight Online direct connect



Setting up the Insight Remote Support central connect environment

Insight Remote Support relies on communication between your environment and Hewlett Packard Enterprise to deliver support services.

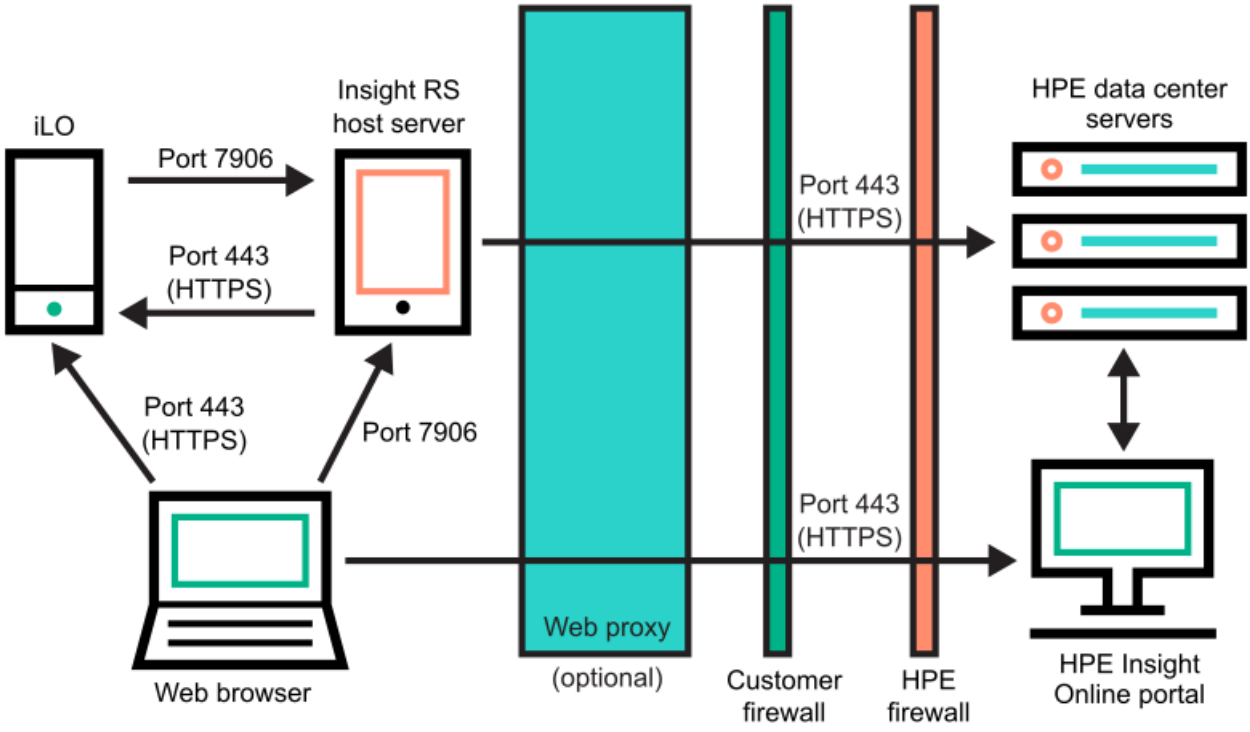
Procedure

1. Verify that the server you will use for the Insight RS host server meets the requirements listed in the Insight Remote Support release notes.

   The host server is called the Hosting Device in the Insight RS software.

2. Ensure that your environment meets the port requirements shown in Figure 4: Network requirements for Insight Remote Support central connect.

Figure 4: Network requirements for Insight Remote Support central connect



3. Set up the Insight RS host server.

   a. Ensure that the version of the Insight RS software on the host server supports the ProLiant servers you want to register. For more information, see the following website: **https://www.hpe.com/support/InsightRS-Support-Matrix**.

   b. Use the Insight RS console to configure the RIBCL protocol for ProLiant servers that will be registered for Insight Remote Support central connect.

   c. (Optional) If you will use HPE SIM with Insight RS, configure the HPE SIM adapter.

   For more information, see the Insight Remote Support installation and configuration guide, at the following website: **https://www.hpe.com/info/insightremotesupport/docs**.

4. Verify communication between the Insight RS host server and the remote support web service.

   To complete this task, start a web browser on the Insight RS host server, and navigate to the following website: **https://api.support.hpe.com/v1/version/index.html**.

   If connectivity between the server and HPE is set up correctly, the web browser displays the version of some of the data center components (for example, `19.1.17.470`).

Verifying access to Insight Online

Procedure

1. Navigate to the following website: **http://www.hpe.com/info/insightonline**.
2. Enter your HPE Passport user ID and password, and then click Sign in.

   If you do not have an HPE Passport account, follow the onscreen instructions to create one.

   The Hewlett Packard Enterprise Support Center website is displayed with the Insight Online My IT Environment tab selected. During the initial setup, your IT Environment shows no entries in the Devices, Service events, and Contracts and warranties sections.

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 HPE Passport account. For more information, see **http://www.hpe.com/info/insightonline**.

Procedure

1. Complete step 1 of Insight Online direct connect registration in the iLO web interface.
2. Complete step 2 of Insight Online direct connect registration in Insight Online.
3. Confirm that registration is complete in the iLO web interface.
4. Complete the optional post-registration steps in the iLO web interface.

Registering for Insight Online direct connect (step 1)

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Remote Support > Registration page.
2. Select Connect this server directly to HPE.
3. Enter your HPE 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: **https://www.hpe.com/software/SWLicensing**.
6. Click Register.

   iLO notifies you that step 1 of the registration process is finished, and prompts you to complete step 2.

   Allow up to 5 minutes for your registration request to be fully processed.

Registering for Insight Online direct connect (step 2)

Procedure

1. Navigate to the following website: **http://www.hpe.com/info/insightonline**.
2. Log in with your HPE Passport credentials.
3. On the Insight Online My IT Environment tab, click Devices with incomplete registration.
4. Select one or more devices on the Step 1: Select target devices page, and then click Next.

   If the selected devices share site, support, and partner information, you can register up to 15 devices at a time.
5. Enter site and support information on the **Step 2: Provide site and support information** page, and then click Next.
6. Do one of the following on the Step 3: Provide HPE Authorized Channel Partner information page:
   - If Hewlett Packard Enterprise supports your IT infrastructure, accept the default settings.
   - If a Hewlett Packard Enterprise Authorized Channel Partner supports your IT infrastructure, enter the Partner location ID for an authorized service partner and an authorized reseller/distributor.

     To verify that you entered the correct partner, click Check ID.
7. (Optional) To allow Hewlett Packard Enterprise or an Authorized Channel Partner to contact you about optimizing your IT environment, select the Optimize my IT environment check box.
8. To continue to the Step 4: Validate and Submit page, click Next.
9. Review the information you entered, and then click Complete registration.

   The Complete device registration window displays a summary of the registration status.
10. Click Done.

Confirming registration is complete (iLO web interface)

Prerequisites

Configure iLO Settings privilege

Procedure

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 optional post-registration steps

Procedure

1. (Optional) Send a test event to confirm the connection between iLO and HPE remote support.
2. (Optional) To receive email alerts about system events, configure AlertMail.

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.

Procedure

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

Procedure

1. Navigate to the Remote Support > Registration page.
2. Select Connect this server through an HPE remote support host server.
3. Enter the Host server hostname or IP address and Port number.

   You can enter a host name, an IPv4 address, or an IPv6 address.

   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 HPE remote support.
6. (Optional) To receive email alerts about system events, configure AlertMail.

Unregistering from Insight Online direct connect

Prerequisites

Configure iLO Settings privilege

Procedure

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

Procedure

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 a 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 > Registraton page in the iLO web interface.
4. Verify that the server is not registered.

Remote support service events

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, service event details are recorded in the service event log. Depending on your remote support configuration, the details are sent to Insight Online (direct connect) or 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). Enabling the maintenance mode feature during planned maintenance prevents the opening of a support case during the planned maintenance period.

Service event transmission

When a service event occurs, information about the event is sent to Hewlett Packard Enterprise.

If a service event transmission failure occurs, two additional attempts are made. If the event cannot be sent after three attempts:

- An SNMP trap (`cpqSm2IrsCommFailure 9020`) is generated. This SNMP trap is defined in the `cpqsm2.mib` file.
- The failure is logged in the service event log.
- The failure is logged in the iLO event log.
- The service event is recorded in the Active Health System log.
- A failure message is recorded in the Active Health System log.

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

Procedure

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.

   TIP:

   To end maintenance mode early, select the Clear Maintenance Mode check box, and then click Apply.

   Maintenance mode ends automatically when the specified amount of time has passed. iLO notifies you when maintenance mode is cleared.

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

Procedure

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.
4. Optional: For Insight Remote Support central connect only: To verify that the test event is displayed, check the Insight RS Console.
5. Optional: To verify that the test event is displayed, check Insight Online.

Viewing a test service event by using Insight Online

Prerequisites

A test service event was sent on a server that is registered for remote support.

Procedure

1. Navigate to the following website: **http://www.hpe.com/info/insightonline**.
2. Log in with your HPE Passport credentials.
3. To view a summary of the recorded service events, click Service events.

   Insight Online converts the service event Time Generated value to Coordinated Universal Time (UTC).
4. To view test events, select View > Test events.

   Test events are closed automatically because no further action is necessary.

   To view activities that occurred after you logged in to Insight Online, click the refresh button.

Viewing a test service event by using the Insight RS Console

Prerequisites

A test service event was sent on a server that is registered for Insight Remote Support central connect.

Procedure

1. Log in to the Insight RS Console (https://<Insight RS host server IP address>:7906).
2. Navigate to the Devices page.
3. Find your server or enclosure, and then click the device name.
4. Click the Service Events tab.
5. The list of service events is displayed.
6. Insight RS converts the service event Time Generated value to the time zone of the browser used to access the Insight RS Console.
7. Test events are closed automatically because no further action is necessary.

Viewing the service event log

Prerequisites

The server is registered for remote support.

Procedure

Navigate to the Remote Support > Service Events page.

Service event log details

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.
- 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:

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
1000	Generic Service Event

Clearing the Service Event Log

Prerequisites

Configure iLO Settings privilege

Procedure

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 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.

Sending data collection information

Depending on your remote support configuration, iLO or the Insight RS host server sends configuration information to Hewlett Packard Enterprise. This information is used for analysis and proactive services in accordance with your warranty and service agreements.

- **Insight Online direct connect**—Data is transmitted every 30 days. You cannot edit or delete the data collection schedule.
- **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.

Use the following procedure to send data collection manually, if you do not want to wait for the next scheduled transmission.

Prerequisites

Configure iLO Settings privilege

Procedure

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.
4. Optional: To verify that the data collection time stamp is accurate, check Insight Online.
5. Optional: To verify that the data collection information is displayed, check the Insight RS Console.

Sending Active Health System reporting information

Depending on your remote support configuration, 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.

- **Insight Online direct connect**—Data is transmitted every seven days. You cannot edit or delete the Active Health System reporting schedule.
- **Insight Remote Support central connect** —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.

Use the following procedure to send Active Health System reporting information manually, if you do not want to wait for the next scheduled transmission. You can also download Active Health System information directly on the Active Health System page.

Prerequisites

Configure iLO Settings privilege

Procedure

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.
4. Optional: To verify that the Active Health System information is displayed, check the Insight RS Console.

Viewing data collection status in iLO

Procedure

Navigate to the Remote Support > Data Collections page.

Data Collection details

- Data Collection Frequency (days) (Insight Online direct connect only)—The frequency at which data is sent to Hewlett Packard Enterprise.
- 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.
- Next Data Collection Scheduled (Insight Online direct connect only)—The next date and time when data will be sent to Hewlett Packard Enterprise.

Viewing Active Health System reporting status in iLO

Procedure

Navigate to the Remote Support > Data Collections page.

Active Health System reporting details

- 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.
- 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.
- 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.

Viewing data collection status in Insight Online

The Insight Online device overview page displays the time stamp of the last data collection transmission.

Procedure

1. Log in to the Hewlett Packard Enterprise Support Center (**http://www.hpe.com/info/insightonline**).
2. Navigate to the Devices page.
3. Click the name of a device.

   The Overview page displays the date and time of the last data collection transmission in the Configuration section.

> **TIP:**
>
> To view activities that occurred after you signed in to Insight Online, click the refresh button.

Viewing data collection status in the Insight RS Console (Insight Remote Support central connect only)

Procedure

1. Log in to the Insight RS Console (https://<Insight RS host server IP address or FQDN>:7906).
2. Navigate to the Devices page.
3. Find your server, and then click the device name.
4. Click the Collections tab.

   The Collections tab displays the following names for data collection information and Active Health System reporting information: Server Basic Configuration Collection and Active Health Service Collection. To expand a collection, click the plus sign (+) to the left of the Result icon. To view additional information or download the collection files, click More Details.

   Insight RS converts the iLO data transmission date and time values to the time zone of the browser used to access the Insight RS Console.

Registering a ProLiant server used as a host server for Insight Online direct connect

Hewlett Packard Enterprise does not support Insight Online direct connect registration of a ProLiant server that is used as an Insight RS host server. If you register an active host server for Insight Online direct connect, all the devices monitored by that host server will be unable to communicate with Hewlett Packard Enterprise to receive remote support.

Use this procedure to stop using a ProLiant server as a host server, unregister the server from Insight Remote Support central connect, and then register the server for Insight Online direct connect.

Procedure

1. (Optional) Use Insight RS to export a Bulk CSV file containing the list of monitored devices.

   For more information, see the **Insight RS documentation**.

   You can use this file later if you want to add the previously monitored devices to a new host server.
2. Unregister the monitored devices from the Insight RS host server on the ProLiant server.
3. Unregister the ProLiant host server from Insight RS.
4. Uninstall Insight RS from the ProLiant server.
5. Register the ProLiant server for Insight Online direct connect.
6. (Optional) Install Insight RS on a different server, and then configure a new host server.
7. (Optional) Import the Bulk CSV file into Insight RS on the new host server.

   For more information, see the **Insight RS documentation**.

Changing the remote support configuration of a supported device

Hewlett Packard Enterprise does not support registering a device for Insight Remote Support central connect and Insight Online direct connect at the same time. If you register a device using both configurations, it will have two communication paths to Hewlett Packard Enterprise and Insight Online. Device information might be overwritten each time data is sent to Hewlett Packard Enterprise.

Changing a supported device from central connect to direct connect remote support

Procedure

1. Unregister the device from Insight Remote Support central connect.
2. Determine the correct time to register the device for Insight Online direct connect.

   If iLO and the Insight RS host server use different time zones, and iLO uses an earlier time zone than the Insight RS host server, do not reregister the device immediately. Wait until the iLO time is the same as or later than the time at which you unregistered the device.

   For example, you might have an Insight RS host server set to the local time in France, and an iLO system set to the local time in California. If you unregister the device at 5 p.m. local time in France, you must wait until 5 p.m. local time in California to register the device for Insight Online direct connect. If you do not wait, the device will not be displayed in Insight Online.
3. If applicable, wait until the time determined in step 2.
4. Register the device for Insight Online direct connect.

Changing a supported device from direct connect to central connect remote support

Procedure

1. Unregister the device from Insight Online direct connect.
2. Determine the correct time to register the device for Insight Remote Support central connect.

   If iLO and the Insight RS host server use different time zones, and the Insight RS host server uses an earlier time zone than iLO, do not reregister the device immediately. Wait until the Insight RS host server time is the same as or later than the time at which you unregistered the device.

   For example, you might have an iLO system set to the local time in France, and a host server set to the local time in California. If you unregister the device at 5 p.m. local time in France, you must wait until 5 p.m. local time in California to register the device for Insight Remote Support central connect. If you do not wait, the device will not be displayed in Insight Online (if enabled).
3. If applicable, wait until the time determined in step 2.
4. Register the device for Insight Remote Support central connect.

iLO ROM-based utilities

You can configure iLO settings by accessing the ROM-based utilities from the physical system console, or by using an iLO Remote Console session.

The ROM-based utility embedded in the system ROM of your server depends on your server model.

- ProLiant Gen8 servers, except for the DL580 Gen8 server, have the iLO RBSU software embedded in the system ROM.

  To access the iLO RBSU, you press F8 during POST.

  Use the arrow keys and the Enter key to navigate the iLO RBSU menus. To make configuration changes, follow the onscreen instructions.

  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.

- ProLiant Gen9 servers, Synergy compute modules, and the DL580 Gen8 server have the UEFI System Utilities software embedded in the system ROM.

  To access the UEFI System Utilities, you press F9 during POST, and then select System Configuration > iLO 4 Configuration Utility.

  For more information, see the UEFI System Utilities user guide.

For information about iLO setup tasks you perform with the ROM-based utilities, see Setting up iLO by using the ROM-based setup utilities.

Configuring network settings with the ROM-based utilities

Configuring NIC and TCP/IP settings (iLO RBSU)

Procedure

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.

   The Network Configuration screen is displayed.
5. View or update the NIC and TCP/IP settings.
6. To save your changes, press F10
7. Select File > Exit.

Configuring DNS/DHCP settings (iLO RBSU)

Procedure

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.

   The Network Autoconfiguration page is displayed.
5. View or update the DNS and DHCP settings.
6. To save your changes, press F10
7. Select File > Exit.

Configuring advanced network settings (iLO RBSU)

Procedure

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.

   The Network Autoconfiguration screen is displayed.
5. Press F1.

   The Advanced Autoconfiguration Setup and Status screen is displayed.
6. View or update the advanced network settings.
7. To save your changes, press F10.
8. Select File > Exit.

Configuring Network Options (iLO 4 Configuration Utility)

Procedure

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.

Configuring Advanced Network Options (iLO 4 Configuration Utility)

Procedure

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.

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

Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network. This option is available only when Network Interface Adapter is ON (iLO Dedicated Network Port).

Transceiver Speed Manual Setting

Sets the link speed for the iLO network interface. This option is available only when Network Interface Adapter is ON (iLO Dedicated Network Port) and Transceiver Speed Autoselect is OFF.

Transceiver Duplex Setting

Sets the link duplex setting for the iLO network interface. This option is available only when Network Interface Adapter is ON (iLO Dedicated Network Port) and Transceiver Speed Autoselect is OFF.

VLAN Enable

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 appear to be on separate LANs, even if they are physically connected to the same LAN. This option is available only when Network Interface Adapter is set to Shared Network Port.

VLAN ID

When a VLAN is enabled, this option 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 available only 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 be used only 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 the DHCP server-supplied gateway.

Gateway #1, Gateway #2, and Gateway #3

If Gateway from DHCP is disabled, enter 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, enter 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, and DNS Server 3

If DNS from DHCP is disabled, enter 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, enter the primary and secondary WINS servers.

Domain Name

The iLO domain name. If DHCP is not used, enter a domain name.

Configuring access settings with the ROM-based utilities

Configuring global settings (iLO RBSU)

Procedure

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.

   The Global iLO 4 Settings screen is displayed.
5. 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 the iLO RBSU, select File > Exit.

Configuring serial CLI options (iLO RBSU)

Procedure

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.

   The Configure iLO Command-Line Interface screen is displayed.
5. Select an option and press the spacebar to toggle through the available settings.
6. To save the changed settings, press F10
7. To close the iLO RBSU, select File > Exit.

Configuring access settings (iLO 4 Configuration Utility)

Procedure

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.

Viewing information about iLO by using the iLO 4 Configuration Utility

Procedure

1. Optional: If you access the server remotely, start an iLO Remote Console session.
2. Restart or power on the server.
3. To start the UEFI System Utilities, press F9 in the server POST screen.
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 iLO

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.

Browser requirements

- JavaScript—iLO 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 Enabling JavaScript for Internet Explorer.

- 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 iLO through a web browser, you must enable TLS 1.0 or later in the browser.

Supported browsers

HPE iLO 4 supports the latest versions of the following browsers:

Preferred browsers

- Google Chrome mobile and desktop versions
- Mozilla Firefox
- Microsoft Edge

Chrome, Firefox, and Edge provide the best performance with HPE iLO 4.

Legacy browsers

- Microsoft Internet Explorer 11

Enabling JavaScript for Internet Explorer

Some versions of Internet Explorer have JavaScript disabled by default. Use the following procedure to enable JavaScript.

Procedure

1. Start Internet Explorer.
2. Select Tools > Internet options.
3. Click Security.
4. Click Custom level.
5. In the Scripting section, set Active scripting to Enable.
6. Click OK.
7. Refresh your browser window.

Logging in to the iLO web interface

Procedure

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:

   - Enter a directory or local user account login 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 beneath the Log In button. You can use the Zero Sign In button to log in without entering a user name and password.

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 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 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 into 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 logging out. 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.
- Logging out of 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 an 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.

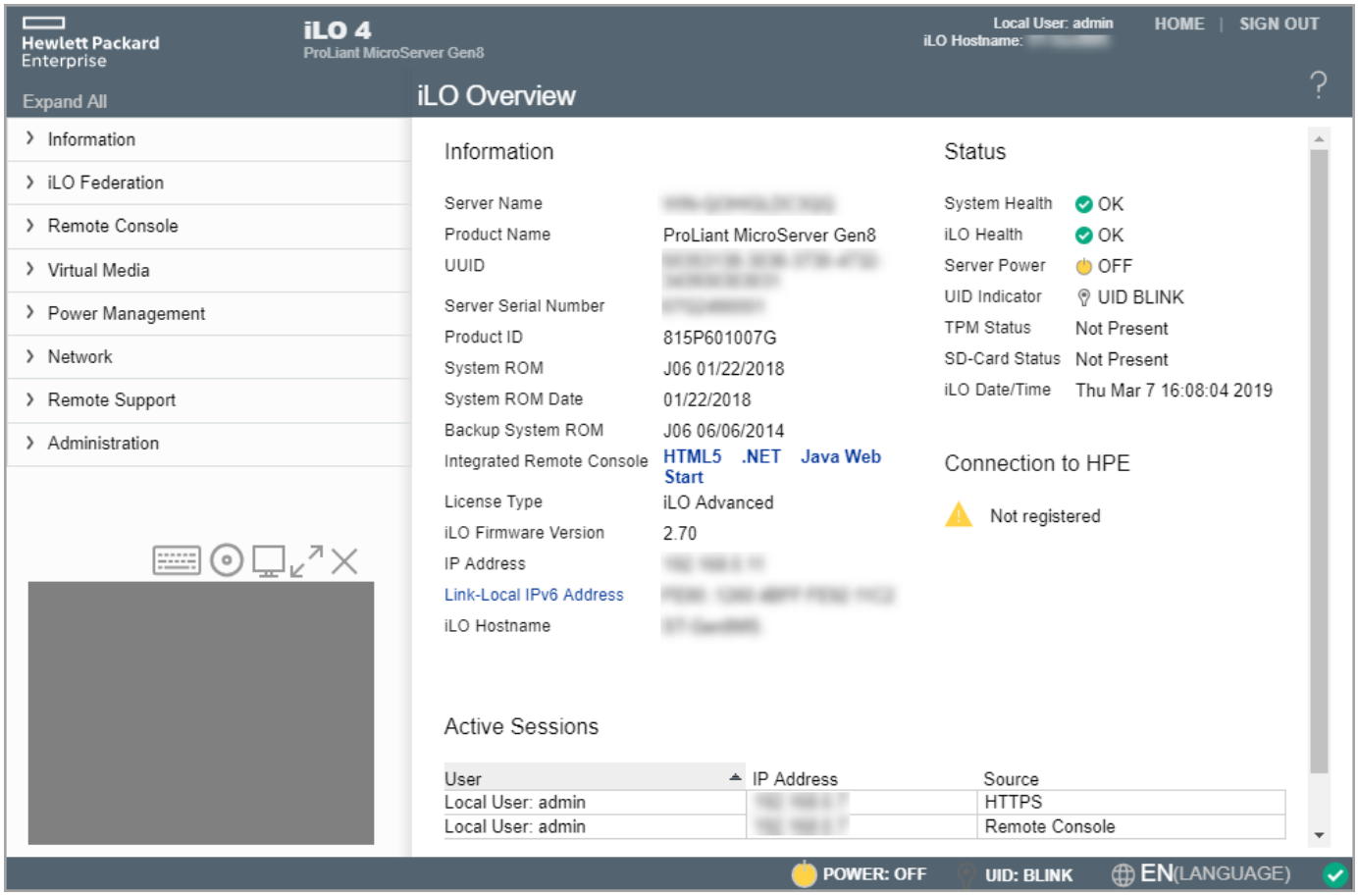
- Log out of an iLO session before you close the browser window.

iLO web interface overview

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.



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.

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 Button features.
- UID—Click this icon to turn the UID LED on and off.
- Language—Use this menu to select a language or to navigate to the 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—Click this icon to view the overall health status for iLO, the server fans, temperature sensors, and other monitored subsystems. For all components except AMS, click a component to view additional details.

Starting a remote management tool from the login page

Prerequisites

iLO is under the control of a remote management tool.

Procedure

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.

Changing the language from the login page

If a language pack is installed, use the language menu on the login screen to select the language for the iLO session. This selection is saved in a browser cookie for future use.

Prerequisites

A language pack is installed.

Procedure

1. Navigate to the iLO Login page.
2. Select a language from the Language menu.

Viewing iLO overview and system information

Viewing iLO overview information

Procedure

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 details

- 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. 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 ROM-based 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. 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.
- 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 ROM-based system utilities during POST.
- Chassis Serial Number—The serial number of the chassis that contains the server node.

  This value is displayed only for server nodes in an HPE Apollo chassis.

  This information is displayed for servers with chassis firmware version 6.0 or later.
- Node Number—The server node number within the chassis.

  This value is displayed only for ProLiant SL and XL servers.
- 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 HTML5 IRC, .NET IRC, or Java IRC for remote, out-of-band communication with the server console.
- 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

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. The possible values are OK, Degraded, and Critical. To navigate to the Health Summary page, click the System Health link.

iLO Health

The iLO health status, which is based on the combined results of the iLO diagnostic self-tests. The possible values are OK and Degraded. To navigate to the Diagnostics page, click the iLO 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.

To turn the UID LED on or off, use 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.

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.

The possible values are:

- 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:
  - 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.

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.

Connection to HPE status

This 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.

You can click the status value to navigate to the remote support registration page.

Active sessions list

The iLO Overview page displays the following information about all users logged in to iLO.

- Login name
- IP address
- Source (for example, HTTPS, Remote Console, or SSH)

Viewing health summary information

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.

Procedure

1. Navigate to the Information > System Information page, and then click the Summary tab.
2. (Optional) To sort by a table column, click the column heading.

   To change the sort order to ascending or descending, click the column heading again or click the arrow icon next to the column heading.
3. (Optional) To navigate to a related page for supported subsystem and device types, click the name of a value in the Subsystems and Devices list.

   Some subsystem and device types, such as the Agentless Management Service, do not have a related page.

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:

- Agentless Management Service
- BIOS/Hardware Health
- Fans
- Memory
- Network
- Power Supplies (nonblade servers only)
- Processors
- Storage
- Temperatures
- Smart Storage Battery Status (supported servers only)

Subsystem and device 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.

  iLO 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. If a redundant fan or power supply fails while the system is powered on, the system health status is 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 device status information. After iLO is reset when the server is powered off, some subsystems display the status Unknown. iLO cannot update the status for these subsystems when the server is powered off.
- Not Installed—The subsystem or device is not installed.

Viewing fan information

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.

Procedure

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.

Fan details

The following details are displayed for each fan:

- Fan—The fan name.
- Location—This value depends on the server type.

  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.
- 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 lack 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 the installed server and nonserver blades to adjust the fans to provide the appropriate enclosure cooling.

Temperature information

The Temperature Information page 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

Procedure

1. Navigate to the Information > System Information page, and then click the Temperatures tab.
2. Optional: Customize the graph display.
   - To display a three-dimensional graph, select the 3D check box.
   - To display a two-dimensional graph, clear the 3D check box.
   - To display the sensors at the front or back of the server, select Front View or Back View.
3. Optional: To view individual sensor details, move the mouse over a circle on the graph.

   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 measured by a sensor increases, the graph changes from green to amber, and then to red if the temperature approaches the critical threshold.

Viewing temperature sensor data

Procedure

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—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 on physical memory DIMMs.
  - Temperature sensors located close to the memory DIMMs, but not 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.
- 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 lower than 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.
- Starting a graceful shutdown of the operating system to avoid data corruption.

Additional policies are implemented after an excessive temperature condition is corrected. For example:

- Returning the fan speed to normal.
- Recording the event in the IML.
- Turning off the LED indicators.
- Canceling shutdowns in progress (if applicable).

Viewing power information

Procedure

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.
- **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

This section is displayed for nonblade servers.

Present Power Reading

When 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 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 Meter page.

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 iPDUs (if Power Discovery Services is used) is not providing 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.

Power Discovery Services Status

The possible values follow:

- Redundant—The server is configured for a redundant iPDU configuration.
- Not Redundant—There are not sufficient iPDUs to support redundancy, or the server power supplies are connected to the same iPDU.
- N/A—No iPDUs were discovered.

When the iLO processor or the server is reset, the iPDU discovery process might take a few minutes to complete.

Power Supplies list

Some power supplies do not provide information for all the values in this list. If a power supply does not provide information for a value, N/A is displayed.

This section is displayed for nonblade servers (DL, ML).

- 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.

Power Discovery Services iPDU Summary

This section is displayed for nonblade servers 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 iPDUs.
- iPDU Not Redundant—This Caution status indicates that the server is not connected to at least two different iPDUs. 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.

Power Readings

This section is displayed for server blades and Synergy compute modules.

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.

Power Microcontroller

This section is displayed for server blades and Synergy compute modules.

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. If redundant power supplies are configured, these conditions result in a loss of redundancy. If redundant power supplies are not used, these conditions result in a loss of operation. 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.

For more information, see the following website: **https://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.

Viewing processor information

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.

Procedure

Navigate to the Information > System Information page, and then click the Processors tab.

Processor details

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

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.

Procedure

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.

Advanced Memory Protection details

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—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

- 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

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

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.

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

If the server is powered off, the health status information on the NIC Information 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.

Procedure

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.

Physical Network Adapters

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 iLO 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 is connected to the network and is functioning correctly, iLO displays the status OK.
  - 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.
  - In configurations with multiple NICs, if a component has failed but the system is still functioning, iLO displays the status Degraded.
  - If a NIC reports a failure, iLO displays the status Critical.
- 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.
  - In configurations with multiple NICs, if a component has failed but the system is still functioning, iLO displays the status Degraded.
  - If a NIC reports a failure, iLO displays the status Critical.
- 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.
  - In configurations with multiple NICs, if a component has failed but the system is still functioning, iLO displays the status Degraded.
  - If a NIC reports a failure, iLO displays the status Critical.

- 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

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

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.

Procedure

Navigate to the Information > System Information page, and then click the Device Inventory tab.

Device Inventory details

- 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

Procedure

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 slot tooltip 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

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.

Procedure

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.

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

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 controllers, enclosures, logical drives, and physical drives.

iLO can monitor 71 physical drives on a controller, 256 physical drives total, and 256 logical drives total.

Controllers

This section provides the following details for each Smart Array controller.

- Controller location—Slot number or system board
- Top-level controller status (displayed to the left of the controller location)—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

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 the listed properties, and some storage configurations do not have drive enclosures.

Logical Drives

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

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

Controllers

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 to 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

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 installed firmware information

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.

Procedure

Navigate to the Information > System Information page, and then click the Firmware tab.

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
- Smart Storage Battery
- TPM or TM firmware
- SAS Programmable Logic Device
- System Programmable Logic Device
- 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

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

Prerequisites

To display a complete set of data on this page, AMS must be installed.

Procedure

1. Navigate to the Information > System Information page, and then click the Software tab.
2. Select one of the following:
   - HPE Software—Lists all 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 the software that is running or available to run on the managed server.
   - Installed Software—Lists all 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.

HPE Software List details

- 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 firmware flash components saved on the local operating system. The displayed version might not match the firmware running on the server.

Running Software details

This section lists all the software that is running or available to run on the managed server.

- 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

The Installed Software list displays the name of each installed software program.

Using the iLO logs

iLO Event Log

The event log provides a record of significant events recorded by the iLO firmware.

Examples of the logged events include server events such as a server power outage or a server reset. Other logged events include logins, virtual power events, clearing the log, and some configuration changes.

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.

When the event log is full, each new event overwrites the oldest event in the log.

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

Procedure

1. Navigate to the Information > iLO Event Log page.
2. Optional: Use the event log sort, search, and filter features to customize the log view.

Event log view controls

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.
- To set the filters back to the default values, click Reset filters.
- Click a column heading to sort the event log table by that column.

  To change the display to ascending or descending order, click the triangle next to the column heading.

Event log details

- 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.

Event log icons

- 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.

Saving the event log to a CSV file

Use a supported browser to export the event log to a CSV file.

Procedure

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. To close the window, click Close.

Clearing the event log

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Information > iLO Event Log page.
2. Click Clear Event Log.

   iLO prompts you to confirm the request.
3. Click OK.

   The event log is cleared of all previously logged information and an event is recorded in the log.

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 you troubleshoot remote host server issues.

When the IML is full, each new event overwrites the oldest event in the log.

Some examples of the information types recorded in the IML include:

- Fan and power supply status changes
- Temperature changes
- Automatic shutdown activities
- Drive failures

Viewing the IML

Procedure

1. Navigate to the Information > Integrated Management Log page.
2. Optional: Use the IML sort, search, and filter features to customize the log view.

IML view controls

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.
- To set the filters back to the default values, click Reset filters.
- Click a column heading to sort the IML table by that column.

  To change the display to ascending or descending order, click the triangle next to the column heading.

IML details

- The first column on the left side of the web interface displays an active check box next to each event with Critical or Caution status. Use this check box to select an event to mark as repaired.
- 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.

IML icons

- 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.

Marking an IML entry as repaired

Use this feature to change the status of an IML entry from Critical or Caution to Repaired.

Prerequisites

Configure iLO Settings privilege

Procedure

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.
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 maintenance notes to create log entries about maintenance activities such as upgrades, system backups, periodic system maintenance, or software installations.

Prerequisites

Configure iLO Settings privilege

Procedure

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.

Procedure

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. To close the window, click Close.

Clearing the IML

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Information > Integrated Management Log page.
2. Click Clear IML.
3. When prompted to confirm the request, click OK.

   The IML is cleared of all previously logged information and an event is recorded in the log.

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.

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 OS data from third-party error event log activities (for example, content created or passed through the OS).

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. Host resources are not consumed in the collection and logging of Active Health System 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 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 the data used 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**.

You can upload the log to #VENDABR# InfoSight to view the log data or create a support case for servers under a valid warranty or support contract. For more information, see the #VENDABR# InfoSight documentation at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

The Active Health System Log is not supported on servers without a NAND.

Active Health System Log download methods

You can use the following methods to download the Active Health System Log:

- **iLO web interface**—Download the log for a range of days or download the entire log from the Active Health System Log page.
- **cURL utility**—Download the log by using the cURL command-line tool.
- **iLO RESTful API and RESTful Interface Tool**—For more information, see **https://www.hpe.com/support/restfulinterface/docs**.

Downloading the Active Health System Log for a date range

Procedure

1. Navigate to the Information > Active Health System Log page.

   The Active Health System Log is inaccessible when it is being downloaded by Intelligent Provisioning, the RESTful Interface Tool, or any other method.

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 (up to 14 characters)
   - Contact name
   - Phone number (up to 39 characters)
   - Email 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 **gsd_csc_case_mngmt@hpe.com**.

   Use the following convention for the email subject: CASE: <case number>.

   Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.

7. Optional: Upload the file to the Active Health System Viewer.

   For more information, see **http://www.hpe.com/servers/ahsv**.

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.

Procedure

1. Navigate to the Information > Active Health System Log page.

   The Active Health System Log is inaccessible when it is being downloaded by Intelligent Provisioning, the RESTful Interface Tool, or any other method.

2. Click Show Advanced Settings.
3. Optional: Enter the following information to include in the downloaded file:

   - Support case number (up to 14 characters)
   - Contact name
   - Phone number (up to 39 characters)
   - Email 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 **gsd_csc_case_mngmt@hpe.com**.

   Use the following convention for the email subject: CASE: <case number>.

   Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.

7. Optional: Upload the file to the Active Health System Viewer.

   For more information, see **http://www.hpe.com/servers/ahsv**.

Downloading 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.

Procedure

1. Install cURL.
2. You can download cURL from the following website: **http://curl.haxx.se/**.
3. Open a command window.
4. Change to the `curl` directory.
5. Enter a command similar to the following examples.

   IMPORTANT:

   When you enter these commands, ensure that you do not use spaces or other unsupported characters.

   If required by your command-line environment, special characters such as the ampersand must be preceded by the escape character. See the command-line environment documentation for more information.

   - To download the Active Health System Log for a range of dates:

     ```
     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 Active Health System Log for the last seven days, and add a Hewlett Packard Enterprise support case number to the log header:

     ```
     curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
     &case_no=<number>" -k -v -u <username>:<password> -o <filename>.ahs
     ```

   - To download the Active Health System Log for the last seven days, and include a case number and contact information:

     ```
     curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?days=<number_of_days>
     &case_no=<number>&contact_name=<name>&phone=<phone_number>&email=
     <email_address>&co_name=<company>" -k -v -u <username>:<password>
     -o <filename>.ahs
     ```

   - To download the entire Active Health System Log:

     ```
     curl "https://<iLO_IP_address>/ahsdata/ahs.ahs?downloadAll=1" -k -v
     -u <username>:<password> -o <filename>.ahs
     ```

6. The file is saved to the specified path.
7. Close the command window.
8. (Optional) If you have an open support case, email the log file to **gsd_csc_case_mngmt@hpe.com**.

   Use the following convention for the email subject: CASE: <case number>.

   Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.
9. (Optional) Upload the file to the Active Health System Viewer.

   For more information, see **http://www.hpe.com/servers/ahsv**.

cURL command usage with iLO

When you use cURL to extract the Active Health System log, the command components include the following:

Options

`<iLO IP address>`

Specifies 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, 2017-07-29 for July 29, 2017.

`days=<number of days>`

Specifies that you want to download the log file for the last `<number of days>` from today's date.

`downloadAll=1`

Specifies that you want to download the entire log.

`-k`

Specifies that HTTPS warnings will be ignored, which could make the connection insecure.

`-v`

Specifies verbose output.

`-u <username>:<password>`

Specifies your iLO user account credentials.

`-o <filename>.ahs`

Specifies the output file name and path.

`case_no=<HPE support case number>`

Specifies a Hewlett Packard Enterprise support case number to add to the log header.

Options for adding contact information to the downloaded log

`phone=<phone number>`

Specifies a phone number to add to the log header.

`email=<email address>`

Specifies an email address to add to the log header.

`contact_name=<contact name>`

Specifies a contact name to add to the log header.

`co_name=<company name>`

Insert your company name in the log header.

Downloading the Active Health System log (iLOREST)

Prerequisites

- The RESTful Interface Tool is installed.
- Configure iLO Settings privilege

Procedure

1. Start the RESTful Interface Tool.
2. Enter
   ```
   ilorest
   ```
   .
3. Log in to an iLO system:

   ```
   iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
   ```
4. Download the Active Health System log for the server you logged into in step 3.
   - To download the log for the last seven days, enter a command similar to the following:

     ```
     iLOrest > serverlogs --selectlog=AHS --directorypath=directory path
     ```
   - To download the log for a specified time period, enter a command similar to the following:

     ```
     iLOrest > serverlogs --selectlog=AHS --directorypath=directory path
     --customiseAHS="from=YYYY-MM-DD&&to=YYYY-MM-DD"
     ```
   - To download the entire Active Health System log, enter a command similar to the following:

     ```
     iLOrest > serverlogs --selectlog=AHS --downloadallahs --directorypath=directory path
     ```

   The log is downloaded with the following file name: `HPE_server serial number_YYYYMMDD.ahs`.
5. (Optional) If you have an open support case, email the log file to **gsd_csc_case_mngmt@hpe.com**.

   Use the following convention for the email subject: CASE: <case number>.

   Files that are larger than 25 MB must be compressed and uploaded to an FTP site. If needed, contact Hewlett Packard Enterprise for FTP site information.
6. (Optional) Upload the file to the Active Health System Viewer.

   For more information, see **http://www.hpe.com/servers/ahsv**.

iLOREST serverlog command usage

`--selectlog=AHS`

Specifies that you want to work with the Active Health System log type.

`--directorypath=`*`directory path`*

Specifies the output file path.

`--customiseAHS="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, 2017-07-29 for July 29, 2017.

`--downloadallahs`

Specifies that you want to download the entire log.

For more information, see the **RESTful Interface Tool documentation**.

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

Procedure

1. Navigate to the Information > Active Health System Log page.

   The Active Health System Log is inaccessible when it is being downloaded by Intelligent Provisioning, the RESTful Interface Tool, or any other method.

2. Click Show Advanced Settings.
3. Scroll to the Clear Log section, and then click Clear.
4. When prompted to confirm the request, click OK.

   iLO notifies you that the log is being cleared.

5. Reset iLO.

   Resetting iLO 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 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.

Using the iLO diagnostics, reboot, and reset features

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.

Procedure

Navigate to the Information > Diagnostics page.

Self-test details

- The iLO health status, which is based on the combined results of the iLO diagnostic self-tests, is listed at the top of the iLO Self-Test Results section.
- 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 counter

    The 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.

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

Virtual Power and Reset privilege

Procedure

1. Navigate to the Information > Diagnostics page.
2. Click Generate NMI to System.

   iLO warns you that generating an NMI to the system might cause data loss.
3. Click OK to confirm, or click Cancel.

   If you clicked OK, iLO confirms that the NMI was sent.

Formatting the Embedded Flash

The Embedded Flash (also called the NAND) is a partition of nonvolatile flash memory that is embedded on the system board of supported HPE servers.

Prerequisites

- Configure iLO Settings privilege
- An experienced support organization recommended that you format the Embedded Flash.
- The iLO health status is Degraded.

Procedure

1. Navigate to the Information > Diagnostics page.
2. Click the iLO health link.

   iLO warns you that this process erases all data on the Embedded Flash. External providers such as Intelligent Provisioning and the BIOS must be reconfigured after you format the Embedded Flash.
3. Click Format Embedded Flash and reset iLO.

   iLO prompts you to confirm the request.
4. Click OK.

   iLO formats the Embedded Flash, and then initiates an iLO reset.

Configuring redundant ROM

Prerequisites

- Virtual Power and Reset privilege
- The server supports redundant ROM.

Procedure

1. Navigate to the Information > Diagnostics page.

   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.

   iLO prompts you to confirm the request.

3. Click OK.

   The change will take effect after the next system reboot.

iLO reboot (reset)

In some cases, it might be necessary to reboot iLO; for example, if iLO is not responding to the browser.

The Reset option initiates an iLO reboot. It 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.

If none of the available reset methods are available or working as expected, power down the server and disconnect the power supplies.

iLO reboot (reset) methods

iLO web interface

Use the Reset button on the Diagnostics page.

iLO 4 Configuration Utility

Use the iLO 4 Configuration Utility in the UEFI System Utilities.

iLO RESTful API

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

Command line and scripting tools

For more information, see the HPE iLO 4 Scripting and Command Line Guide.

Insight Management Agents (5.40 and later)

Use the Reset iLO option on the Management Agent page in the iLO section.

IPMI

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

Server UID

Use the server UID button on supported servers to initiate a graceful reboot or a hardware reboot.

This method can be used if none of the other reset methods are available or working as expected.

Rebooting (resetting) iLO with the web interface

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Information > Diagnostics page.
2. Click Reset.

   iLO prompts you to confirm the request.
3. Click OK.

   iLO resets and closes your browser connection.

Rebooting (resetting) iLO with the iLO 4 Configuration Utility

Prerequisites

Configure iLO Settings privilege

Procedure

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.

   iLO prompts you to confirm the request.
6. Press Enter.

   iLO resets and all active connections are ended. If you are managing iLO remotely, the remote console session ends automatically.

   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.

Performing a graceful iLO reboot with the server UID button

The UID button on supported servers can be used to initiate a graceful iLO reboot.

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.

Procedure

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

The UID button on supported servers can be used to initiate an iLO hardware reboot.

When you initiate a hardware iLO reboot, the server hardware initiates the iLO reboot.

Procedure

To initiate a hardware iLO reboot, press and hold the UID button for 10 seconds or longer.

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 iLO network failed flash recovery feature. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

Do not initiate a hardware reboot if other troubleshooting options are available.

The UID button/LED flashes blue 8 Hz/cycle per second to indicate that an iLO hardware reboot is in progress.

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.

Resetting iLO to the factory default settings (iLO RBSU)

CAUTION:

This operation clears all user and license data.

Procedure

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.

   iLO prompts you to confirm the request.
5. Press F10 to continue.

   iLO RBSU notifies you that iLO will be reset to the factory defaults, and will reboot. The iLO RBSU utility closes.
6. Press Enter.

   iLO resets and the server boot process finishes.

   NOTE:

   If a server has an installed iLO Advanced license when you perform a factory reset, 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.
7. Optional: Log in to iLO.

   Use the default iLO account information to log in to iLO after a factory reset.

Resetting iLO to the factory default settings (iLO 4 Configuration Utility)

CAUTION:

This operation clears all user and license data.

Procedure

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.

   The iLO 4 Configuration Utility prompts you to confirm the request.
6. Press Enter.

   iLO resets to the factory default settings. If you are managing iLO remotely, the Remote Console session ends automatically. 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 factory reset to finish. Log in to iLO, and then start the iLO Remote Console.

      Use the default iLO account information to log in to iLO after a factory reset.

      The iLO 4 Configuration Utility screen remains 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.

NOTE:

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.

Using the iLO Federation features

iLO Federation

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-docs**.

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 the servers in the selected group.
- The changes you make on iLO Federation pages apply to all 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 the servers in the selected group that meet the filter criteria.
- The changes you make on iLO Federation pages apply to all 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.
- You can remove a filter by clicking the X icon or the filter name.

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

The following iLO Federation pages allow you to export information to a CSV file:

- Multi-System View—Export the Systems with critical or degraded status list.
- Multi-System Map—Export the iLO peers list.
- Group Virtual Media—Export the Affected Systems list.
- Group Power—Export the Affected Systems list.
- Group Firmware Update—Export the Affected Systems list.
- Group Licensing—Export the Affected Systems list.
- Group Configuration—Export the Affected Systems list.

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Navigate to a page 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.

   If multiple pages of servers are included in the list, the CSV file contains 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 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

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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.

Viewing servers with critical and degraded status

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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

- 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.

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 you navigate to one of the iLO Federation pages, 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 the data for the selected group is retrieved.

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Navigate to the iLO Federation > Multi-System Map page.
2. Select a group from the Selected Group menu.

iLO peer details

- #—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.

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

- Virtual Media privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Procedure

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 systems in the selected group.
3. Enter the disk image URL in the Scripted Media URL box in the Connect Virtual Floppy section (IMG files) or the Connect CD/DVD-ROM section (ISO files).
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 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 image remains connected until it is manually ejected. The servers boot to the image on all subsequent server resets, if the system boot options are configured accordingly.

   If a server in the group is in POST when you enable the Boot on Next Reset check box, an error occurs. You cannot modify the server boot order during POST. Wait for POST to finish, and then try again.

   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.
5. Click Insert Media.

   iLO displays the command results.

Viewing scripted media status for groups

Procedure

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/USB Key/Virtual Folder Status or Virtual CD/DVD-ROM Status section:

- Media Inserted—The Virtual Media type that is connected. Scripted Media is displayed when URL-based media is connected.
- Connected—Indicates whether a Virtual Media device is connected.
- Image URL—The URL that points to the connected media.

The Virtual Floppy/USB Key/Virtual Folder Status and Virtual CD/DVD-ROM Status sections are displayed only when media is connected.

Ejecting a scripted media device

Prerequisites

- Virtual Media privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.

Procedure

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 the systems in the selected group.
3. Click Eject Media in the Virtual Floppy/USB Key/Virtual Folder 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 Prev (if available) to view more servers in the list.

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

- Virtual Power and Reset privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Each member of the selected iLO Federation group has granted the Virtual Power and Reset privilege to the group.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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.

   iLO prompts you to confirm the request.
4. 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.

Power state options for groups

- 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 a group power state change

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 Prev (if available) to view more servers in the list.

Configuring group power capping

Prerequisites

- Configure iLO Settings privilege
- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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 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 lower than the server minimum power value.
5. 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.
6. Click Apply.

Group power capping considerations

The group power capping 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 idle servers.
- 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 HPE 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 also the Maximum Power Cap threshold. It is the highest power cap that can be set.
  - Peak Observed Power—The maximum observed power for all servers in a group. This value is also the Minimum High-Performance Cap threshold. It is the lowest power cap value that can be set without affecting the performance of the servers in a group.
  - Minimum Observed Power—The minimum observed power for all servers in a group. This value is also the Minimum Power Cap threshold. 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 all servers. For more information, check the server specifications.
- For some servers, power capping settings must be managed outside of the iLO web interface. You can use tools such as:
  - HPE ProLiant Power Interface Control Utility
  - HPE Advanced Power Manager

  See the server specifications at **http://www.hpe.com/info/qs** for information about the power management features your server supports.

Viewing group power capping information

Prerequisites

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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

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 group firmware update feature supports the following firmware types. You can update these firmware types only if your servers and environment support them:

- iLO firmware
- System ROM (BIOS)
- Chassis firmware (Power Management)
- Power Management Controller
- System Programmable Logic Device (CPLD)
- NVMe Backplane Firmware

Some firmware types are delivered as a combined update. For example:

- A SAS Programmable Logic Device update is often combined with a SAS controller firmware update.
- The Intelligent Platform Abstraction Data firmware is often combined with a System ROM/BIOS update.

Updating the firmware for multiple servers

Prerequisites

- Configure iLO Settings privilege
- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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 iLO firmware update on a server with a TPM or TM installed, iLO prompts you to suspend or back up software that stores information on the TPM or TM. For example, if you use drive encryption software, suspend it before initiating a firmware 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 Update Firmware.

   The URL to enter is similar to the following: `http://<server.example.com>/<subdir>/iLO 4_<yyy>.bin`, where `<yyy>` represents the firmware version.

   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 or 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.

Viewing group firmware information

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Navigate to the iLO Federation > Group Firmware Update page.
2. Select a group from the Selected Group menu.
3. (Optional) To filter the list of displayed systems, click a firmware version, flash status, or TPM or TM Option ROM Measuring status link.

Firmware details

The Firmware Information section displays the following information:

- The number of servers with each supported iLO 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 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 status is also displayed.
- The number of servers with each system ROM version. The percentage of the total number of servers with the listed system ROM version is also displayed.

Servers affected by a group firmware update

The Affected Systems list provides the following details about the servers affected by a group 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 Prev (if available) to view more servers in the list.

Installing license keys (iLO Federation group)

The Group Licensing page displays the license status for members of a selected iLO Federation group. Use the following procedure to enter a key to activate iLO licensed features.

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 it cannot be removed or replaced.

Procedure

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 Prev (if available) to view more servers in the list.

Viewing iLO Federation group license information

Prerequisites

The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

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.

iLO Remote Console

The iLO Remote Console can be used to remotely access the graphical display, keyboard, and mouse of the host server. The Remote Console provides access to the remote file system and network drives.

With Remote Console access, you can observe POST messages as the server starts, and initiate ROM-based setup activities to configure the server hardware. When you install operating systems remotely, the Remote Console (if licensed) enables you to view and control the host server monitor throughout the installation process.

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.

Access options

You can access the following Remote Console options from the iLO web interface:

- **HTML5 Integrated Remote Console**—For clients with a supported browser.
- **.NET Integrated Remote Console**—For Windows clients with a supported version of the Windows .NET Framework. This console is not supported by Google Chrome or Mozilla Firefox because these browsers do not support a ClickOnce extension to launch .NET applications.
- **Java Integrated Remote Console (Web Start)**—For Windows or Linux clients with the Oracle JRE.
- **Java Integrated Remote Console (Applet)**—For Windows or Linux clients with the Java plug-in.

The following Remote Console options are available from outside of the iLO web interface:

- **Standalone Remote Console (HPLOCONS)**—Provides iLO Remote Console access directly from your Windows desktop, without going through the iLO web interface.

  HPLOCONS has the same functionality and requirements as the .NET IRC. Download HPLOCONS from the following website: **http://www.hpe.com/support/ilo4**.

- **iLO Mobile Application for iOS and Android devices**—Provides Remote Console access from your supported mobile phone or tablet.

  For information about the mobile app features and how to use them, see the mobile app documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

General usage information and tips

- The Integrated Remote Console is suitable for high-latency (modem) connections.
- Do not run the iLO Integrated Remote Console from the host operating system 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.
- When you finish using the Integrated Remote Console, close the window or click the browser Close button (X) to exit.
- The UID LED flashes when an Integrated Remote Console session is active.
- 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.
- When the mouse is positioned over the Integrated Remote Console window, the console captures all keystrokes, regardless of whether the console window has focus.

Starting the integrated remote console

Starting the HTML5 IRC

Use this procedure to access the remote console in a supported browser.

Prerequisites

- Remote Console privilege
- For Microsoft Internet Explorer only: You connected to the iLO web interface by using a hostname or an IPv4 address.

  The HTML5 IRC is not supported with Microsoft Internet Explorer over an IPv6 connection. The Microsoft WebSocket implementation requires a nonstandard IPv6 literal address.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click the HTML5 Console button.

   The HTML5 IRC starts.
3. Use the remote console features.

Starting the HTML5 IRC from the Overview page

Use this procedure to access the remote console in a supported browser.

Prerequisites

- Remote Console privilege
- For Microsoft Internet Explorer only: You connected to the iLO web interface by using a hostname or an IPv4 address.

  The HTML5 IRC is not supported with Microsoft Internet Explorer over an IPv6 connection. The Microsoft WebSocket implementation requires a nonstandard IPv6 literal address.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Information > Overview page.
2. Click the HTML5 link.

   The HTML5 IRC starts.
3. Use the remote console features.

HTML5 remote console modes

The HTML5 remote console has several available viewing modes. When you use the console, you can switch from one viewing mode to another supported mode.

Windowed mode

The remote console is displayed in a secondary window in the same browser window as the iLO web interface. You cannot move the console out of the browser window.

You can switch from this mode to docked mode or full screen mode.

Docked mode

The remote console is displayed in a small Remote Console window below the navigation tree.

You can switch from this mode to windowed mode or full screen mode.

Full screen mode

The remote console is displayed at the full size of your monitor. To view the remote console menu, move the cursor to the top of the screen. The default position of the menu is the top left. Click and drag to move the menu to a different position. If you change the menu position, the change persists for the current remote console session.

This mode is available in all console modes.

HTML5 remote console controls

The following controls are available at the top of the remote console window (from left to right). A tooltip description is provided when you move the cursor over a control icon.

Menu

This icon enables you to do the following:

- Access the iLO Virtual Power button feature.
- Use the Preferences menu to show or hide the Remote Console status bar.

Virtual Keyboard

This icon enables you to do the following:

- Access the following keyboard shortcut that you can send to the remote server: CTRL+ALT+DEL.
- Access the following remote console virtual keys:
  - CTRL—Control
  - ESC—Escape
  - CAPS—CapsLock
  - NUM—NumLock
  - L OS—Left OS-specific key
  - L ALT—Left ALT key
  - R ALT—Right ALT key
  - R OS—Right OS-specific key
- View or change the HTML5 remote console keyboard layout.

Virtual Media

This icon provides access to the virtual media feature.

Close Remote Console

This icon disconnects the remote console session.

Remote console display and mode controls

Use the following controls to change the display of the remote console or to switch to a different viewing mode.

The available controls vary, depending on the active console mode. If a control is not supported in the active console mode, then it is not displayed.

Maximize and Restore

The Maximize icon maximizes the remote console window within the browser window.

The Restore icon resets the window to its previous size.

These features are available in windowed mode.

Switch to full screen

This feature is available in all modes.

Docked mode

This icon enables you to change from windowed mode to docked mode.

This feature is available in windowed mode.

Exit full screen

This icon enables you to exit full screen mode and return to the previously selected mode.

You can also press Esc to exit full screen mode.

Windowed mode

This icon enables you to change from docked mode to a secondary window.

This feature is available in docked mode.

Pin icon

This icon enables you to pin or unpin the toolbar at the top of the screen. This setting persists for the current remote console session.

This feature is available in full screen mode.

Starting the .NET IRC

Use this procedure to access the remote console in a supported browser on a Windows client.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- A supported version of the Microsoft .NET Framework is installed.
- Your browser supports using ClickOnce to start a .NET application.

  For information about using the .NET IRC with Microsoft Edge, see the user guide.
- Pop-up blockers are disabled.

  In some cases, you can bypass the pop-up blocker by Ctrl+clicking the .NET Console button.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click the Launch button.

   The remote console starts in a separate window.
3. Use the remote console features.

Starting the .NET IRC from the Overview page

Use this procedure to access the remote console in a supported browser on a Windows client.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- A supported version of the Microsoft .NET Framework is installed.
- Your browser supports using ClickOnce to start a .NET application.
- Pop-up blockers are disabled.

  In some cases, you can bypass the pop-up blocker by Ctrl+clicking the .NET Console button.

Procedure

1. Navigate to the Information > Overview page.
2. Click the .NET link.
3. Use the remote console features.

.NET IRC requirements

Microsoft .NET Framework

The .NET IRC requires version 4.5.1 or later of the .NET Framework.

For Windows 7, 8, 8.1, and 10, a supported version of the .NET Framework is included in the operating system. The .NET Framework is also available at the Microsoft Download Center: **http://www.microsoft.com/download**.

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...
```

Google Chrome and Mozilla Firefox do not support the .NET IRC because they do not support a ClickOnce extension to launch .NET applications. As a workaround, choose a different Remote Console, or use a different browser.

Starting the Java IRC (Oracle JRE)

Use this procedure to start the Java IRC in environments with Windows or Linux and the Oracle JRE. The version of the Java IRC that supports the Oracle JRE is a Java Web Start application.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Your environment supports Java Web Start and the latest version of Java 8 is installed.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click the Web Start button.

   The browser prompts you to save and open the Hewlett Packard Enterprise JNLP file.
3. To save and open the JNLP file, follow the browser instructions.
4. If a Security Warning dialog box is displayed, click Continue.

   If you do not click Continue, the Java IRC will not start.
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.

   The Java Web Start application opens 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.
6. Use the remote console features.

Starting the Java IRC (Oracle JRE) from the Overview page

Use this procedure to start the Java IRC in environments with Windows or Linux and the Oracle JRE. The version of the Java IRC that supports the Oracle JRE is a Java Web Start application.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Your environment supports Java Web Start and the latest version of Java 8 is installed.

Procedure

1. Navigate to the Information > Overview page.
2. Click the Java Web Start link.

   The browser prompts you to save and open the Hewlett Packard Enterprise JNLP file.
3. To save and open the JNLP file, follow the browser instructions.
4. If a Security Warning dialog box is displayed, click Continue.

   If you do not click Continue, the Java IRC will not start.
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.

   The Java Web Start application opens 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.
6. Use the remote console features.

Starting the Java IRC (OpenJDK JRE)

Use this procedure to start the Java IRC in environments with Linux and the OpenJDK JRE. The version of the Java IRC that supports the OpenJDK JRE is a Java applet.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The OpenJDK JRE is installed.
- Pop-up blockers are disabled.

  In some cases, you can bypass the pop-up blocker by Ctrl+clicking the remote console launch button.
- The Java plug-in is installed in the client browser.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click the Applet button.
3. If a Security Warning dialog box or a confirmation dialog box appears, follow the onscreen instructions to continue.
4. 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.

   The Java applet opens in a separate window.
5. Use the remote console features.

Acquiring the remote console

If another user is working in the remote console, you can acquire it from that user.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click the button for the remote console you want to use.

   iLO notifies you that another user is working in the remote console.
3. To send a request to acquire the remote console, follow the onscreen instructions.

   The other user is prompted to approve or deny the request.

   If the other user approves, or they do not respond in 10 seconds, permission is granted. The remote console starts.

Joining a Shared Remote Console session (.NET IRC only)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Click Launch in the .NET Integrated Remote Console (.NET IRC) section.

   A message notifies you that the .NET IRC is 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 keyboard and mouse access.

Shared remote console (.NET IRC only)

The shared remote console feature allows multiple users to connect to the same remote console session. 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. The request includes the requester user name and DNS name or IP address. The session leader is prompted to grant or deny access. If there is no response, permission is denied.

Passing the session leader designation to another user is not supported.

If a connection failure occurs, reconnecting is not supported. A remote console session must be restarted to allow user access after a connection failure.

During a shared remote console session, the session leader has access to all remote console features. Other users can access only the keyboard and mouse.

iLO encrypts shared remote console sessions by authenticating the client first, and then the session leader determines whether to allow new connections.

Viewing the remote console status bar

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start a remote console.

   The remote console window opens with the status bar displayed.
3. (Optional) To turn the status bar on or off, click the Menu icon ☰, and then select Preferences > Show status bar.

   Only the HTML5 IRC supports this feature.

Remote console status bar details

Resolution

The remote console window resolution.

POST codes

During POST, POST codes are displayed in the center of the status bar.

Console Capture (.NET IRC only)

These controls enable you to record and play back activities displayed in the console window.

Screen Capture

You can click the camera icon in the HTML5 IRC to create a screen capture of the activity displayed in the console window.

You can double-click the status bar in the .NET IRC to capture the screen, and then paste the screen capture into an image editor.

Encryption

The status and encryption type of the connection between the remote console and iLO.

Health status

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. The possible values are OK, Degraded, and Critical.

Activity LED

The activity indicator for local virtual media devices connected through the remote console. This feature is not active for URL-based virtual media devices.

Power status

The server power state (ON or OFF).

Integrated remote console features

The integrated remote console (IRC) supports the following features:

- Keyboard actions with the IRC
- Virtual power IRC features
- Virtual media IRC features
- Console capture (.NET IRC)
- Screen captures with the IRC

Keyboard actions with the IRC

Sending a keyboard action with the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the HTML5 IRC.
3. Do one of the following:
   - Use your client keyboard to press the desired keys.
   - To send the Ctrl+Alt+Del action, click the Virtual Keyboard icon , and then click the CTRL+ALT+DEL keyboard shortcut.
   - To enable or disable the Caps Lock or Num Lock setting, do one of the following:
     - Press the NumLock or CapsLock key on your client keyboard.
     - Click the Virtual Keyboard icon , and then click the CAPS or NUM keyboard shortcut.

Sending a keyboard action with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start a remote console.
3. Do one of the following:
   - Use your client keyboard to press the desired keys.
   - To send the Ctrl+Alt+Del action, select Keyboard > CTRL-ALT-DEL.
   - To enable or disable the Caps Lock or Num Lock setting, do one of the following:
     - Press the NumLock or CapsLock key on your client keyboard.
     - Select Keyboard > Caps Lock or Keyboard > Num Lock.

Sending a remote console hot key

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Remote console hot keys are configured on the Hot Keys page.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start a remote console.
3. On your client keyboard, press the key combination for a configured remote console hot key.

Changing the keyboard layout in the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The server OS is configured to support the keyboard layout you want to use.
- The client you used to browse to iLO is configured to support the keyboard layout you want to use.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the HTML5 IRC.
3. Click the Virtual Keyboard icon .
4. Select Keyboard Layout > *Keyboard layout name*.

   iLO supports the following keyboard layouts: EN 101 and JP 106/109.

   This setting is saved in a cookie and remains persistent when you use the remote console with the same browser.

Virtual power IRC features

Using the remote console virtual power switch with the HTML5 IRC

Prerequisites

- Remote Console privilege
- Virtual Power and Reset privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the HTML5 IRC.
3. Click the Menu icon , and then select an option from the Power menu.

   The Press and Hold, Reset, and Cold Boot options are not available when the server is powered off.

   iLO prompts you to confirm the request.
4. Click OK.

Using the remote console virtual power switch with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege

- Virtual Power and Reset privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC or Java IRC.
3. Select an option from the remote console Power Switch menu.

   The Press and Hold, Reset, and Cold Boot options are not available when the server is powered off.

   iLO prompts you to confirm the request.
4. 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 8 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Virtual media IRC features

The integrated remote console (IRC) allows you to perform the following tasks:

- Connect and disconnect virtual drives including:
  - Physical drives on a client PC (floppy disk, CD/DVD-ROM, USB key)
  - Local IMG or ISO files
  - URL-based media (IMG or ISO)
  - Virtual folders

  To verify that the console you want to use supports a virtual media type, check the instructions for using that media type.
- Create media images (Java IRC only)

Using a virtual drive (physical drive on a client PC)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- If you are using the remote console with Windows, you have Windows administrator rights, which are required for mounting a physical drive.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start a remote console that supports this feature.

   In this release, the .NET IRC and Java IRC support this feature.
3. Click the Virtual Drives menu, and then select the drive letter of a floppy disk, CD-ROM/DVD, or USB key drive on your client PC.

   The virtual drive activity LED will show virtual drive activity.

Using a local IMG or ISO file with the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the HTML5 IRC.
3. Click the Virtual Media icon, and then select Floppy > Local *.img file or CD/DVD > Local *.iso file.

   The remote console prompts you to select a file.
4. Enter the path or file name of the image file in the File name text box.

   You can also browse to the file location, and then click Open.

   The virtual drive activity LED will show virtual drive activity.

Using a local IMG or ISO file with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC or Java IRC.
3. Click the Virtual Drives menu, and then select Image File Removable Media (IMG) or Image File CD-ROM/DVD (ISO).

   The IRC prompts you to select a file.
4. Enter the path or file name of the image file in the File name text box.

   You can also browse to the file location, and then click Open.

   The virtual drive activity LED will show virtual drive activity.

Using a virtual drive to install an OS and provide a required driver (.NET IRC or Java IRC)

You can use the remote console virtual drive feature to install an operating system. During the installation, you might be prompted to provide access to a required driver, such as a storage controller driver.

Prerequisites

- Remote Console privilege
- The operating system ISO file is available on the client you will use to run the remote console.
- If you will install an operating system on an NVMe drive, the Boot Mode is set to Unified Extensible Firmware Interface (UEFI).

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Download and extract the required driver.

   You can obtain drivers from the SPP or download them from the following website: **http://www.hpe.com/support/hpesc**.
2. Copy the driver to a USB key or a folder on the client where you will access the remote console.
3. Start the remote console.
   - If you will use a USB key to provide the required driver, choose the .NET IRC or Java IRC.
   - If you will use a virtual folder to provide the required driver, choose the .NET IRC.
4. Mount the operating system ISO.
   a. Select Virtual Drives > Image File CD-ROM/DVD.

      The remote console prompts you to select a file.

   b. Enter the path or file name of the image file in the File name text box.

      You can also browse to the file location, and then click Open.
5. If you will provide the required driver on a USB key, do the following:
   a. Connect the USB key to the client you are using to manage iLO.
   b. In the remote console, click the Virtual Drives menu, and then select the drive letter of the USB key on your client PC.
6. If you will provide the required driver in a folder on the client you use to manage iLO, do the following:
   a. Select Virtual Drives > Folder.
   b. In the Browse for Folder window, select the folder that contains the driver file.
7. Boot to the operating system ISO.
8. Follow the onscreen instructions until the operating system installer prompts you for the path to the driver.
9. When prompted for the driver location, enter the path to the USB key or virtual folder that contains the driver.
10. Follow the onscreen instructions to complete the operating system installation.
11. Install any additional required device drivers.

    You can obtain device drivers from the SPP.

Using a URL-based image file with the HTML5 IRC

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The image file you want to use is on a web server on the same network as iLO.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the HTML5 IRC.
3. Click the Virtual Media icon and select Floppy > Scripted Media URL for an IMG file, or select CD/DVD > Scripted Media URL for an ISO file.

   iLO prompts you to enter an image file URL.
4. Enter the URL for the image file that you want to mount as a virtual drive, and then click Apply.

The virtual drive activity LED does not show drive activity for URL-mounted virtual media.

Using a URL-based image file with the .NET IRC or Java IRC

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The image file you want to use is on a web server on the same network as iLO.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC or Java IRC.
3. Select Virtual Drives > URL Removable Media for an IMG file or Virtual Drives > URL CD-ROM/DVD for an ISO file.

   iLO prompts you to enter an image file URL.
4. 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 a virtual folder (.NET IRC only)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC.
3. Select Virtual Drives > Folder.
4. 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. You can browse to the server and transfer the files from the virtual image to the server.

A virtual folder is nonbootable and read-only; the mounted folder is static. Changes to the client folder are not replicated in the mounted folder. To update your view of a virtual folder after changing the client folder, simply disconnect and then reconnect the virtual folder.

Create Media Image feature (Java IRC only)

When you use virtual media, performance is fastest when you use image files 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 (Java IRC)

The Create Media Image feature enables you to create disk image files from data in a file or on a physical disk. You can create an ISO-9660 disk image file (IMG or ISO).

Prerequisites

- Remote Console privilege

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the Java IRC.
3. Select Virtual Drives > Create Disk Image.

   The Create Media Image dialog box opens.
4. Verify that the Disk>>Image button is displayed. If the button label is Image>>Disk, click the button to change it to Disk>>Image.
5. Do one of the following:
   - If you will use a file, select Media File, and then click Browse and navigate to the file you want to use.
   - If you will use physical media, select Media Drive, and then select the drive letter of the floppy disk, USB key, or CD in the Media Drive menu.
6. Enter the path and file name for the image file in the Image File text box.
7. Click Create.

   iLO notifies you when the image creation is complete.
8. Click Close.
9. Confirm that the image was created in the specified location.

Copying data from an image file to a physical disk (Java IRC)

The Create Media Image feature enables you to copy the data from a disk image file to a floppy disk or USB key. Only disk image (IMG) files are supported. Copying data to a CD is not supported.

You can copy disk image data to a floppy disk or USB key.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the Java IRC.
3. Select Virtual Drives > Create Disk Image.

   The Create Media Image dialog box opens.
4. In the Create Media Image window, click Disk>>Image.

   The Create Media Image changes to the Image>>Disk option.
5. Select the drive letter of the floppy disk or USB key in the Media Drive menu.
6. Enter the path and file name for the existing image file in the Image File text box.

   iLO notifies you when the operation is complete.
7. Click Close.
8. Confirm that the files were copied to the specified location.

Console capture (.NET IRC)

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.

- 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 information when server startup is detected. It stops when the file runs out of space. This file is overwritten each time the server starts.
- The server prefailure file starts capturing information when the server startup file is full. It 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 at the bottom of the .NET IRC session window.

Console capture controls

The following console capture controls are available, from left to right:

- Skip to Start—Restarts playback from the beginning of the file.
- Pause—Pauses 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

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC.
3. Press the Play button.

   The Play button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.

   The Playback Source dialog box opens.
4. Select Server Startup or Server Prefailure.
5. Click Start.

Saving server startup and server prefailure video files

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC.
3. Press the Play button.

   The Play button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.

4. Select Server Startup or Server Prefailure.
5. Click Start.
6. Press the Play button again to stop playback.

   iLO notifies you that the recording is no longer write-protected, and prompts you to save it.
7. Click Yes.
8. Select a save location, enter a file name, and then click Save.
9. (Optional) Play the video file.

Capturing video files with the remote console

Use this procedure to capture video files of sequences other than server startup and server prefailure.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC.
3. Click the Record button.

   The Record button has a red circle icon, and it is located in the toolbar at the bottom of the remote console window.

   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.
6. (Optional) Play the video file.

Viewing saved video files with the remote console

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the .NET IRC.
3. Press the Play button.

   The Play button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.

   The Playback Source dialog box opens.
4. Click the magnifying glass icon next to the From File box.
5. Navigate to a video file, and then click Open.

   Video files captured in the remote console use the iLO file type.
6. Click Start.

Screen captures with the IRC

Use the remote console screen capture feature when you want to save a screen capture of the server activity. For example, you might

want to capture a POST code displayed on the remote console screen.

When you use the IRC screen capture feature, the remote console status bar is not included in the captured image. If you want a screen capture that includes the status bar, use a different screen capture method.

Capturing the HTML5 remote console screen

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console** --> **Remote Console** page.
2. Start the HTML5 remote console.
3. Click the camera icon in the status bar.

   The screen capture opens in a new browser tab.
4. (Optional) Save the screen capture.

Capturing the .NET IRC screen

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console** --> **Remote Console** page.
2. Start the .NET IRC.
3. Double-click the status bar.

   A screen capture is saved in the clipboard.
4. (Optional) Paste the screen capture into an image editor.

Integrated remote console features

The integrated remote console (IRC) supports the following features:

- Keyboard actions with the IRC
- Virtual power IRC features
- Virtual media IRC features
- Console capture (.NET IRC)
- Screen captures with the IRC

Keyboard actions with the IRC

Sending a keyboard action with the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the HTML5 IRC.
3. Do one of the following:
   - Use your client keyboard to press the desired keys.
   - To send the **Ctrl+Alt+Del** action, click the **Virtual Keyboard** icon ⌨, and then click the **CTRL+ALT+DEL** keyboard shortcut.
   - To enable or disable the Caps Lock or Num Lock setting, do one of the following:
     - Press the **NumLock** or **CapsLock** key on your client keyboard.
     - Click the **Virtual Keyboard** icon ⌨, and then click the **CAPS** or **NUM** keyboard shortcut.

Sending a keyboard action with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start a remote console.
3. Do one of the following:
   - Use your client keyboard to press the desired keys.
   - To send the **Ctrl+Alt+Del** action, select **Keyboard > CTRL-ALT-DEL**.
   - To enable or disable the Caps Lock or Num Lock setting, do one of the following:
     - Press the **NumLock** or **CapsLock** key on your client keyboard.
     - Select **Keyboard > Caps Lock** or **Keyboard > Num Lock**.

Sending a remote console hot key

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- Remote console hot keys are configured on the **Hot Keys** page.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start a remote console.
3. On your client keyboard, press the key combination for a configured remote console hot key.

Changing the keyboard layout in the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The server OS is configured to support the keyboard layout you want to use.
- The client you used to browse to iLO is configured to support the keyboard layout you want to use.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the HTML5 IRC.
3. Click the **Virtual Keyboard** icon ⌨.
4. Select **Keyboard Layout >** ***Keyboard layout name***.

   iLO supports the following keyboard layouts: EN 101 and JP 106/109.

   This setting is saved in a cookie and remains persistent when you use the remote console with the same browser.

Virtual power IRC features

Using the remote console virtual power switch with the HTML5 IRC

Prerequisites

- Remote Console privilege
- Virtual Power and Reset privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the HTML5 IRC.
3. Click the **Menu** icon ☰, and then select an option from the **Power** menu.

   The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.

   iLO prompts you to confirm the request.
4. Click **OK**.

Using the remote console virtual power switch with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege
- Virtual Power and Reset privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC or Java IRC.
3. Select an option from the remote console **Power Switch** menu.

   The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered off.

   iLO prompts you to confirm the request.
4. 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 8 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Virtual media IRC features

The integrated remote console (IRC) allows you to perform the following tasks:

- Connect and disconnect virtual drives including:
  - Physical drives on a client PC (floppy disk, CD/DVD-ROM, USB key)
  - Local IMG or ISO files
  - URL-based media (IMG or ISO)
  - Virtual folders

  To verify that the console you want to use supports a virtual media type, check the instructions for using that media type.
- Create media images (Java IRC only)

Using a virtual drive (physical drive on a client PC)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they

support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

- If you are using the remote console with Windows, you have Windows administrator rights, which are required for mounting a physical drive.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start a remote console that supports this feature.

   In this release, the .NET IRC and Java IRC support this feature.
3. Click the **Virtual Drives** menu, and then select the drive letter of a floppy disk, CD-ROM/DVD, or USB key drive on your client PC.

   The virtual drive activity LED will show virtual drive activity.

Using a local IMG or ISO file with the HTML5 IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the HTML5 IRC.
3. Click the **Virtual Media** icon, and then select **Floppy > Local *.img file** or **CD/DVD > Local *.iso file**.

   The remote console prompts you to select a file.
4. Enter the path or file name of the image file in the **File name** text box.

   You can also browse to the file location, and then click **Open**.

   The virtual drive activity LED will show virtual drive activity.

Using a local IMG or ISO file with the .NET IRC or Java IRC

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC or Java IRC.
3. Click the **Virtual Drives** menu, and then select **Image File Removable Media** (IMG) or **Image File CD-ROM/DVD** (ISO).

   The IRC prompts you to select a file.
4. Enter the path or file name of the image file in the **File name** text box.

   You can also browse to the file location, and then click **Open**.

   The virtual drive activity LED will show virtual drive activity.

Using a virtual drive to install an OS and provide a required driver (.NET IRC or Java IRC)

You can use the remote console virtual drive feature to install an operating system. During the installation, you might be prompted to provide access to a required driver, such as a storage controller driver.

Prerequisites

- Remote Console privilege
- The operating system ISO file is available on the client you will use to run the remote console.
- If you will install an operating system on an NVMe drive, the **Boot Mode** is set to **Unified Extensible Firmware Interface (UEFI)**.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Download and extract the required driver.

   You can obtain drivers from the SPP or download them from the following website: **http://www.hpe.com/support/hpesc**.
2. Copy the driver to a USB key or a folder on the client where you will access the remote console.
3. Start the remote console.

- If you will use a USB key to provide the required driver, choose the .NET IRC or Java IRC.
- If you will use a virtual folder to provide the required driver, choose the .NET IRC.

4. Mount the operating system ISO.
   a. Select **Virtual Drives > Image File CD-ROM/DVD**.

      The remote console prompts you to select a file.
   b. Enter the path or file name of the image file in the **File name** text box.

      You can also browse to the file location, and then click **Open**.
5. If you will provide the required driver on a USB key, do the following:
   a. Connect the USB key to the client you are using to manage iLO.
   b. In the remote console, click the **Virtual Drives** menu, and then select the drive letter of the USB key on your client PC.
6. If you will provide the required driver in a folder on the client you use to manage iLO, do the following:
   a. Select **Virtual Drives > Folder**.
   b. In the **Browse for Folder** window, select the folder that contains the driver file.
7. Boot to the operating system ISO.
8. Follow the onscreen instructions until the operating system installer prompts you for the path to the driver.
9. When prompted for the driver location, enter the path to the USB key or virtual folder that contains the driver.
10. Follow the onscreen instructions to complete the operating system installation.
11. Install any additional required device drivers.

    You can obtain device drivers from the SPP.

Using a URL-based image file with the HTML5 IRC

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The image file you want to use is on a web server on the same network as iLO.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the HTML5 IRC.
3. Click the **Virtual Media** icon and select **Floppy > Scripted Media URL** for an IMG file, or select **CD/DVD > Scripted Media URL** for an ISO file.

   iLO prompts you to enter an image file URL.
4. Enter the URL for the image file that you want to mount as a virtual drive, and then click **Apply**.

   The virtual drive activity LED does not show drive activity for URL-mounted virtual media.

Using a URL-based image file with the .NET IRC or Java IRC

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The image file you want to use is on a web server on the same network as iLO.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC or Java IRC.
3. Select **Virtual Drives > URL Removable Media** for an IMG file or **Virtual Drives > URL CD-ROM/DVD** for an ISO file.

   iLO prompts you to enter an image file URL.
4. 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 a virtual folder (.NET IRC only)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC.
3. Select **Virtual Drives > Folder**.
4. 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. You can browse to the server and transfer the files from the virtual image to the server.

A virtual folder is nonbootable and read-only; the mounted folder is static. Changes to the client folder are not replicated in the mounted folder. To update your view of a virtual folder after changing the client folder, simply disconnect and then reconnect the virtual folder.

Create Media Image feature (Java IRC only)

When you use virtual media, performance is fastest when you use image files 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 (Java IRC)

The Create Media Image feature enables you to create disk image files from data in a file or on a physical disk. You can create an ISO-9660 disk image file (IMG or ISO).

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the Java IRC.
3. Select **Virtual Drives > Create Disk Image**.

   The **Create Media Image** dialog box opens.
4. Verify that the **Disk>>Image** button is displayed. If the button label is **Image>>Disk**, click the button to change it to **Disk>>Image**.
5. Do one of the following:
   - If you will use a file, select **Media File**, and then click **Browse** and navigate to the file you want to use.
   - If you will use physical media, select **Media Drive**, and then select the drive letter of the floppy disk, USB key, or CD in the **Media Drive** menu.
6. Enter the path and file name for the image file in the **Image File** text box.
7. Click **Create**.

   iLO notifies you when the image creation is complete.
8. Click **Close**.
9. Confirm that the image was created in the specified location.

Copying data from an image file to a physical disk (Java IRC)

The Create Media Image feature enables you to copy the data from a disk image file to a floppy disk or USB key. Only disk image (IMG) files are supported. Copying data to a CD is not supported.

You can copy disk image data to a floppy disk or USB key.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the Java IRC.
3. Select **Virtual Drives > Create Disk Image**.

   The **Create Media Image** dialog box opens.
4. In the **Create Media Image** window, click **Disk>>Image**.

   The **Create Media Image** changes to the **Image>>Disk** option.

5. Select the drive letter of the floppy disk or USB key in the **Media Drive** menu.
6. Enter the path and file name for the existing image file in the **Image File** text box.

   iLO notifies you when the operation is complete.
7. Click **Close**.
8. Confirm that the files were copied to the specified location.

Console capture (.NET IRC)

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.

- 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 information when server startup is detected. It stops when the file runs out of space. This file is overwritten each time the server starts.
- The server prefailure file starts capturing information when the server startup file is full. It 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 at the bottom of the .NET IRC session window.

Console capture controls

The following console capture controls are available, from left to right:

- **Skip to Start**—Restarts playback from the beginning of the file.
- **Pause**—Pauses 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

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC.
3. Press the **Play** button.

   The **Play** button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.

   The **Playback Source** dialog box opens.
4. Select **Server Startup** or **Server Prefailure**.
5. Click **Start**.

Saving server startup and server prefailure video files

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC.
3. Press the **Play** button.

   The **Play** button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.
4. Select **Server Startup** or **Server Prefailure**.
5. Click **Start**.
6. Press the **Play** button again to stop playback.

   iLO notifies you that the recording is no longer write-protected, and prompts you to save it.
7. Click **Yes**.
8. Select a save location, enter a file name, and then click **Save**.
9. (Optional) Play the video file.

Capturing video files with the remote console

Use this procedure to capture video files of sequences other than server startup and server prefailure.

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC.
3. Click the **Record** button.

   The **Record** button has a red circle icon, and it is located in the toolbar at the bottom of the remote console window.

   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.
6. (Optional) Play the video file.

Viewing saved video files with the remote console

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console > Remote Console** page.
2. Start the .NET IRC.
3. Press the **Play** button.

The **Play** button has a green triangle icon, and it is located in the toolbar at the bottom of the remote console window.

The **Playback Source** dialog box opens.

4. Click the magnifying glass icon next to the **From File** box.
5. Navigate to a video file, and then click **Open**.

   Video files captured in the remote console use the iLO file type.
6. Click **Start**.

Screen captures with the IRC

Use the remote console screen capture feature when you want to save a screen capture of the server activity. For example, you might want to capture a POST code displayed on the remote console screen.

When you use the IRC screen capture feature, the remote console status bar is not included in the captured image. If you want a screen capture that includes the status bar, use a different screen capture method.

Capturing the HTML5 remote console screen

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console** --> **Remote Console** page.
2. Start the HTML5 remote console.
3. Click the camera icon in the status bar.

   The screen capture opens in a new browser tab.
4. (Optional) Save the screen capture.

Capturing the .NET IRC screen

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Remote Console** --> **Remote Console** page.
2. Start the .NET IRC.
3. Double-click the status bar.

   A screen capture is saved in the clipboard.
4. (Optional) Paste the screen capture into an image editor.

Remote console hot keys

The 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. The key combination is sent to the host server when the hot key is pressed. Hot keys are active during remote console sessions that use the integrated remote console 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.

NOTE:

If will you do a lot of typing in remote console sessions, you might want to avoid assigning hot keys that use Ctrl+X and Ctrl+V shortcuts. These shortcuts are normally assigned to the cut and paste features.

Creating remote console hot keys

Prerequisites

Configure iLO Settings privilege

Procedure

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 key on the international keyboard. Keys for configuring remote console computer lock keys and hot keys 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 computer lock keys and hot keys

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

Resetting hot keys

Resetting the hot keys clears all current hot key assignments.

Prerequisites

Configure iLO Settings privilege

Procedure

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)

Prerequisites

- Remote Console privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Remote Console > Remote Console page.
2. Start the Java IRC.
3. 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, described in the following sections:

- iLO Virtual Serial Port
- Text-based Remote Console (Textcons)

iLO Virtual Serial Port

You can access a text-based console from iLO using a standard license and the Virtual Serial Port.

The Virtual Serial Port provides 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.

> **NOTE:**
>
> If connecting through the physical serial port is unsuccessful when Microsoft Windows boots, COM port settings must be modified manually or through a task. For more information, see **Advisory: HPE Integrated Lights-Out 5 (iLO 5) - iLO 5 Connecting Through the Physical Serial Port Is Not Successful When Microsoft Windows Boots** on the HPE Support Center.

The Virtual Serial Port is displayed as a text-based console, but 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. This feature enables an iLO Standard system to observe and interact with the server during POST.

By using the Virtual Serial Port, a remote user can perform operations such as the following:

- Interact with the server POST sequence and the operating system boot sequence.

  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 + shift 9 or Esc + (.

- 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 Virtual Serial Port to view a login session to the Linux OS.
- Use the EMS Console through the Virtual Serial Port. EMS is useful for debugging Windows boot issues and kernel-level issues.

Before you can access the Virtual Serial Port, you must configure it in the ROM-based system utility, and then configure the server OS to use it. The method you use to configure the Virtual Serial Port depends on whether your server supports the legacy ROM-based system utility or the UEFI System Utilities. To determine which utility a server supports, see the server QuickSpecs at **http://www.hpe.com/info/qs**.

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 Virtual Serial Port. This procedure is required for both Windows and Linux systems.

Use this procedure on servers that do not support the UEFI System Utilities.

Procedure

1. Optional: If you access the server remotely, start a 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 Virtual Serial Port does not use a physical UART. The BIOS Serial Console Baud Rate value has no effect on the speed the Virtual Serial Port uses to send and receive data.
7. For Windows environments only: Set the EMS Console COM port.
   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 Virtual Serial Port. This procedure is required for both Windows and Linux systems.

Use this procedure on servers that support the UEFI System Utilities.

Procedure

1. Access the UEFI System Utilities.
   a. Optional: If you access the server remotely, start a 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 Virtual Serial Port does not use a physical UART. The BIOS Serial Console Baud Rate value has no effect on the speed the Virtual Serial Port uses to send and receive data.
   c. Press ESC.

      The main menu is displayed.
5. For Windows environments only: Set the EMS Console COM port.
   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 Linux to use the iLO Virtual Serial Port

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 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).

Configuring Red Hat Enterprise Linux 6 to use the iLO Virtual Serial Port

Procedure

1. Configure GRUB based on the following configuration examples.

   NOTE:

   In the following configuration examples, 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 /vmlinux-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 /vmlinux-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.

2. 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
   ```

3. Use SSH to connect to iLO, and then use the CLP command `start /system1/oemhp_vsp1` to view a login session to the Linux operating system.

Configuring Red Hat Enterprise Linux 7 to use the iLO Virtual Serial Port

Procedure

1. Open `/etc/sysconfig/grub` with a text editor.

   This configuration example uses `ttys0`.

   - At the end of the line `GRUB_CMDLINE_LINUX`, enter `console=ttys0`.
   - Remove `rhgb quiet`.
   - Enter the following parameters:

     ```
     GRUB_TIMEOUT=5
     GRUB_DEFAULT=saved
     GRUB_DISABLE_SUBMENU=true
     GRUB_TERMINAL_OUTPUT="console"
     GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
     console=ttyS0,115200n8"
     GRUB_DISABLE_RECOVERY="true"
     ```

2. Enter the following command to create the `grub.cfg` file:

   ```
   grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
   ```

3. Enable a `getty` login service for the serial port.

   For example:

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

4. Configure `getty` to listen on the serial port.

   For example:

   ```
   systemctl start getty@ttyS0.service
   ```

5. 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
   ```

6. Use SSH to connect to iLO, and then use the CLP command `start /system1/oemhp_vsp1` to view a login session to the Linux operating system.

Configuring SUSE Linux Enterprise Server to use the iLO Virtual Serial Port

Procedure

1. Open `/etc/default/grub` with a text editor.

   This configuration example uses `ttys0`.

   At the end of the line `GRUB_CMDLINE_LINUX_DEFAULT`, enter `"console=tty0 console=ttyS0,115200n8"`.

2. To update the `grub.cfg` file, enter one of the following commands:

   For servers using the UEFI boot mode:

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

   For servers using the Legacy BIOS boot mode:

   ```
   grub-mkconfig -o /boot/efi/EFI/sles/grub.cfg
   ```

3. Use `systemctl` to configure `getty` to listen on `/dev/ttyS0`:

   ```
   systemctl start getty@ttyS0.service
   ```

4. To configure `getty` to listen on `/dev/ttyS0` for every boot, enable the service for that specific port.

   For example:

   ```
   systemctl enable serial-getty@ttyS0.service
   ```

5. 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
   ```

6. 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:

- The Windows EMS console must be configured in the OS before you can use the 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 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 Remote Console at the same time.
- To display the `SAC>` prompt, you might have to press Enter after connecting through the Virtual Serial Port.

Configuring Windows for use with the iLO Virtual Serial Port

Enter
`bcdedit /?`
for syntax help when you complete these steps.

Procedure

1. Open a command window.
2. To edit the boot configuration data, enter the following command:

   ```
   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.

4. To enable or disable emergency management services for a boot application, enter the following command:

   ```
   bcdedit /bootems on
   ```

5. Reboot the operating system.

Starting an iLO Virtual Serial Port session

Prerequisites

- The Virtual Serial Port settings are configured in the iLO RBSU or UEFI System Utilities.
- The Windows or Linux operating system is configured for use with the Virtual Serial Port.

Procedure

1. Start an SSH session.

   For example, you could enter
   ```
   ssh Administrator@<iLO IP address>
   ```
   or connect through port 22 with `putty.exe`.

2. When prompted, enter your iLO account credentials.

3. At the `</>hpiLO->` prompt, enter
   ```
   VSP
   ```
   , and press Enter.

4. For Windows systems only: At the `<SAC>` prompt, enter
   ```
   cmd
   ```
   to create a command prompt channel.

5. For Windows systems only: To switch to the channel specified by the channel number, enter
   ```
   ch - si <#>
   ```
   .

6. When prompted, enter the OS login credentials.

Viewing the iLO Virtual Serial Port log

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.

You can view Virtual Serial Port activity by using the `vsp log` command.

Prerequisites

- Secure Shell (SSH) Access and Virtual Serial Port Log are enabled on the Access Settings page.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Connect to the CLI through SSH.
2. Use the
   ```
   vsp
   ```
   command to view Virtual Serial Port activity.
3. Enter
   ```
   ESC (
   ```
   to exit.
4. To view the Virtual Serial Port log, enter
   ```
   vsp 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. This boot mode does not use the framebuffer console. This feature is not supported on servers that are configured to use the UEFI boot mode.

When you use Textcons, the presentation of colors, characters, and screen controls depends on your SSH client. You can use any standard SSH client that is 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

Using the Text-based Remote Console

Prerequisites

The server is configured to use the Legacy BIOS boot mode.

Procedure

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.

4. To exit the Text-based Remote Console and return to the CLI session, press Esc+Shift+9.

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.

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.

Controlling 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
```

Controlling 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
```

Configuring 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. The following table lists the supported equivalents.

Table 2: 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 iLO virtual media

Virtual media considerations

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 use USB technology to connect to the host server.

When you use virtual media, consider the following:

- 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 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 OS, a virtual floppy/USB key or virtual CD/DVD-ROM behaves like any other drive. When you use virtual media for the first time, the host OS 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 finish 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 OS 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 media device enables you to perform tasks such as deploying an OS from network drives, and performing disaster recovery of failed operating systems.

  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.
  - When the host server OS is running, you can use the virtual floppy/USB key 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 a physical floppy disk, a USB key, a 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 that is accessible through a high-speed network link.
- If the host server OS supports USB mass storage devices, the iLO Virtual CD/DVD-ROM is available after the host server OS loads.
  - When the host server OS is running, you can use the virtual CD/DVD-ROM 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.
- When the virtual floppy/USB key or virtual CD/DVD-ROM feature is in use, you cannot typically access the floppy drive or CD/DVD-ROM drive from the client OS.

  CAUTION:

  To prevent file and data corruption, do not try to access the local media when you are using it as a virtual media device.
- For the HTML5 IRC and Java IRC with OpenJDK only: When you refresh or close the iLO web interface window, the remote console connection is closed.

  When a remote console connection is closed, you lose access to virtual media devices connected through the remote console, except for devices that were connected by using URL-based virtual media.

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

By default, Windows 7 powers off the iLO virtual hub when no Virtual Media devices are enabled or connected during boot.

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

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.

Red Hat Enterprise Linux, SUSE Linux Enterprise Server, and Ubuntu 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 virtual CD/DVD-ROM mounts automatically in a Linux GUI.

For information about mounting a virtual CD/DVD-ROM in the Linux command line, see Mounting a USB virtual media CD/DVD-ROM (Linux command line).

Depending on the Linux distribution, the virtual CD/DVD-ROM is accessible at one of the following device files:

- `/dev/cdrom`
- `/dev/scd0`
- `/dev/sr0`

On servers that have a local CD/DVD-ROM device, the Virtual CD/DVD-ROM device is accessible with the device number that follows the local DVD device (for example, `/dev/cdrom1`).

Mounting a USB virtual media CD/DVD-ROM (Linux command line)

Procedure

1. Log in to the iLO web interface.
2. Start the .NET IRC or Java IRC.
3. Select the Virtual Drives menu.
4. Select a CD/DVD-ROM or ISO file.
5. Locate the iLO virtual media device entry on the Linux system.

   You can view the device entry in the system message log file. For example, the following image shows the device entry `/dev/sr0`.

6. Create a mount point.

   For example:

   - Red Hat Enterprise Linux: `mkdir /mnt/cdrom`*`X`*, where X is a number you choose.
   - SUSE Linux Enterprise Server: `mkdir /media/cdrom`*`X`*, where X is a number you choose.

7. Mount the device by entering a command similar to the following: `mount` *`device file mount point`*.

   For example:

   - Red Hat Enterprise Linux: `mount /dev/cdrom1 /mnt/cdrom1`
   - SUSE Linux Enterprise Server: `mount /dev/scd0 /media/cdrom1`

iLO web interface Virtual Media options

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 Access Settings page.

- View or eject local media, including physical drives, local image files, and virtual folders.
- 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

Procedure

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 connected local media

Prerequisites

Virtual Media privilege

Procedure

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.

- Connection Status—Indicates whether a virtual media device is connected.
- Read-Only—Whether the virtual media device is connected with read-only permission.

Virtual CD/DVD-ROM Status

- Media Inserted—The virtual media type that is connected.

  Local Media is displayed when local media is connected.

- Connection Status—Indicates whether a virtual media device is connected.

Ejecting a local virtual media device

Prerequisites

Virtual Media privilege

Procedure

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 Remote Console, 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).

Prerequisites

- Virtual Media privilege
- The IMG or ISO image you want to connect is on a web server on the same network as iLO.

Procedure

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.

   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.

   The image will be ejected automatically on the second server reboot so that the server does not boot to the image twice.

   If this check box is not selected, the image remains connected until it is manually ejected. The server will boot to the image 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. You cannot modify the boot order during POST. Wait for POST to finish, and then try again.

4. Click Insert Media.
5. Optional: To boot to the connected image now, click Server Reset.

Viewing connected scripted media

Prerequisites

Virtual Media privilege

Procedure

Navigate to the Virtual Media > Virtual Media page.

Scripted media details

When scripted media is connected, the details are listed in the Virtual Floppy/USB Key/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.

The Virtual Floppy/USB Key/Virtual Folder Status and Virtual CD/DVD-ROM Status sections are displayed only when media is connected.

Ejecting scripted media

Prerequisites

Virtual Media privilege

Procedure

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.

   For server blades without an iLO license that grants full Virtual Media privileges, you cannot use the Force Eject Media option with a URL-based virtual media image. 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.

Setting up IIS for scripted virtual media

Prerequisites

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

Use this procedure to configure IIS to serve diskette or ISO-9660 CD images for read-only access.

Procedure

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

Procedure

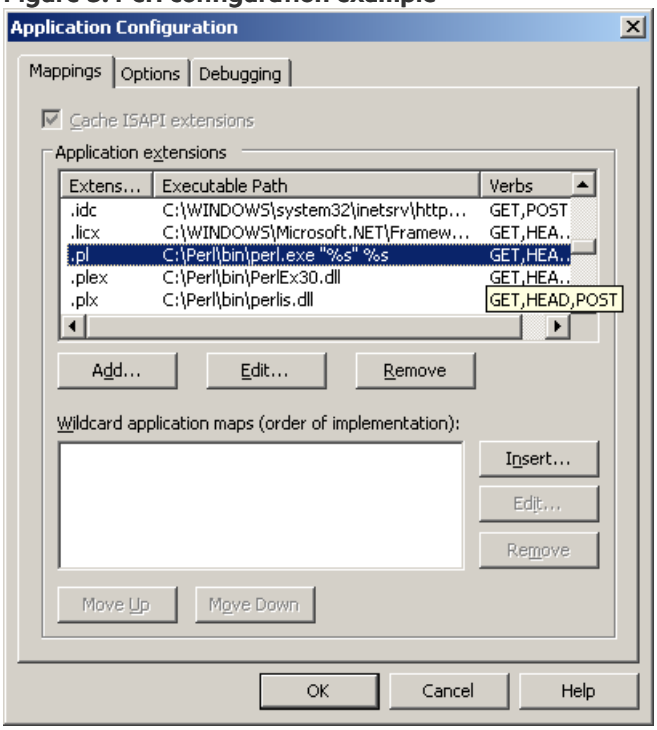
1. Install Perl (for example, ActivePerl).
2. Customize the virtual media helper application as needed.
3. Create a directory on your website for the virtual media helper script, and then copy the script to that directory.

   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 the following example:

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.

Inserting virtual media with a helper application

When you use 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 HPE iLO 4 Scripting and Command Line 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";
```

Boot Order

The 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

Procedure

1. Navigate to the Virtual Media > Boot Order page.
2. Select Unified Extensible Firmware Interface (UEFI) or Legacy BIOS, and then 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.
3. Click OK.
4. Click Server Reset.

Configuring the server boot order

Prerequisites

Configure iLO Settings privilege

Procedure

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. To move a device up or down in the boot order, select the device in the Server Boot Order list, and then click Up or Down.

   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.

Changing the one-time boot status in Legacy BIOS mode

Prerequisites

Configure iLO Settings privilege

Procedure

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

Prerequisites

Configure iLO Settings privilege

Procedure

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 Boot Order page options

The Additional Options section on the Boot Order page provides buttons for resetting the server and booting to the system setup utilities.

Prerequisites

- The Virtual Media and Configure iLO Settings privileges are required for the Boot to System RBSU and Boot to System Setup Utilities features.
- The Virtual Power and Reset privilege is required for the Server Reset feature.

Procedure

1. Navigate to the Virtual Media > Boot Order page.
2. Do one of the following:
   - To load the ROM-based setup utility on the next server reset, click Boot to System RBSU (Legacy BIOS) or Boot to System Setup Utilities (UEFI).
   - To reboot the server, click Server Reset.

Using the power management features

Server power-on

Nonblade servers

Before the introduction of ProLiant Gen8 servers, some ProLiant servers (ML and DL) could be powered on by pressing the power button within a few seconds after AC power was connected. If an AC power loss occurs on ProLiant Gen8 or ProLiant 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 flash, 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 ProLiant 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, the 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 drivers must be loaded. iLO communicates with the drivers and uses the appropriate operating system method of shutting down the system safely to ensure that data integrity is preserved.

If the drivers are 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.

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). 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.

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 > Power page.

Power-on protection

iLO 4 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 and compute modules)

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

Procedure

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 8 seconds. Using this option circumvents the graceful shutdown features of the operating system.

Configuring the System Power Restore Settings

The System Power Restore Settings enable you to control system behavior after power is lost.

Prerequisites

Configure iLO Settings privilege

Procedure

1. Navigate to the Power Management > Server Power page.
2. Select an Auto Power-On value.

   Changes to the Auto Power On value might not take place until after the next server reboot.
3. Select a Power-On Delay value.

   This setting is not available if the Auto Power-On option is set to Always Remain Off.
4. Click Submit.

Auto Power-On

The Auto Power-On 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.

Choose from the following Auto Power-On settings:

- Always Power On—Power on the server after the power-on delay.

  This option is the default setting 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.

  When a Synergy compute module is configured to use this setting, iLO attempts to restore the previous power state when power is restored. If an issue such as insufficient power or insufficient cooling occurs, or an HPE OneView power hold occurs, then it might not be possible to restore the power state. For more information, check HPE OneView or the IML.

Power-On Delay

The Power-On Delay 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.

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.

The 15, 30, 45, and 60 second delay values are not available on c-Class blade servers or Synergy compute modules. These server types are managed by external products such as OA, HPE OneView, or the Frame Link Module. iLO will attempt to power on the servers based on the configured power-on delay setting, but external factors might affect the actual startup time.

Viewing server power usage

The Power Meter page displays the server power consumption over time.

Prerequisites

- The server power supplies and the system BIOS support power readings. If power readings are not supported, this page displays the following message: `The Power Manager is unavailable for this configuration`.
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

Navigate to the Power Management > Power Meter page.

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.

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

Prerequisites

The server power supplies and the system BIOS support power readings. If power readings are not supported, this page displays the following message: `The Power Manager is unavailable for this configuration`.

Procedure

Navigate to the Power Management > Power Meter page.

The Current State section displays the current power state details.

Current power state details

The values displayed in the Current State table vary depending on the server type. The following values are possible:

- 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 to the server.

  This value is displayed for ML and DL servers.

- Power Regulator Mode—The configured mode. For information about the possible settings, see Power settings.

  This value is displayed for all servers.

- 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

Prerequisites

The server power supplies and the system BIOS support power readings. If power readings are not supported, this page displays the following message: `The Power Manager is unavailable for this configuration`.

Procedure

Navigate to the Power Management > Power Meter page.

The Power History section displays the server power history details.

Power history details

The Power History table shows power readings from three time periods: 5 minutes, 20 minutes, and 24 hours.

- 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.
- 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.
- 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 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.

Configuring 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
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The server is not in POST. The Power Regulator settings cannot be changed while the server is in POST.

Procedure

1. Navigate to the Power Management > Power Settings page.
2. Select a Power Regulator mode, and then 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.
3. If iLO notified you that a reboot is required, reboot the server.

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 value for the system. Performance impacts are greater for environments with higher processor utilization.
- Static High Performance Mode—Processors will run at maximum power and performance at all times, regardless of the OS power management policy.
- OS Control Mode—Processors will run at maximum power and performance at all times, unless the OS enables a power management policy.

Configuring power caps

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- The server model supports power capping.

  See the server specifications for support information.

  Power capping is not supported on Synergy compute modules.
- The server does not have a mismatched power supply configuration.

Procedure

1. Navigate to the Power Management > Power Settings page.
2. Select the Enable power capping check box.
3. 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 lower than the server minimum power value.
4. (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.
5. 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 Maximum Power Cap threshold (the highest power cap that can be set).

    For server blades, this value is the initial power-on request value.

    For nonblade servers, this value is the power supply capacity.

  - Peak Observed Power—The maximum observed power for the server. This value is also the Minimum High-Performance Cap threshold. It is the lowest power cap value that can be set without affecting server performance.

  - Minimum Observed Power—The minimum observed power for the server. This value is also the Minimum Power Cap threshold. 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 lower than 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.
- Power capping settings for some servers must be managed outside of the iLO web interface with tools such as:

  - HPE ProLiant Power Interface Control Utility
  - HPE Advanced Power Manager

  See the server specifications at **http://www.hpe.com/info/qs** for information about the power management features your server supports.

- The power capping feature is disabled on servers with mismatched power supplies.

Configuring battery backup unit settings

When the power supplies cannot provide power to a server with a battery backup unit, 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.

> **NOTE:**
>
> Battery backup unit settings are disabled when the system is configured for Scalable Persistent Memory.

Prerequisites

Configure iLO Settings privilege

Procedure

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 specifications at the following website: **http://www.hpe.com/info/qs**.

Configuring SNMP alert on breach of power threshold 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

Procedure

1. Navigate to the Power Management > Power Settings page.
2. Select a value in the Warning Trigger list.
3. If you selected Peak Power Consumption or Average Power Consumption, enter the following:
   - Warning Threshold
   - Duration
4. (Optional) To change the Warning Threshold display to Watts or BTU/hr, click Show values in Watts or Show values in BTU/hr.
5. Click Apply.

SNMP Alert on breach of power threshold options

- Warning Trigger—Determines whether warnings are based on peak power consumption, average power consumption, or if they are disabled.
- 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. Enter a value from 5 to 240 minutes. The value must be a multiple of 5.

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 USB 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

Procedure

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.

Working with enclosures, frames, and chassis

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 provides information about the primary OA in the enclosure in which the iLO processor is located. You can view enclosure information, start the OA web interface, and toggle the server or enclosure UID LEDs. This page is displayed only when an enclosure is present.

Viewing OA information

The Active Onboard Administrator page provides general information about the primary OA in the enclosure in which the iLO processor is located.

Procedure

Navigate to the BL c-Class > Active Onboard Administrator page.

OA details

- 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

Procedure

1. Navigate to the BL c-Class > Active Onboard Administrator page.
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

Procedure

1. Navigate to the BL c-Class > Active Onboard Administrator page.
2. To change the state of the enclosure UID LED where iLO is located, click the Toggle UID button.

   The UID LED status on the Active Onboard Administrator 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 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.

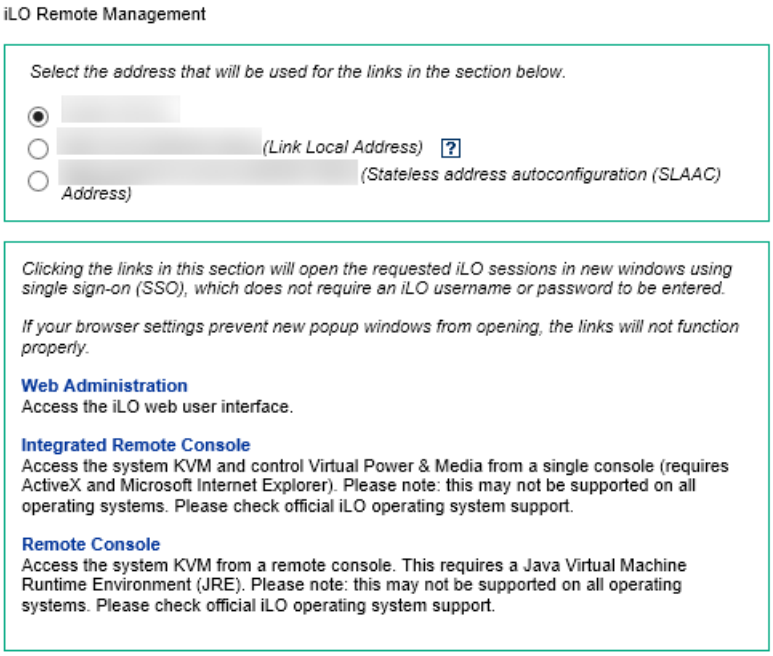
iLO virtual fan

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.

Viewing frame information

The Frame Information page provides information about the frame that contains the Synergy compute module that includes the iLO processor.

Procedure

1. Navigate to the Synergy Frame > Frame Informaton page.
2. Optional: To view compute module details, move the cursor over the compute module in the frame diagram.

   The following compute module details are available: Health status, host name, model, and UID status.
3. Optional: To view the frame health status or UID LED status, move the cursor over the frame icons in the frame diagram.

Frame details

- 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 compute module in the frame.
- Frame serial number—The frame serial number.
- Frame unique ID (UUID)—The frame UUID.

Toggling the frame or compute module UID

Procedure

1. Navigate to the Synergy Frame > Frame Informaton page.
2. To change the state of the frame or compute module UID LED, click in the frame diagram.

   The UID LED status values on the Frame Information page update automatically when iLO detects a status change. To update the status immediately, refresh the page.

Viewing chassis information

Procedure

Navigate to the Chassis > Chassis Information page.

The Chassis Information page is available for SL and XL servers.

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 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 iPDUs.

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 PDU 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

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 Number—The battery serial number.
- Capacity—The battery capacity.
- Firmware—The installed battery firmware version.

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 with read and write access through the server operating system.

To determine whether your server includes a 4 GB iLO NAND, see the server QuickSpecs at **http://www.hpe.com/info/qs/**.

Embedded User Partition use cases

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 boot mode only)

  To select the Embedded User Partition for an OS or hypervisor installation, select the volume iLO LUN <number>.

- Storing iLO scripts
- Storing iLO language packs

IMPORTANT:
Do not use the Embedded User Partition for high-frequency write operations.

Configuring the Embedded User Partition

You can use the UEFI System Utilities, UEFI Shell, and RESTful Interface Tool to configure the Embedded User Partition.

This guide covers the UEFI System Utilities and UEFI Shell. For information about using the RESTful Interface Tool, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

Configuring the Embedded User Partition (UEFI System Utilities)

Procedure

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.

   After 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)

Procedure

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 boot settings

You can use the UEFI System Utilities, UEFI Shell, iLO web interface, or RESTful Interface Tool to configure the Embedded User Partition boot settings.

This guide covers the iLO web interface, UEFI System Utilities, and UEFI Shell. For information about using the RESTful Interface Tool, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.

Configuring the Embedded User Partition boot order setting (iLO web interface)

Prerequisites

- Configure iLO Settings privilege
- Virtual Media privilege
- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Procedure

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 Partition
   ```

3. Click Apply.

   The following message appears:

   ```
   Successfully set boot order.
   ```

Configuring the Embedded User Partition for one-time boot (iLO web interface)

- Configure iLO Settings privilege
- Virtual Media privilege
- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Use the following procedure to set the position of the Embedded User Partition in the Server Boot Order list.

Prerequisites

Procedure

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.

Prerequisites

- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Procedure

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.

Prerequisites

- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Procedure

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)

Prerequisites

- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Procedure

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 more information about using this command, see the UEFI Shell user guide.

Configuring the Embedded User Partition for one-time boot (UEFI Shell)

Prerequisites

- The Embedded User Partition feature is enabled.
- The server is configured to use the Unified Extensible Firmware Interface (UEFI) boot mode.

  This feature is not supported when the Legacy BIOS boot mode is selected.

Procedure

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.

   For more information, see the UEFI Shell user guide.

Using iLO with other software products and tools

Viewing Location Discovery Services information

Prerequisites

A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

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

- 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-docs**.

Opening the System Management Homepage

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 > SNMP Settings page.

Procedure

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 various industry-standard tools can provide the SMS functionality. For more information, see the IPMI specification on the Intel website at **http://www.intel.com**.

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**.
- **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 driver is enabled, any IPMI traffic through the KCS interface can affect iLO performance and system health. Do not issue any IPMI commands through the KCS interface that might have a negative effect on IPMI services. 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 can communicate securely with the iLO firmware by using the IPMI 2.0 RMCP+ protocol. This feature 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 key managers with iLO

iLO 4 supports key managers, which can be used in conjunction with HPE Smart Array Secure Encryption and UEFI-managed encryption.

HPE Smart Array 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.

UEFI-managed encryption allows data-at-rest encryption for supported system devices such as HPE Persistent Memory and NVMe drives.

A key manager 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 key manager and the other products. iLO uses a unique user account based on its own MAC address for communicating with the key manager. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the key manager with administrator privileges. For more information about the deployment user account, see the key manager documentation.

Supported key managers

iLO supports the following key managers:

- Utimaco Enterprise Secure Key Manager (ESKM) 4.0 and later

  ESKM 5.0 or later is required when FIPS mode is enabled.

  CAUTION:

  If you use ESKM, ensure that you install the software update that includes updated code signing certificates. If you do not install the required update, your ESKM will enter an error state when restarted after January 1, 2019. For more information, see the **ESKM documentation**.

- Thales TCT KeySecure for Government G350v (previously known as SafeNet AT KeySecure G350v 8.6.0)
- Thales KeySecure K150v (previously known as SafeNet KeySecure 150v 8.12.0)
- Thales CipherTrust Manager 2.2.0, K170v (virtual) and K570 (physical) appliances

Configuring key manager servers

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Administration > Key Manager page.
2. Enter the following information:
   - Primary Key Server
   - Primary Key Server Port
   - Secondary Key Server
   - Secondary Key Server Port
3. (Optional) To check for server redundancy in configurations with a primary and secondary key server, enable the Require Redundancy option.

   Hewlett Packard Enterprise recommends enabling this option.
4. Click Apply.

Key manager server options

Primary Key Server Address

The primary key server hostname, IP address, or FQDN. This string can be up to 79 characters long.

Primary Key Server Port

The primary key server port.

Secondary Key Server Address

The secondary key server hostname, IP address, or FQDN. This string can be up to 79 characters long.

Secondary Key Server Port

The secondary key server port.

Require Redundancy

When this option is enabled, iLO verifies that the encryption keys are copied to both of the configured key servers.

When this option is disabled, iLO will not verify that encryption keys are copied to both of the configured key servers.

Hewlett Packard Enterprise recommends enabling this option.

Adding key manager configuration details

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Administration > Key Manager page.
2. Enter the following information in the iLO Account on Key Manager section:
   - Group
   - (Optional) Key Manager Local CA Certificate Name

   The Account Name value is read-only.
3. Enter the following information in the Key Manager Administrator Account section:
   - Login Name
   - Password
4. Click Update Key Manager.

   If iLO is not a member of a key manager local group, it will try to create a group with the requested name. If iLO is already a member of a key manager local group, it ignores the group you entered in step 3, and uses the existing group assignment that is present on the key manager. Attempted group changes in iLO do not affect current key group permissions that are set on the key manager. If a new group assignment is needed, update the key manager before updating the iLO settings.

   If you entered the Key Manager Local CA Certificate Name in step 3, certificate information is listed in the Imported Certificate Details section of the Key Manager page.

Key manager configuration details

Name

The listed iLO Account on Key Manager account name is ilo-<iLO MAC address>. The account name is read-only and is used when iLO communicates with the key manager.

Group

The local group created on the key manager for use with iLO user accounts and the keys iLO imports into the key manager. When keys are imported, they are automatically accessible to all devices assigned to the same group.

See the Secure Encryption installation and user guide for more information about groups and their use with key management.

Key Manager Local CA Certificate Name

To ensure that iLO is communicating with a trusted key manager server, enter the name of the local certificate authority certificate in the key manager. It is typically named Local CA and is listed in the key manager under local CAs. iLO will retrieve the certificate and use it to authenticate the key manager servers for all future transactions.

Secure Encryption does not support using a third-party trusted or intermediate CA.

Login Name

The local user name with administrator permissions that is configured on the key manager. This user name is the key manager 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 key manager.

Testing the key manager configuration

Use the Test Key Manager Connections option to verify the configuration settings. The tests confirm that iLO and the key manager servers are set up to provide key management services.

During the test, iLO attempts the following tasks:

- Connects to the primary key manager server (and secondary key manager server, if configured) by using TLS.
- Tries to authenticate to the key manager by using the configured credentials and account.
- Confirms that the version of the key manager software is compatible with iLO.

Prerequisites

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- A key manager is set up and the key manager configuration is complete in iLO.

Procedure

1. Navigate to the Administration > Key Manager page.
2. Click Test Key Manager Connections.

   The test results are displayed in the Key Manager Events table.

Viewing key manager events

Prerequisites

A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Administration > Key Manager page.
2. Scroll to the Key Manager Events section.

   Each event is listed with a time stamp and description.

Clearing the key manager log

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the Administration > Key Manager page.
2. Click Clear Key Manager Log.

   iLO prompts you to confirm the request.
3. Click Yes, clear.

Using key managers with iLO

iLO 4 supports key managers, which can be used in conjunction with HPE Smart Array Secure Encryption and UEFI-managed encryption.

HPE Smart Array 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.

UEFI-managed encryption allows data-at-rest encryption for supported system devices such as HPE Persistent Memory and NVMe drives.

A key manager 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 key manager and the other products. iLO uses a unique user account based on its own MAC address for communicating with the key manager. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the key manager with administrator privileges. For more information about the deployment user account, see the key manager documentation.

Supported key managers

iLO supports the following key managers:

- Utimaco Enterprise Secure Key Manager (ESKM) 4.0 and later

  ESKM 5.0 or later is required when FIPS mode is enabled.

  CAUTION:

  If you use ESKM, ensure that you install the software update that includes updated code signing certificates. If you do not install the required update, your ESKM will enter an error state when restarted after January 1, 2019. For more information, see the **ESKM documentation**.

- Thales TCT KeySecure for Government G350v (previously known as SafeNet AT KeySecure G350v 8.6.0)
- Thales KeySecure K150v (previously known as SafeNet KeySecure 150v 8.12.0)
- Thales CipherTrust Manager 2.2.0, K170v (virtual) and K570 (physical) appliances

Configuring key manager servers

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Administration > Key Manager** page.
2. Enter the following information:
   - **Primary Key Server**
   - **Primary Key Server Port**
   - **Secondary Key Server**
   - **Secondary Key Server Port**
3. (Optional) To check for server redundancy in configurations with a primary and secondary key server, enable the **Require Redundancy** option.

   Hewlett Packard Enterprise recommends enabling this option.
4. Click **Apply**.

Key manager server options

Primary Key Server Address

The primary key server hostname, IP address, or FQDN. This string can be up to 79 characters long.

Primary Key Server Port

The primary key server port.

Secondary Key Server Address

The secondary key server hostname, IP address, or FQDN. This string can be up to 79 characters long.

Secondary Key Server Port

The secondary key server port.

Require Redundancy

When this option is enabled, iLO verifies that the encryption keys are copied to both of the configured key servers.

When this option is disabled, iLO will not verify that encryption keys are copied to both of the configured key servers.

Hewlett Packard Enterprise recommends enabling this option.

Adding key manager configuration details

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Administration > Key Manager** page.
2. Enter the following information in the **iLO Account on Key Manager** section:
   - **Group**
   - (Optional) **Key Manager Local CA Certificate Name**

     The **Account Name** value is read-only.
3. Enter the following information in the **Key Manager Administrator Account** section:
   - **Login Name**
   - **Password**
4. Click **Update Key Manager**.

   If iLO is not a member of a key manager local group, it will try to create a group with the requested name. If iLO is already a member of a key manager local group, it ignores the group you entered in step3 , and uses the existing group assignment that is present on the key manager. Attempted group changes in iLO do not affect current key group permissions that are set on the key manager. If a new group assignment is needed, update the key manager before updating the iLO settings.

   If you entered the **Key Manager Local CA Certificate Name** in step 3, certificate information is listed in the **Imported Certificate Details** section of the **Key Manager** page.

Key manager configuration details

Name

The listed **iLO Account on Key Manager** account name is **ilo-<iLO MAC address>**. The account name is read-only and is used when iLO communicates with the key manager.

Group

The local group created on the key manager for use with iLO user accounts and the keys iLO imports into the key manager. When keys are imported, they are automatically accessible to all devices assigned to the same group.

See the Secure Encryption installation and user guide for more information about groups and their use with key management.

Key Manager Local CA Certificate Name

To ensure that iLO is communicating with a trusted key manager server, enter the name of the local certificate authority certificate in the key manager. It is typically named **Local CA** and is listed in the key manager under local CAs. iLO will retrieve the certificate and use it to authenticate the key manager servers for all future transactions.

Secure Encryption does not support using a third-party trusted or intermediate CA.

Login Name

The local user name with administrator permissions that is configured on the key manager. This user name is the key manager 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 key manager.

Testing the key manager configuration

Use the **Test Key Manager Connections** option to verify the configuration settings. The tests confirm that iLO and the key manager servers are set up to provide key management services.

During the test, iLO attempts the following tasks:

- Connects to the primary key manager server (and secondary key manager server, if configured) by using TLS.
- Tries to authenticate to the key manager by using the configured credentials and account.
- Confirms that the version of the key manager software is compatible with iLO.

Prerequisites

- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.
- A key manager is set up and the key manager configuration is complete in iLO.

Procedure

1. Navigate to the **Administration > Key Manager** page.
2. Click **Test Key Manager Connections**.

   The test results are displayed in the **Key Manager Events** table.

Viewing key manager events

Prerequisites

A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Administration > Key Manager** page.
2. Scroll to the **Key Manager Events** section.

   Each event is listed with a time stamp and description.

Clearing the key manager log

Prerequisites

- Configure iLO Settings privilege
- A license that supports this feature is installed. For information about the available license types and the features they support, see the licensing documentation at the following website: **http://www.hpe.com/info/ilo-docs**.

Procedure

1. Navigate to the **Administration > Key Manager** page.

2. Click **Clear Key Manager Log**.

   iLO prompts you to confirm the request.

3. Click **Yes, clear**.

iLO and remote management tools

iLO 4 1.30 and later supports 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.

Procedure

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.

Procedure

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.

   iLO warns you to proceed only if the managed server is no longer managed by the remote management tool.
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 supported servers. 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 HPE SSO page.
- NTP (time server) configuration
- User Account—An administrative user account is added to iLO.
- Firmware version—If a supported version of the iLO firmware is not already installed when you add a server to HPE OneView, the iLO firmware is updated automatically. 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.

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 an 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 **https://www.hpe.com/support/restfulinterface/docs**.

Adding hotfixes to create an HPE OneView custom firmware bundle

To add hotfixes to create an HPE OneView custom firmware bundle for using as a baseline (and optionally for SUT installation), follow the procedure:

Procedure

1. Download all the required update packages to your local system.
2. From the HPE OneView main menu, select Appliance and then select Firmware Bundles.

   The ServicePack baseline packages are listed.

   > **NOTE:**
   >
   > There must be at least one ServicePack baseline loaded. If not, download a compatible Service Pack for ProLiant, HPE Synergy Custom SPP, or HPE Synergy Service Pack and load it into HPE OneView before proceeding.

3. Click Add Firmware Bundle. The Add Firmware Bundle dialog box appears.
4. On the Add Firmware Bundle dialog, click Browse and then select one of the update packages downloaded in step 1.

   You can select only one file at a time. The file type must be scexe, exe, rpm, zip, or fwpkg

   > **NOTE:** HPE Smart Update Manager (SUM) version 8.7.0 or later supports the fwpkg file type. If you have baseline Service Pack that was released prior to October 2020, select a supported file type other than fwpkg.

5. Click OK to upload the file.
6. After the file is uploaded, HPE OneView may display an error indicating a missing signature file. This is an expected behavior for Gen10 update packages.

   To upload a missing signature file:

   a. Expand the error message and click **Upload signature** file link. Alternatively, from the menu, select Actions and then select Upload signature file. The Upload signature file dialog box appears.

   b. Click Browse and select the signature file that was included with the package. The signature file will have a .compsig extension.

      Some update packages require multiple signature files. You must upload each signature file individually.

   c. Click OK to upload the signature file.

      Wait for HPE OneView to process and associate the signature file. When the process is complete, HPE OneView validates the update files and the **Hotfix** will show a healthy status.

7. From the Firmware Bundles Actions menu, choose Create custom firmware bundle. The Create Custom Firmware Bundle dialog box appears.
8. Select a name for the custom firmware bundle, noting that a custom firmware bundle may contain one or more hotfix packages.
9. Select the base firmware bundle to which one or more hotfix packages will be added to create the custom firmware bundle.
10. Click Add Hotfix. The Add Hotfix dialog box appears.
11. Select all hotfix packages required by this custom firmware bundle. You can select multiple hotfix packages.
12. When all the required hotfix packages are selected, click Add.

    The selected hotfix packages are displayed on the Create Custom Firmware Bundle dialog box.

13. Click OK. The Create Custom Firmware Bundle dialog is dismissed and HPE OneView creates a firmware bundle. The new firmware bundle will include the base firmware bundle and the hotfix packages previously added.

    After the custom firmware bundle is created, you can select it as a new logical enclosure firmware baseline. It can also be used as a firmware baseline for server profiles and server profile templates.

14. To install the updates online using HPE Smart Update Tools:

    - Set the Firmware baseline option in the server profile to the custom baseline and then select the Firmware and OS Drivers using Smart Update Tools installation method.

    This will make the driver packages available for installation on the Operating System using the HPE Smart Update Tools.

For more information on using HPE Smart Update Tools, see HPE OneView online help and SUT documentation at **Hewlett Packard Enterprise Support Center - Smart Update Manager Software**.

Using HPE Smart Update Manager to create a custom ISO on Windows

NOTE: HPE Smart Update Manager (SUM) starts an http server and initiates a browser to communicate to that server. Do not block Ports 63001–63002.

For more information, see the **Smart Update Manager User Guide**.

Procedure

1. Download a supported HPE Service Pack for ProLiant, HPE Synergy Service Pack, or HPE Synergy Custom SPP to use as a baseline. Mount the firmware bundle to a virtual CD drive.
2. Download all your required additional components (firmware and drivers) along with any required signature files.
3. Copy the downloaded files to a single local folder.
4. From the top-level folder of the mounted firmware bundle, run `.\launch_sum.bat` command. The Smart Update Manager opens in a browser.
5. Select Baseline Library from the main menu. The baseline inventory starts automatically. Wait for the inventory of the baseline to finish (the first inventory of this bundle from your local system takes more time).

   If the baseline inventory did not start automatically:

   a. Click Add Baseline and in the Location Details, enter the packages path from the mounted firmware bundle. (For example, F:\packages).

   b. Click Add. The baseline inventory is added.
6. Click Add Baseline to add the additional components folder as a Baseline (not Custom).
7. In the Location Details, enter the location of the additional components folder and then click Add.

   Confirm that all the expected additional components and versions are present.
8. Choose Actions and Create Custom option from the menu.
9. Enter the following options:
   - Description
   - Version
   - Output Location (requires an empty folder)
   - Make Bootable ISO file (yes-checked)
   - Extracted Source ISO Location (the top-level folder of the starting firmware bundle virtual CD)

   NOTE: Date is mandatory in the version string. Click the date to edit the date.
10. Ensure both the original and additional baselines are selected under Step 1–Baseline Sources.
11. **IMPORTANT:** Do not remove other components as that may result in the custom ISO unusable.

    Optionally, under Step 3– Review, click Apply Filters to confirm that your additional firmware and drivers are selected. If there are conflicting packages in the original baseline, you may clear them.
12. Click Create ISO and then click Save Baseline. The process will take significant time to complete.

    When the process is complete, the following message appears:

    ```
    Baseline has been saved successfully.  ISO creation was successful.  Baseline has been added successfully.
    ```

    You may close the dialog box without losing any changes. After the ISO file is created:

    - SUM will inventory the newly created firmware bundle.
    - The ISO file name will be bp-date-version.iso. You may rename the resulting ISO file. You do not have to retain the contents. The title of the mounted ISO will retain the original firmware bundle name.

- You can locate the ISO file in the Output Location along with its comprising contents. Optionally, search on a keyword or version to confirm that your additional components are part of the ISO inventory.

  At this point, you can mount a virtual CD to inspect the contents. You can also boot the ISO using an appropriate Compute module.

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 SNMP 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

Procedure

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 the previous step, 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.

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 configuring the Level of Data Returned value on the Administration > Management page.

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 with 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.

Procedure

1. To enable iLO to send SNMP traps:
   a. Navigate to the Administration > Management > SNMP Settings page.
   b. Configure the SNMP Settings, SNMP Alerts, and Insight Management Integration options.

      Enter the IP address of the HPE SIM computer in the SNMP Alert Destination(s) box.
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.

iLO and HPE SIM HTTP port matching requirement

HPE SIM is configured to start an HTTP session to check for iLO at the default Web Server Non-SSL Port (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, update the Web Server Non-SSL Port value on the Access Settings page.
- To change the port number in HPE SIM, add the port to the `config\identification\additionalWsDisc.props` file in the HPE SIM installation directory.

  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). The following 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 a 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.

Setting up 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

Procedure

1. Configure the iLO host name and domain name.
2. Install an iLO license to enable Kerberos Authentication .
3. Prepare the domain controller for Kerberos support .
4. Generate a Kerberos keytab file.
5. Verify that your environment meets the Kerberos authentication time requirement .
6. Configure the iLO Kerberos-specific parameters.
7. Configure directory groups.
8. Configure supported browsers for single-sign-on

Configuring the iLO hostname and domain name for Kerberos authentication

Use the following procedure if a DHCP server does not provide the domain name or DNS servers you want to use.

Procedure

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. To restart iLO, click Reset.

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 `SOMEDOMAIN.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.

Procedure

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

Procedure

1. Use the `Ktpass.exe` tool to generate a keytab file and set the shared secret.
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.

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 `kvno` 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 result is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. To close the window and continue creating the keytab file, click OK.

Setspn

Syntax

```
Setspn [options]
```

Description

The `Setspn` command 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 result 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.

Procedure

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

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 Microsoft Internet Explorer

Procedure

1. Enable authentication in Internet Explorer.
   a. Select Tools > Internet options.
   b. Click the Advanced tab.
   c. In the Security section, verify that the Enable Integrated Windows Authentication option is selected.
   d. Click OK.
2. Add the iLO domain to the intranet zone.
   a. Select Tools > Internet options.
   b. Click the Security tab.
   c. Click the Local intranet icon.
   d. Click the Sites button.
   e. Click the Advanced button.
   f. Enter the site to add in the Add this website to the zone box.

      On a corporate network, `*.example.net` is sufficient.
   g. Click Add.
   h. Click Close.
   i. To close the Local intranet dialog box, click OK.
   j. To close the Internet Options dialog box, click OK.
3. Enable the Automatic login only in Intranet zone setting.
   a. Select Tools > Internet options.
   b. Click the Security tab.
   c. Click the Local intranet icon.
   d. Click Custom level.
   e. In the User Authentication section, verify that the Automatic logon only in Intranet zone option is selected.
   f. To close the Security Settings - Local Intranet Zone window, click OK.
   g. To close the Internet Options dialog box, click OK.
4. If any options were changed in steps 1–3, close and restart Internet Explorer.
5. Verify the single sign-on configuration.

Enabling single sign-on in Mozilla Firefox

Procedure

1. Enter
   `about:config`
   in the browser location bar to open the browser configuration page.

   Firefox displays the following message:

   ```
   This might void your warranty!
   ```

2. Click the I accept the risk! button.
3. Enter
   `network.negotiate`
   in the Search box.
4. Double-click `network.negotiate-auth.trusted-uris`.
5. Enter the iLO DNS domain name (for example, `example.net`), and then click OK.
6. Verify the single sign-on configuration.

Single-sign on with Google Chrome

Configuration is not required for Google Chrome.

Enabling single sign-on in Microsoft Edge

Configuration is not required for Microsoft Edge.

Verifying the single sign-on (Zero Sign In) configuration

Procedure

1. Navigate to the iLO login page (for example, `http://iloname.example.net`).
2. Click the **Zero Sign In** button.

Verifying that login by name works

Procedure

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.

Directory integration 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)—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)—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 remember a new set of credentials for iLO.
- **Flexibility** (HPE Extended Schema)—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 range of IP addresses.
- **Compatibility**—iLO directory integration supports Active Directory and OpenLDAP.
- **Standards**—iLO directory support is based on the LDAP 2.0 standard for secure directory access. iLO Kerberos support is based on LDAP v3.

Choosing a directory configuration to use with iLO

Before you configure iLO for directories, 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—You are using OpenLDAP. The HPE Extended Schema is not currently supported with OpenLDAP.

     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 answers 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.

Schema-free directory authentication

When you use schema-free directory authentication, 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 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 multiple iLO systems at the same time.

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=EXAMPLE,DC=COM` for Active Directory, or `UID=username,ou=People,dc=example,dc=com` for OpenLDAP) 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=EXAMPLE,DC=COM`, is configured, iLO uses the following DN: `CN=JOHN.SMITH,CN=USERS,DC=EXAMPLE,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.

Configuring iLO for schema-free directory integration: Process Overview:

Procedure

1. Verify that your environment meets the prerequisites for using schema-free directory integration .
2. Configure the iLO schema-free directory parameters.
3. Configure directory groups.

Prerequisites for using schema-free directory integration

Procedure

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 license that enables Directory Service Authentication .
5. Verify that the correct DNS server is specified on the iLO network settings IPv4 or IPv6 page .

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.

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.

Configuring the HPE Extended Schema with Active Directory: Process overview

Procedure

Plan

1. Review the following:
   - Directory-enabled remote management (HPE Extended Schema configuration)
   - Directory services schema

Install

2. Complete the following steps:
   a. Verify that your environment meets the prerequisites for configuring Active Directory with the HPE Extended Schema.
   b. Install an iLO license to enable directory service authentication.
   c. 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.
   d. Use the Schema Extender to extend the schema.

Update

3. Set directory server settings and the DN of the management processor objects in the iLO web interface.

   You can also complete this step by using the Directories Support for ProLiant Management Processors software.

Manage roles and objects

4. Use the HPE Active Directory snap-ins to configure device and role objects:
   a. 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.

Handle exceptions

5. For complex role associations, consider using a directory scripting utility.

   The iLO utilities are easier to use with a single role. If you plan to create multiple roles in the directory, you might want to use directory scripting utilities, like `LDIFDE` or VBScript utilities. These utilities create complex role associations.

Prerequisites for configuring Active Directory with the HPE Extended Schema configuration

Procedure

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. Verify that version 3.5 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. Read the following Microsoft Knowledge Base article: 299687 MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed.

Installing the iLO directory support software

Procedure

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 3.5 or later on the target server.

   The .NET Framework 3.5 or later is used to install the Directories Support for ProLiant Management Processors software.
3. Double-click the downloaded EXE file.
4. Click Next.
5. Select I accept the terms in the license agreement , and then click Next.
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.
   e. Click Close.
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.
   e. Click Close.

   After the snap-ins are installed, you can create iLO objects and iLO roles in the directory. Install the snap-ins on each computer that will be used to manage directory objects. For more information, see Directory services objects.
8. To install the Directories Support for ProLiant Management Processors software, click Directories Support for ProLiant Management Processors.
   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.
   e. Click Close.

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 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

Procedure

1. Start the Management Devices Schema Extender from the Windows Start menu.
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 preference

   The Results window displays the results of the installation, including whether the schema was extended and the changed attributes.

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.

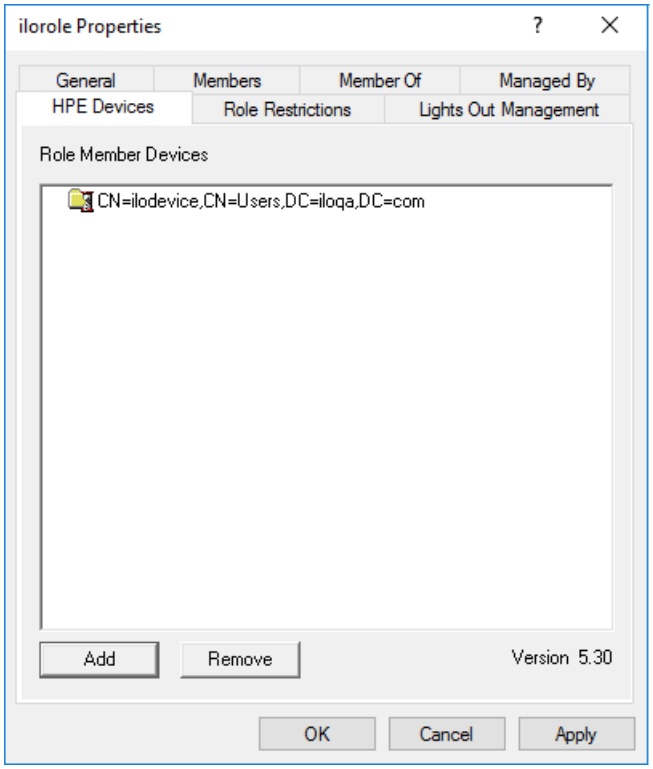
After the snap-ins are installed, iLO objects and iLO roles can be created in the directory. The following tasks are completed by using the Active Directory Users and Computers tool:

- Create iLO and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

Management options added by the HPE Active Directory snap-ins

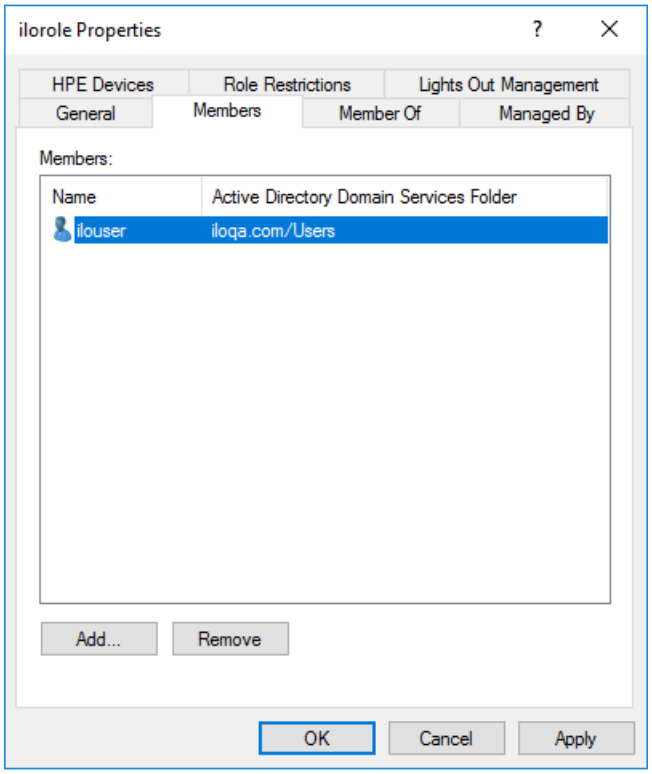
The following management options are available in Active Directory Users and Computers after you install the Hewlett Packard Enterprise snap-ins.

Devices tab



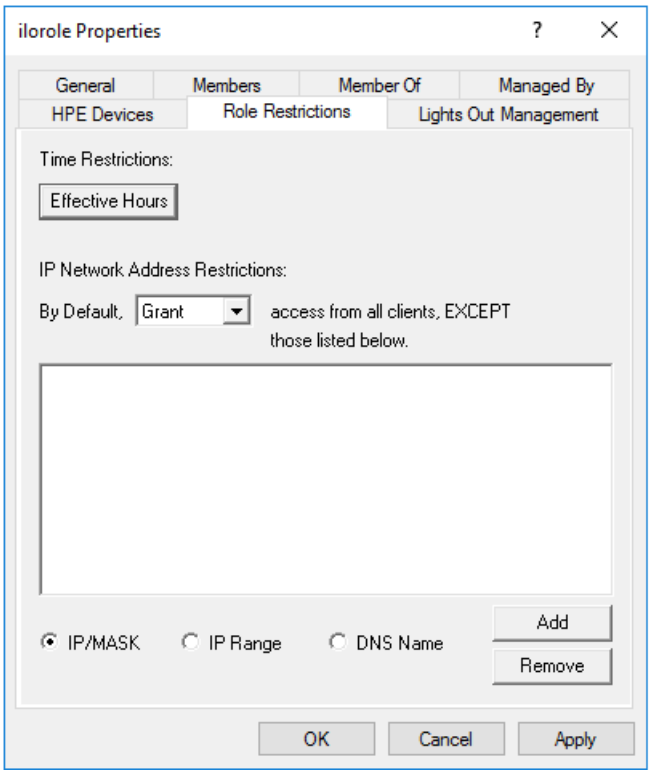
This tab enables you to add the Hewlett Packard Enterprise devices to be managed within a role. Clicking Add enables you to navigate to a device and add it to the list of member devices. Selecting an existing device and clicking Remove removes the device from the list of valid member devices.

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.

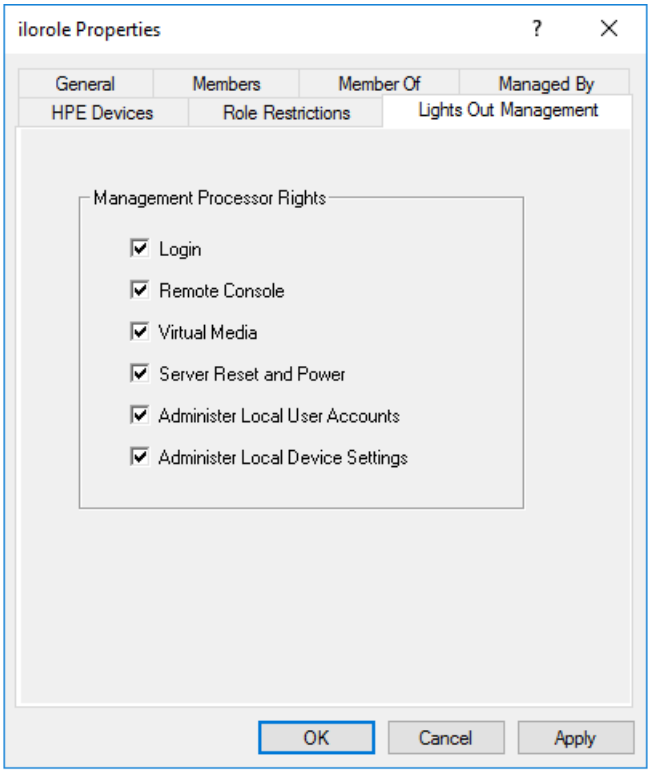
Role Restrictions tab



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. To change multiple squares, click and hold the mouse button, drag the cursor across the squares, and then release 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, if a user is in both the `remoteAdmins` and `remoteMonitors` roles, they have all available rights, because `remoteAdmins` has all rights.

The available rights follow:

- Login—Controls whether users can log in to the associated devices.

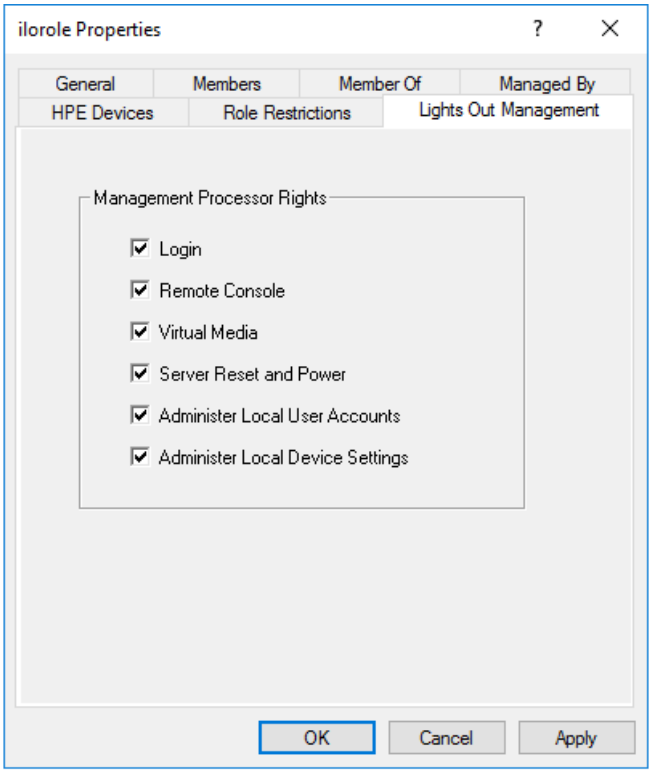
- Remote Console—Enables users to access the iLO Remote Console.
- Virtual Media—Enables users to access the iLO Virtual Media feature.
- Server Reset and Power—Enables users to use the iLO Virtual Power button.
- Administer Local User Accounts—Enables users to administer user accounts. Users can modify 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

Procedure

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.

Directory-enabled remote management (HPE Extended Schema configuration)

Directory-enabled remote management enables you to do the following:

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 using meaningful names for LOM device objects. For example, you could use 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. To provide more redundancy, you can use 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

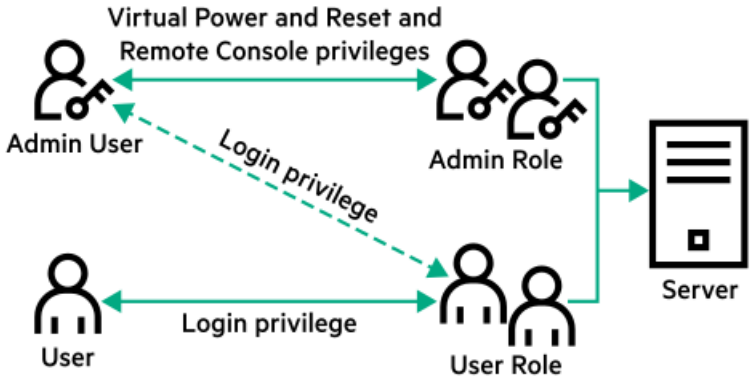
Most deployments do not require that the same user must be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can 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.

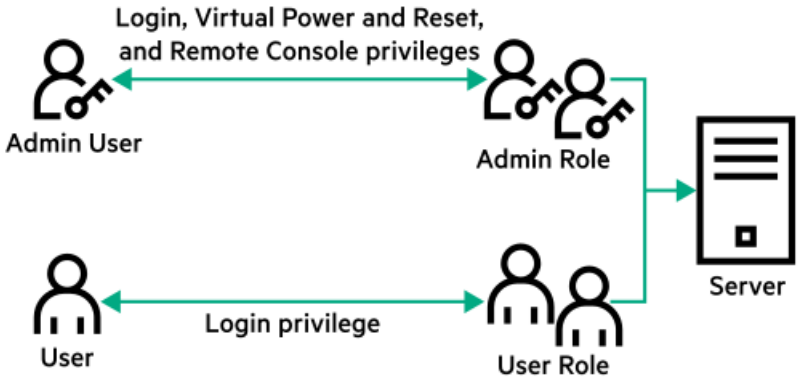
Figure 6: Multiple roles (overlapping) shows an example in which the Admin user gains the Login privilege from the User role, and advanced privileges are assigned through the Admin role.

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, as shown in Figure 7: Multiple roles (separate).

Figure 7: Multiple roles (separate)

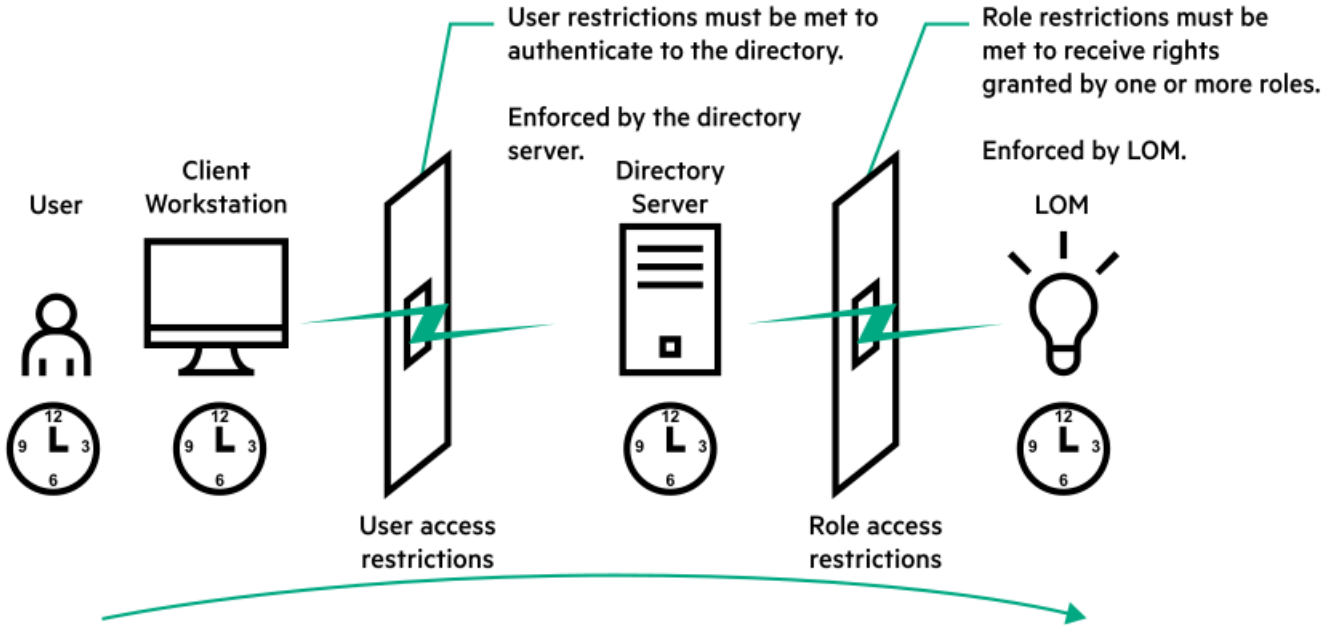


How role access restrictions are enforced

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 the ability of an authenticated user to receive LOM privileges based on rights specified in one or more roles.

Figure 8: Directory login restrictions



User access restrictions

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.

IPv4 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.

IPv4 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.

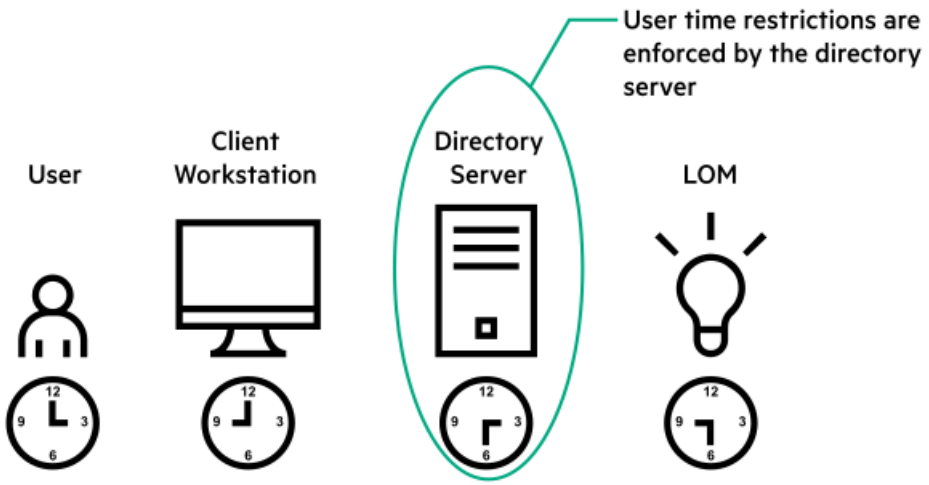
Using DNS-based restrictions might create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address 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


User time restrictions are enforced by the directory server
User
Client Workstation
Directory Server
LOM

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 with 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. SNTP allows the LOM device to compensate for leap years and minimizes 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

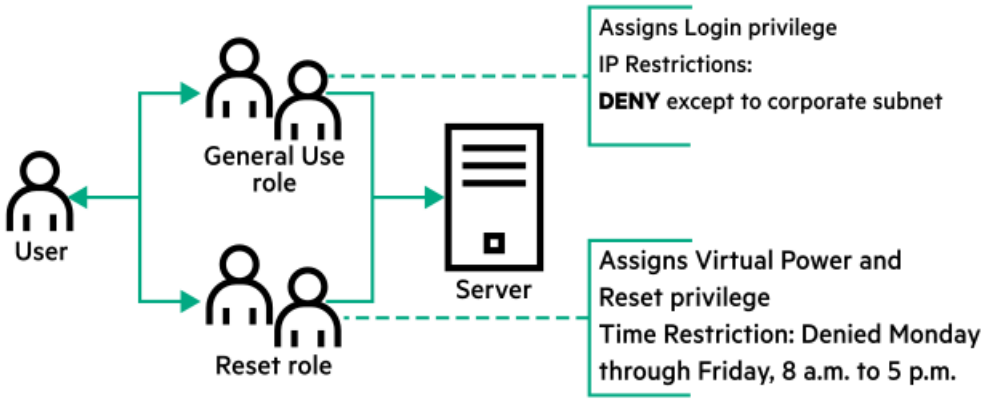
The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships 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: Creating restrictions and roles 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

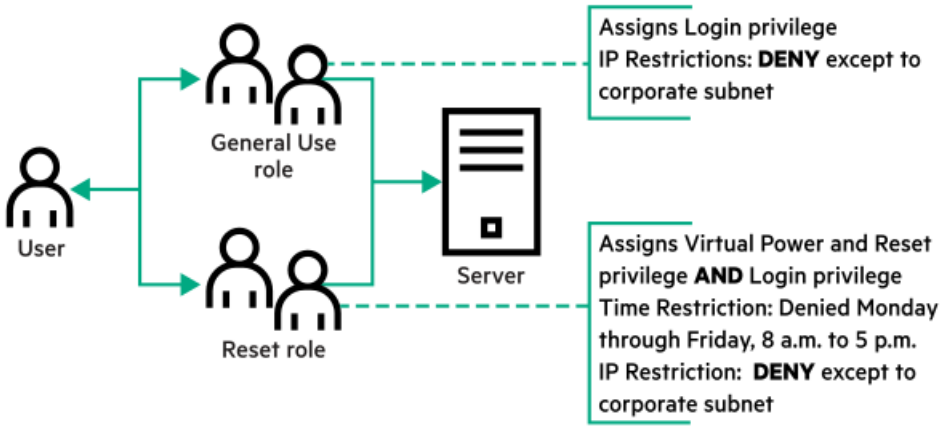


Alternatively, the directory administrator might create a role that grants the login right and restrict it to the corporate network, and then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous 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: Creating restrictions and roles 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: Restricting the Reset and General Use roles.

Figure 11: Restricting the Reset and General Use roles



Configuring Active Directory and HPE Extended Schema (Example configuration)

This procedure provides an example of how to configure Active Directory with the HPE Extended Schema.

Procedure

1. Verify that your environment meets the prerequisites for configuring Active Directory with the HPE Extended Schema.
2. Install an iLO license to enable directory service authentication.
3. Install the iLO directory support software.
4. Extend the schema by using the Schema Extender.
5. Configure device and role objects.
6. Log in to iLO and enter the directory settings on the Directory page.
7. Verify that the correct DNS server is specified on the iLO network settings IPv4 or IPv6 page.

Creating and configuring directory objects for use with iLO in Active Directory

The following example procedures describe 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 Active Directory Users and Computers snap-ins.

Procedure

1. Create the iLOs organizational unit and add LOM objects.
2. Create the Roles organizational unit and add role objects.
3. Assign rights to the roles and associate the roles with users and devices.

Creating the iLOs organizational unit and adding LOM objects

Procedure

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 HPE 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.

Creating the Roles organizational unit and adding role objects

Procedure

1. Create an organizational unit called Roles.
2. Right-click the Roles organizational unit, and then select New HPE 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**.

Assigning rights to the roles and associating the roles with users and devices

Procedure

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 HPE 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, and then click Apply.
5. Click the Members tab, and add users by using the Add button.
6. Click OK, and then click Apply.

   The devices and users are now associated.
7. Click the Lights Out Management tab.

   All users and groups within a role will have the rights assigned to the role on all the iLO devices that the role manages.
8. 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 iLO functionality.
9. Click OK.
10. To edit the remoteMonitors role, repeat the process:
    a. Add the rib-email-server device to the list on the HPE 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.

Configuring iLO and associating it with a Lights-Out Management object

Procedure

Enter settings similar to the following on the 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
```

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.

The maximum password length for LDAP user login is 63.

When you connect through the diagnostics port (on a blade server), 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 and OpenLDAP)

  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 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 Directory page.

Local users

Enter the Login Name of your iLO local user account.

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.

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 the Directory services schema.

Directories Support for ProLiant Management Processors (HPLOMIG)

HPLOMIG 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 is available from the following website: **http://www.hpe.com/support/ilo4**.

Operating system support

HPLOMIG runs on Microsoft Windows and requires the Microsoft .NET Framework version 3.5 or later. The following operating systems are supported:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Requirements

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 Server 2008 [1]	4.0 or earlier	Supported	Not Supported
	4.5	Supported	Not Supported
Windows 7 Windows Server 2008 R2	4.0 or earlier	Supported	Not Supported
	4.5	Supported	Supported
Windows 8 Windows 8.1 Windows 10 Windows Server 2012 Windows Server 2012 R2 Microsoft Windows Server 2016 Microsoft Windows Server 2019	4.0 or earlier	Supported	Not Supported

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
	4.5	Supported	Supported

[1] Windows Server 2008 does not support TLS v1.1 or v1.2, even if the NET Framework version 4.5 is installed.

Configuring directory authentication with HPLOMIG

Procedure

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. Complete the unique steps for your configuration:
   a. Name the management processors (HPE Extended Schema only)
   b. Configure the directory (HPE Extended Schema only)
   c. Configure the management processors to use the default schema (Schema-free only)
5. Configure communication between iLO and the directory.
6. Import an LDAP CA Certificate.
7. (Optional) Run the iLO directory tests.

Discovering management processors

Procedure

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.

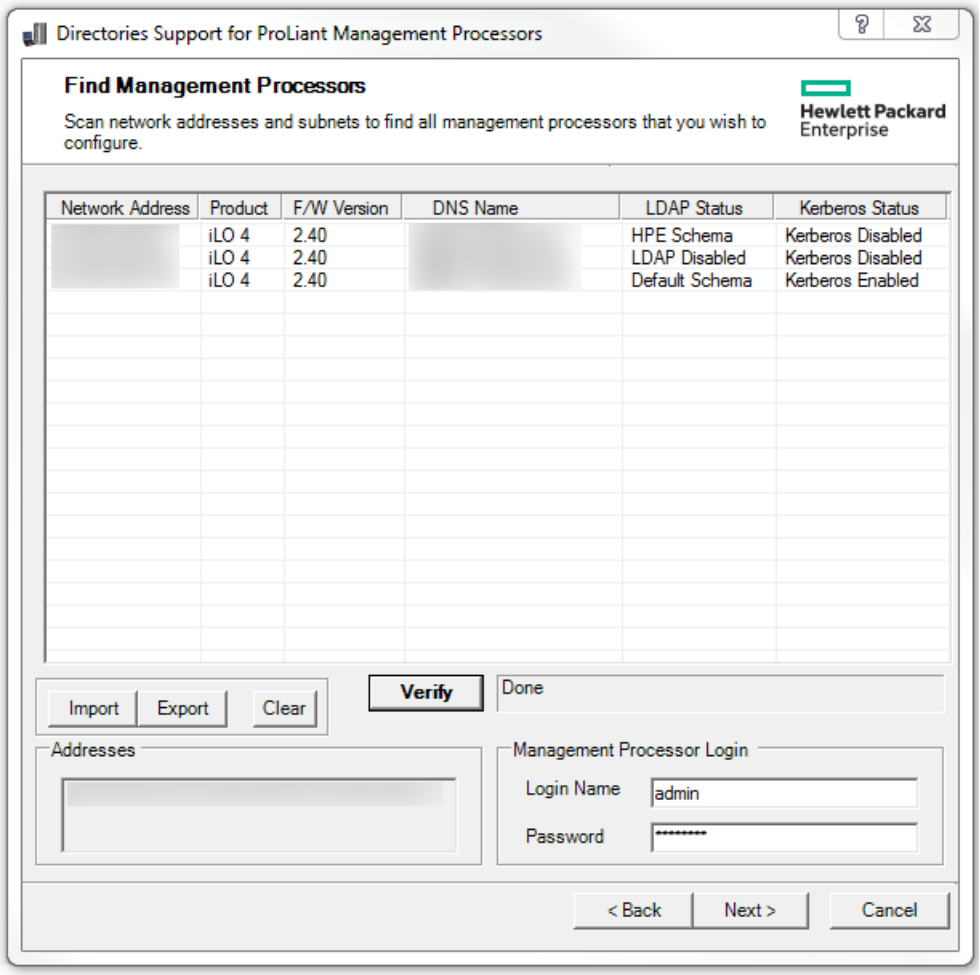
   TIP:

   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.



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 the user name and password cannot be included in the file (for security reasons), 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.

IMPORTANT:

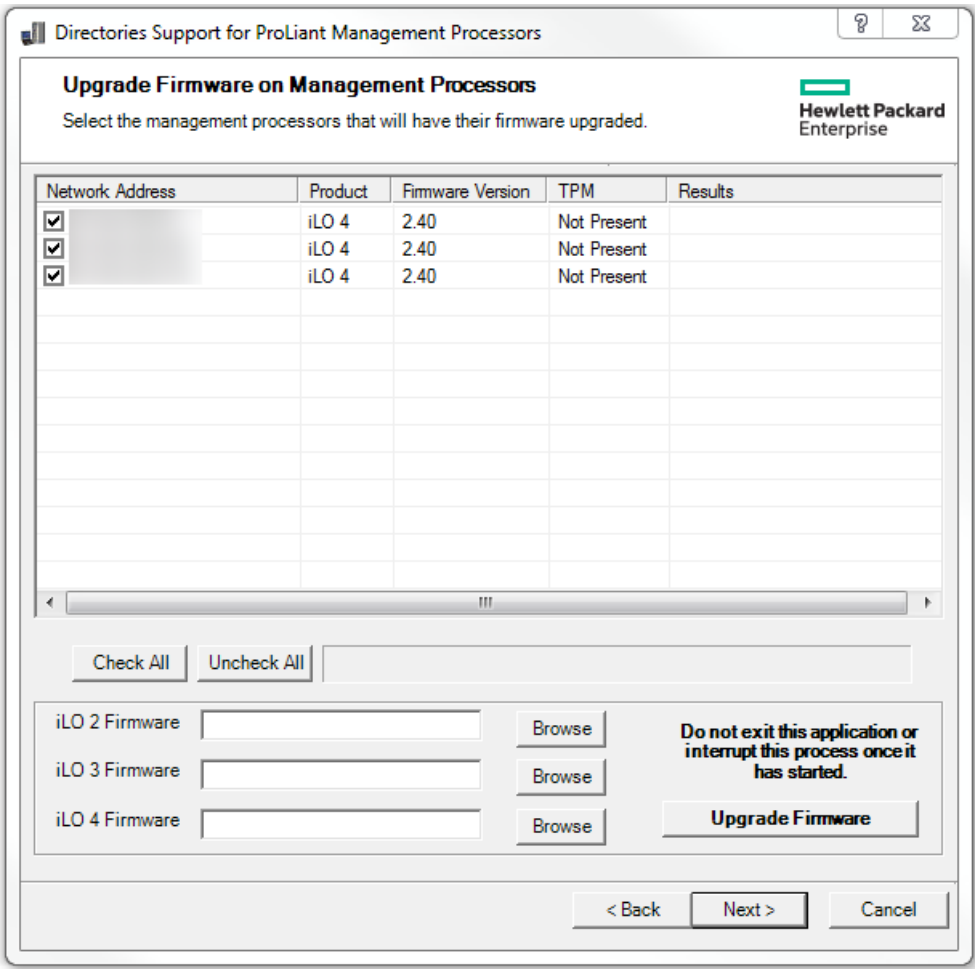
Before you run HPLOMIG on a production network, Hewlett Packard Enterprise recommends that you test the upgrade process and verify the results in a test environment. An incomplete transfer of the firmware image to a management processor might result in the need to reprogram the management processor locally.

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**.

Procedure

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.

   During the firmware upgrade process, all buttons are deactivated to prevent navigation.

   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.

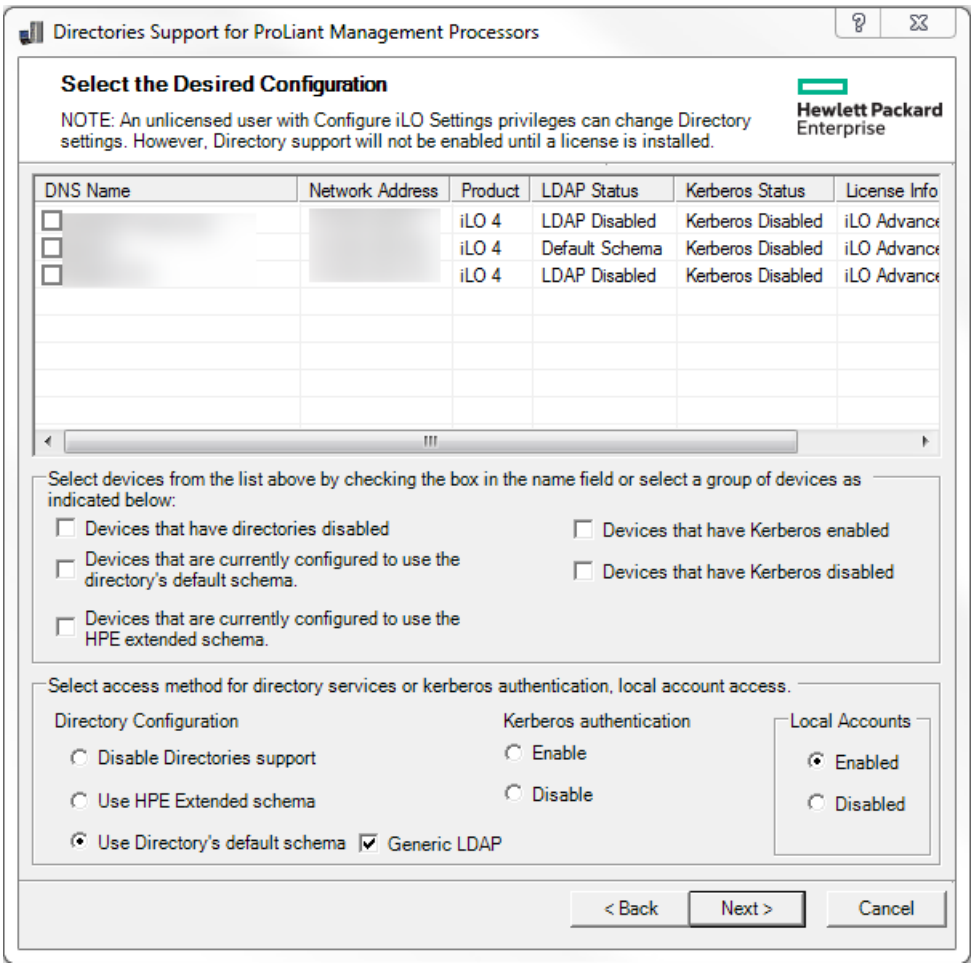
   If an upgrade fails, a message is displayed in the Results column, and the utility continues to upgrade the other selected management processors.
5. After the upgrade is complete, click Next.

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.

Procedure

1. Navigate to the Select the Desired Configuration window if it is not already open.



2. Select the iLO management processors to configure.
3. (Optional) Use the selection filters to exclude iLO management processors that are already configured for Kerberos authentication or directory services. You can also exclude management processors that have Kerberos authentication and directory services disabled.
4. Select the directory, Kerberos, and local account settings in the Directory Configuration, Kerberos authentication, and Local accounts sections.
5. Click Next.

   The selections you make on this page determine the windows that are displayed when you click Next.
6. If you selected a schema free configuration, skip to Configuring management processors (Schema-free configuration only). If you selected an HPE Extended Schema configuration, continue to Naming management processors (HPE Extended Schema only).

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.
- Generic LDAP—Use the OpenLDAP supported BIND method 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.

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.

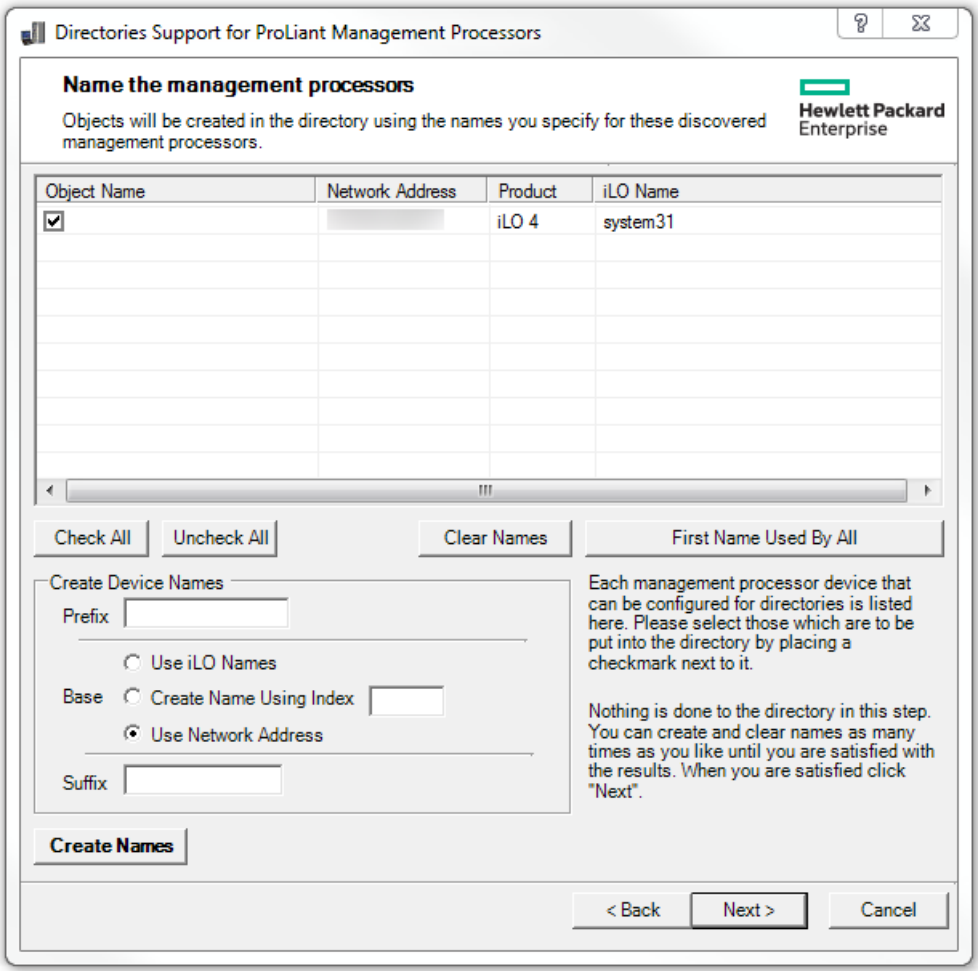
You can create names by using one or more of the following:

- 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:

Procedure

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.



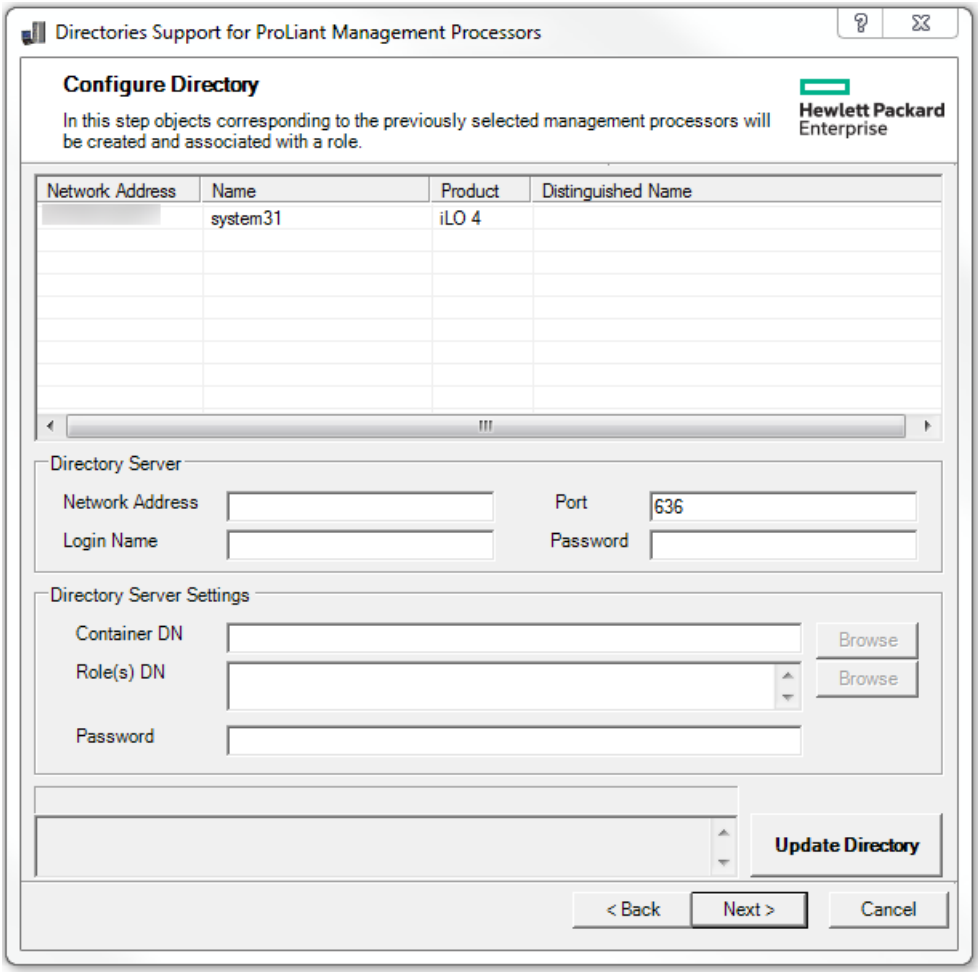
The names appear in the Object Name column as they are generated. At this point, names are not written to the directory or the management processors. The names are stored until the next Directories Support for ProLiant Management Processors window is displayed.

4. (Optional) To change the names, click Clear Names, and rename the management processors.
5. When the names are correct, click Next.

   The Configure Directory window opens. Continue with Configuring directories when HPE Extended Schema is selected .

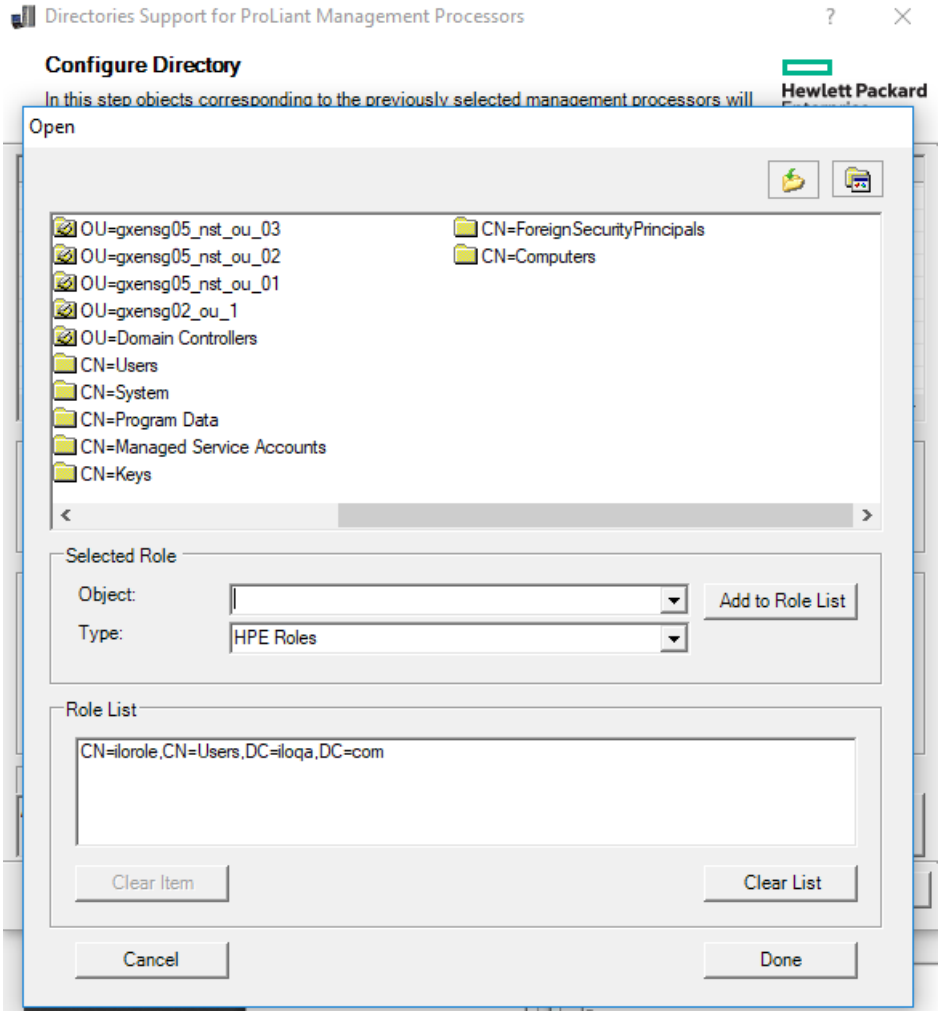
Configuring directories when HPE Extended Schema is selected

After you click Next in the Name the management processors window, 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.

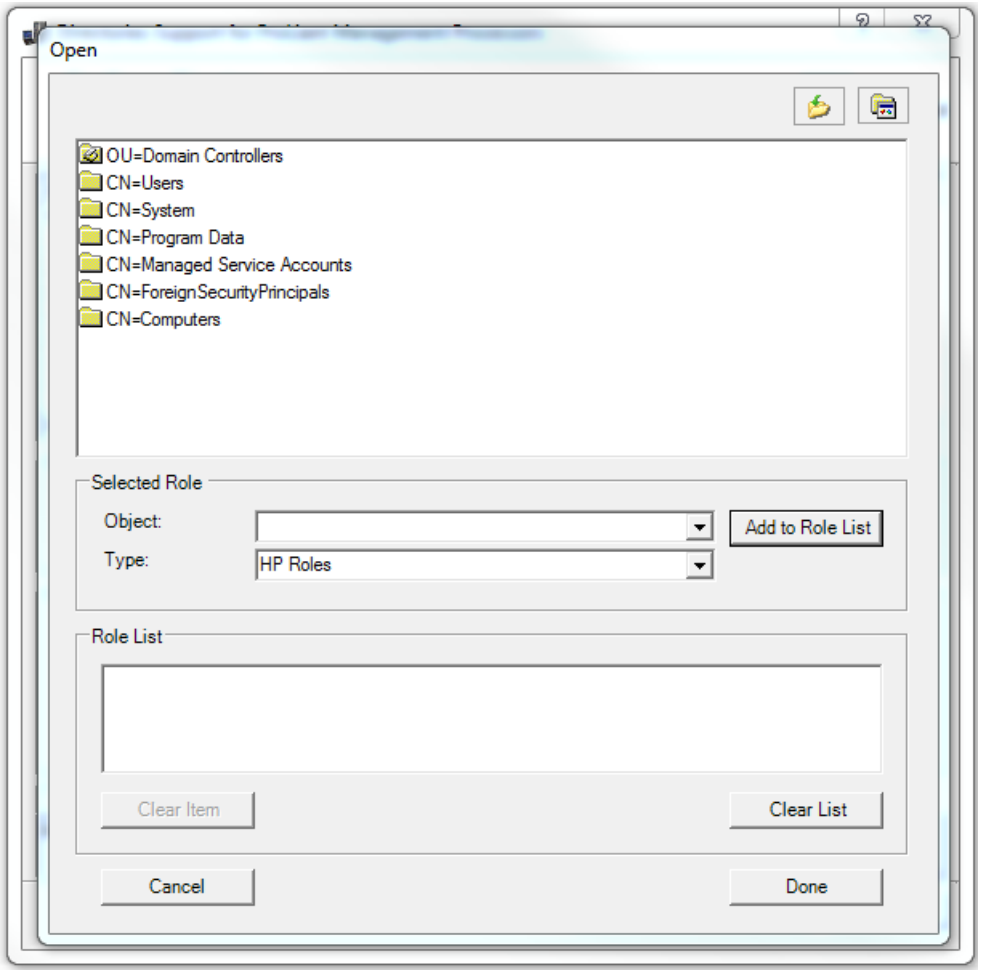


Procedure

1. In the Directory Server section, enter the Network Address, Login Name, and Password for the designated directory server.
2. Enter the Container DN value, or click Browse to select a container DN.



3. Enter the Role(s) DN value, or click Browse to select a role DN.

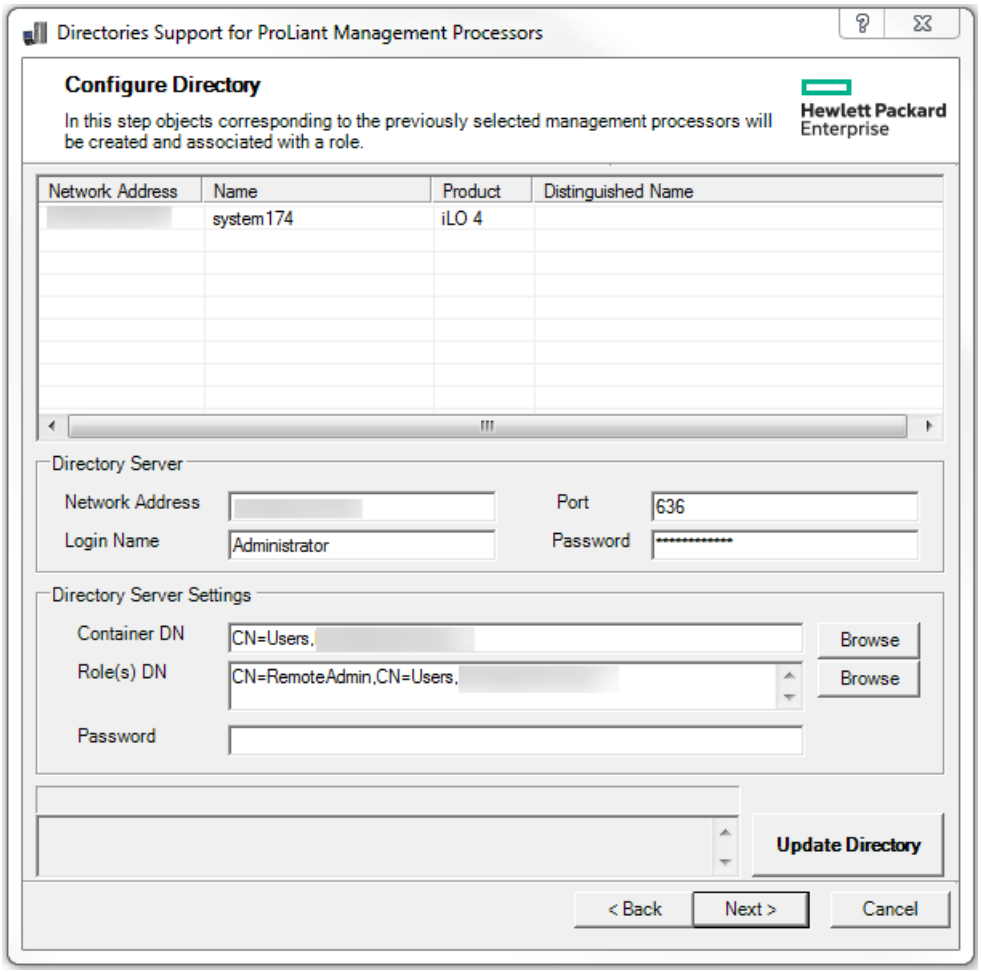


4. Click Update Directory.

HPLOMIG connects to the directory, creates the management processor objects, and adds them to the selected roles.

5. After the device objects have been associated to roles, click Next.

   The values you entered are displayed in the Configure Directory window.



6. Click Next.

   The Set up Management Processors for Directories window opens.

7. Continue with Setting up management processors for directories .

Configure directory window options

The boxes on the Configure Directory window follow:

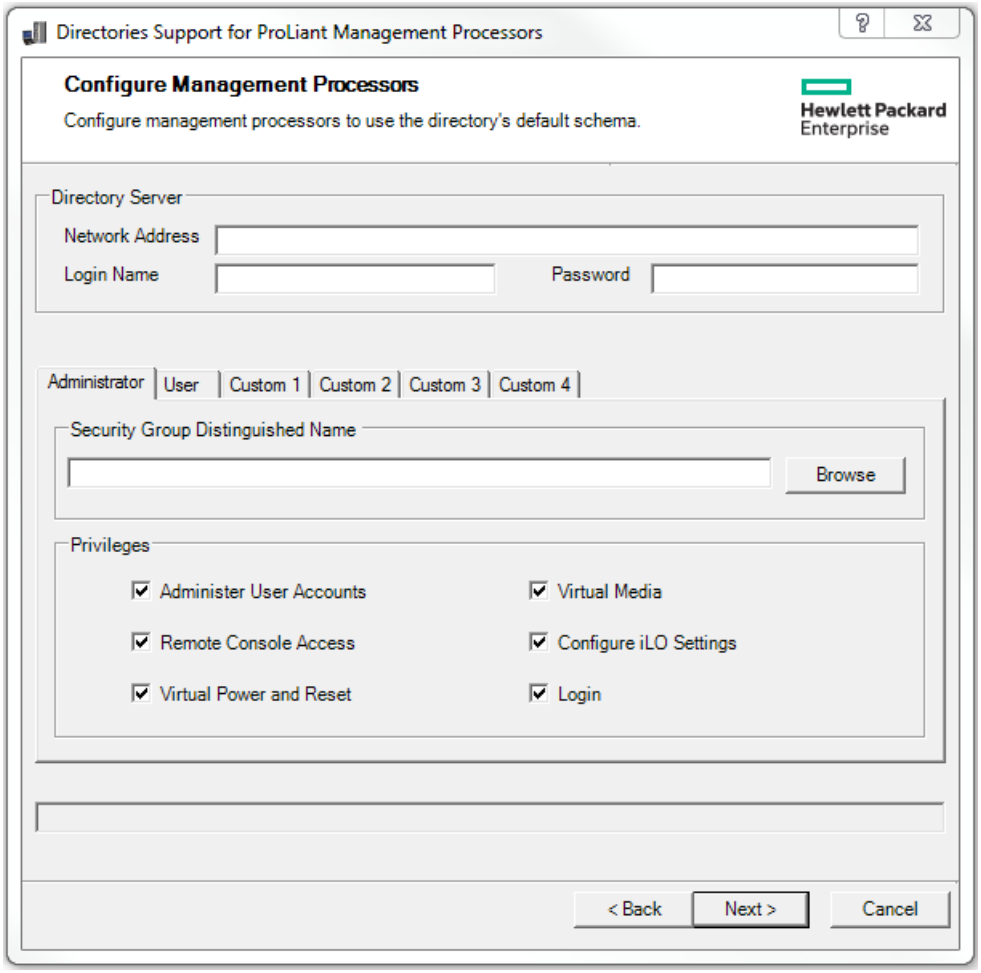
- Network Address—The network address of the directory server, which can be a valid DNS name or IP address.
- Port—The SSL port to the directory. The default port is 636. Management processors can communicate with the directory only by using SSL.
- Login Name and Password—Enter the login name and password 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.

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.

Procedure

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.

   The Set up Management Processors for Directories window opens.
6. Continue to Setting up management processors for directories .

Management processor settings

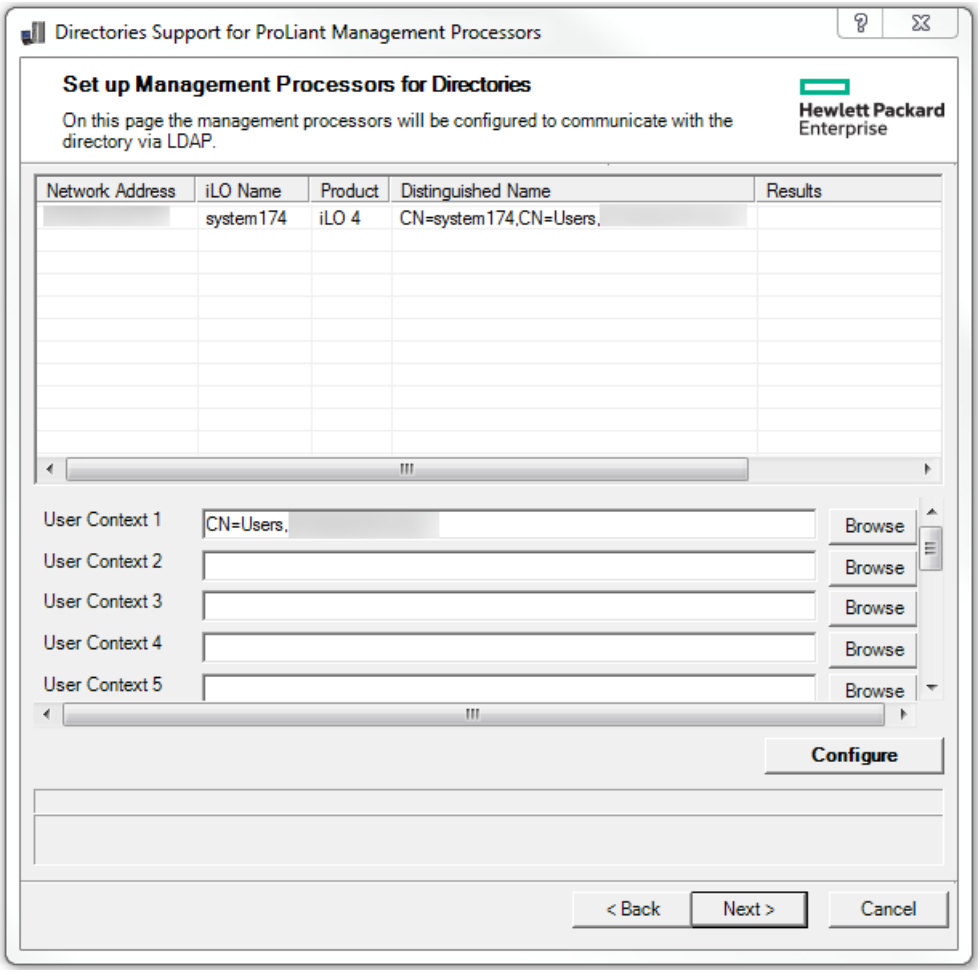
- Network Address—The network address of the directory server, which can be a valid DNS name or IP address.
- Login Name and Password—Enter the login name (DN) and password for an account that has domain administrator access to the directory.
- Security Group Distinguished Name—The DN of the group in 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 Configure Directory or Configure Management Processors window, the next step is to set up the management processors to communicate with the directory.

Procedure

1. Navigate to the Set up Management Processors for Directories window if it is not already open.
2. 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 in the User Context boxes, or click Browse to select user contexts.

Up to 15 user contexts are supported.

3. Click Configure.
4. When the process is complete, click Next

The LDAP CA Certificate Import window opens.

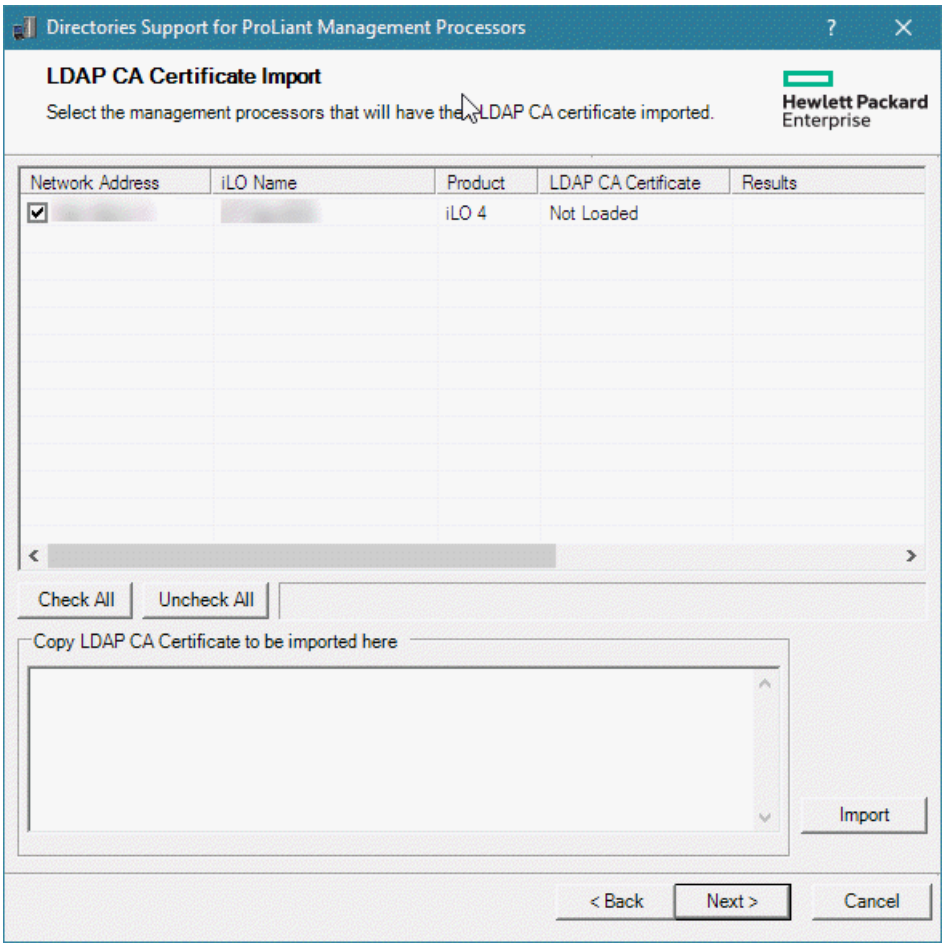
5. Continue with Importing an LDAP CA Certificate.

Importing an LDAP CA Certificate

After you click Next in the Set up Management Processors for Directories, the next step is to import LDAP CA Certificates.

Procedure

1. Navigate to the LDAP CA Certificate Import window if it is not already open.



2. Select the iLO systems for which you will import a certificate.
3. Paste the certificate in the text box, and then click Import.
4. When you are finished importing certificates, click Next.

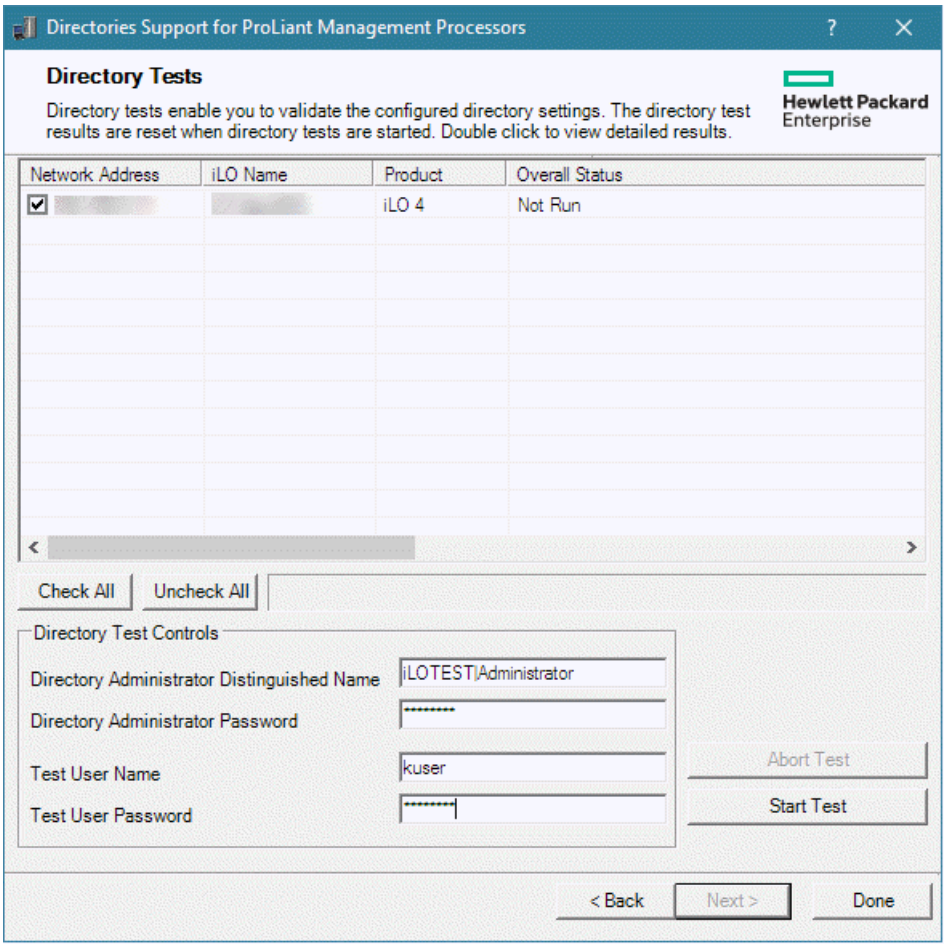
   The Directory Tests window opens.
5. Continue with (Optional) Running directory tests with HPLOMIG.

(Optional) Running directory tests with HPLOMIG

After you click Next in the LDAP CA Certificate Import, the next step is to test the directory configuration.

Procedure

1. Navigate to the Directory Tests window if it is not already open.

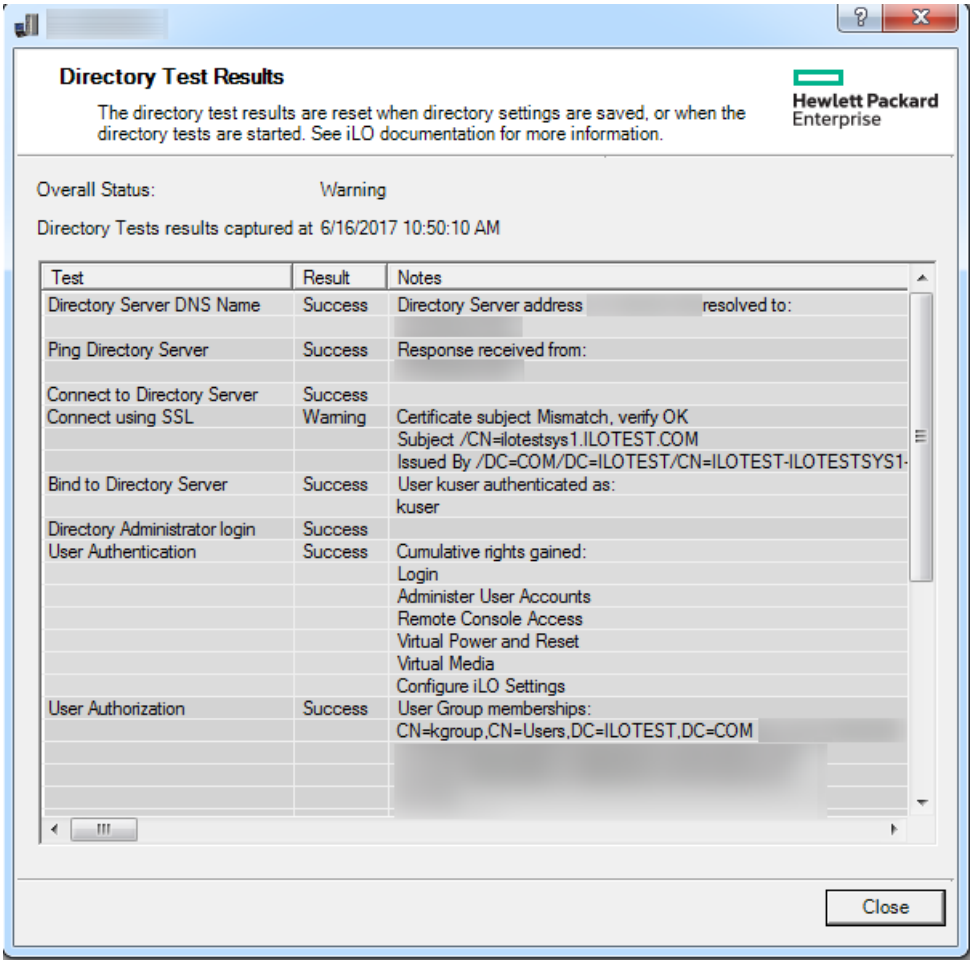


2. Test the directory settings.
   a. Select one or more iLO systems
   b. In the Directory Test Controls section, enter the following:
      - Directory Administrator Distinguished Name and Directory Administrator Password—Searches the directory for iLO objects, roles, and search contexts. This user 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.
3. To view the individual test results, double-click an iLO system.



For more information, see Running directory tests.

4. Click Done.

Directory services schema

The Directory services schema describes the classes and attributes that are used to store Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 `TRUE`, IP restrictions will be satisfied for unexceptional network clients. If this attribute is `FALSE`, 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	This attribute is used only on role objects. 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. Values are an identifier byte followed by a type-specific number of bytes that specify a network address. • For IP subnets, the identifier is <0x01>, followed by the IP network address in network order, followed by the IP network subnet mask in network order. For example, the IP subnet 127.0.0.1/255.0.0.0 would be represented as <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. For IP ranges, the identifier is <0x02>, 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 <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. • For DNS names or domains, the identifier is <0x03>, followed by the ASCII encoded DNS name. DNS names can be prefixed with an * (ASCII 0x2A), to indicate they must match all names that end with the specified string. For example, the DNS domain *.acme.com is represented as <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. 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	This attribute is used only on role objects. 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. • 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 Hewlett Packard Enterprise Management core classes and attributes.

Table 3: 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
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
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.6
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightConfigureSettings	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.

Table 4: 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 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 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 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 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 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.

Using the iLO mobile app

iLO mobile app features

- Operate the server power switch.
- Use a remote console to interact with the OS, including BIOS and ROM configuration changes.
- Mount an ISO CD/DVD image from an image file hosted on a web server (http or https). The disk image is available on the server as a USB CD/DVD drive. You can boot from the CD/DVD image and deploy an OS.
- Launch iLO scripts and monitor their progress.
- Access the iLO web interface.
- Store the list of servers you want to manage.

iLO mobile app limitations

- ProLiant servers with iLO 3 or later are supported. All ProLiant G7 and later servers are supported, except for ProLiant G7 100 series servers with Lights-Out 100i.
- You must have network access to the iLO systems you want to manage. When connecting from a cellular network, you might have to reconfigure a firewall or configure a VPN.

  You can connect through a firewall using a VPN or you can open or forward the following ports:

  - **HTTP:** Port 80
  - **HTTPS:** Port 443
  - **Remote Console:** Port 17990

  These ports are the default values. You can view or change the port settings on the Access Settings page in the iLO web interface.

  For information about how to use VPN functionality with your mobile device, see your device user guide.
- The following features require an iLO license on the server:
  - iLO virtual media
  - Remote console—This feature is included on blade servers. A license is required on all other servers.
  - Scripting—This feature is available on all servers. A license is required for the scripting of certain features such as iLO virtual media.

  For information about iLO licensing, see the iLO licensing guide at the following website: **http://www.hpe.com/info/ilo-docs**.
- The iLO mobile app can consume significant network bandwidth. When using the cellular network, monitor your data use if you do not have an unlimited data plan. Consider using Wi-Fi when possible.
- Acquiring the remote console and shared remote console are not supported through the mobile app.

Using the iLO mobile app on an Android device

Adding an iLO system to the mobile app

Procedure

1. Tap +Configure iLO on the Select iLO page.
2. Enter the iLO Network Address.

   You can use the iLO DNS name or IP address.
3. Enter the Login Name and Password for an iLO user account.
4. (Optional) To save the login credentials, set the Save Login Credentials option to Yes.

   The default value is Yes.

   Login credentials are saved only if the connection to iLO is successful.
5. (Optional) To add this iLO to the favorites list, set the Favorite option to Yes.

   The default value is Yes.
6. Tap Done to save this iLO and return to the list page.

   The iLO system is displayed in the list. After a successful connection, the system description is displayed beneath the network address.

Adding an iLO system to the mobile app by scanning a QR code

Procedure

1. Download and install a QR code generator.
2. Create a QR code with the code type set to **text**.
3. Enter the iLO network address, login name, and password in the following format: **address;login_name;password**.
4. Save the QR code image.
5. Start the iLO mobile app.
6. Tap +Configure iLO on the Select iLO page.
7. Tap Scan.
8. Use the device camera to scan the QR code.

   The network address, login name, and password from the QR code are displayed in the mobile app.
9. Tap Done to save the iLO system details.

   The iLO system is displayed in the list. After a successful connection, the system description is displayed beneath the display name or network address.

Editing the list of iLO systems

Procedure

1. Tap and hold an iLO system in the list on the Select iLO page.

   The app prompts you to edit or delete the selected iLO system.

2. Tap Edit.
3. Edit the iLO information, and then tap Done.

   The app prompts you to confirm the changes.

4. Tap Overwrite.

Deleting an iLO system from the list

Procedure

1. Tap and hold an iLO system in the list on the Select iLO page.

   The app prompts you to edit or delete the selected iLO system.

2. Tap Delete.

   The iLO system is removed from the list.

Viewing the list of iLO systems

Procedure

1. Open the iLO mobile app.

   The list of all iLO systems displayed.

2. (Optional) To view only the iLO systems in the Favorites list, tap Favorites.
3. (Optional) To view the iLO systems you have accessed, tap History
4. (Optional) To change the list order, drag the horizontal bar icon.

Starting the remote console

Prerequisites

The remote console is not in use.

Procedure

1. Tap an iLO system on the Select iLO page.
2. Tap Remote Console.
3. If prompted, enter the iLO login credentials.

Remote console usage

The iLO mobile app displays the server console in full screen mode with a virtual mouse and keyboard.

The remote console features are available from the status bar. If your device supports it, you can tap once with two fingers to show or hide the status bar.

- To access the keyboard, tap the keyboard icon.
- To access the iLO web interface, tap the server health icon. This icon represents the server health, and might be gray, green, yellow, or red.

  When you start the web interface, no additional login is required.

  To return to the remote console, tap X or tap the Back button.
- To access the virtual power switch, tap the power icon.
- To use the virtual media feature, tap the CD/DVD-ROM icon.
- To disconnect from iLO, tap X or tap the Back button.

  If you are idle for a specified amount of time, iLO disconnects your session. You can configure the time limit in the iLO web interface.

Mobile app keyboard usage

- Tapping the following keys is equivalent to pressing and holding down the key: Ctrl, Alt, Shift.

  When one of these keys is activated, it is displayed in green.

- Tapping the Home (Windows) key on Windows systems opens the Start menu.
- Tapping ?123 makes the following keys available:
  - Numbers and symbols
  - Cursor control keys
  - ESC
  - DEL

  To return to the standard keyboard, tap FN, and then tap ABC.

- Tapping ?123, and then tapping FN makes the following keys available:
  - Function keys
  - SysRq

  To return to the standard keyboard, tap ABC.

- Use the mobile app keyboard to enter special key commands not available on the standard keyboard.

  For example, tap ?123 to access the extended keyboard, and then tap the Ctrl, Alt, and DEL keys to enter Ctrl+Alt+Del.

Supported remote console gestures

- **Click or left-click**—Tap.
- **Left mouse button double-click** —Double-tap.
- **Right-click**—Tap and hold for 1 second.
- **Select and drag**—Touch and hold, then drag the selected item.
- **Zoom in or out**—Pinch the screen.
- **Pan**—Drag with two fingers.

Launching a script stored on a web server

Procedure

1. Tap an iLO system on the Select iLO page.
2. Tap Launch Script.

   Saved scripts are listed in the Select Script window.
3. (Optional) Add a script.
   a. Tap Add Script.

      The app prompts you to enter the full URL for an iLO RIBCL script.
   b. Enter the URL, and then tap OK to return to the Select Script page.
4. On the Select Script page, tap a script URL in the list.

   If you saved the iLO login information when you added the system to the mobile app, the app uses the saved credentials. If you did not save the iLO login credentials, the app uses the login credentials provided in the XML script.

   The script progress and results are displayed.

Starting the iLO web interface

Procedure

1. Tap an iLO system on the Select iLO page.
2. Tap iLO Web Interface.
3. When you are finished using the web interface, tap < iLOs to return to the iLO list page.

Clearing the iLO mobile app history

Procedure

1. Tap History to view the list of iLO systems accessed through the mobile app.
2. Tap Clear.
3. When prompted to confirm the request, tap OK.

Using the iLO mobile app on an iOS device

Adding an iLO system to the mobile app

Procedure

1. Tap the plus sign (+) icon on the iLO list page.
2. Enter the iLO network address.

   You can use the iLO DNS name or IP address.
3. (Optional) Enter a Display name to use for this iLO system within the mobile app.
4. (Optional) To use a display name, enable the Use display name option.

   The default setting is off.
5. Enter the Login name and Password for an iLO user account.
6. (Optional) To save the login credentials, tap the Save login credentials on/off switch.

   The default setting is off.

   Login credentials are saved only if the connection to iLO is successful.
7. (Optional) To specify whether you want to add this iLO to the favorites list, tap the Favorite on/off switch.

   The default setting is on.
8. Tap Save to save this iLO and return to the list page.

   The iLO system is displayed in the list. After a successful connection, the system description is displayed beneath the display name or network address.

Adding an iLO system to the mobile app by scanning a QR code

Procedure

1. Download and install a QR code generator.
2. Create a QR code with the code type set to **text**.
3. Enter the iLO network address, login name, and password in the following format: **address;login_name;password**.
4. Save the QR code image.
5. Start the iLO mobile app.
6. Tap the plus sign (+) icon on the iLO list page.
7. Tap Scan.
8. Use the device camera to scan the QR code.

   The network address, login name, and password from the QR code are displayed in the mobile app.
9. Tap Save to save the iLO system details.

   The iLO system is displayed in the list. After a successful connection, the system description is displayed beneath the display name or network address.

Editing the list of iLO systems

Procedure

1. Tap Edit on the iLO list page.
2. Tap the information (i) icon in the row of the iLO system you want to edit.

   The Edit iLO window opens.
3. Update the iLO details, and then click Save.
4. Click Done to return to the list of iLO systems.

Deleting iLO systems from the list

Procedure

1. Tap Edit.
2. Tap the row of each iLO system you want to delete.
3. Tap the trash can icon at the bottom left of the window.

   The app prompts you to confirm the request.
4. Tap Delete.
5. Tap Done to return to the list of iLO systems.

Viewing the list of iLO systems

Procedure

1. Open the iLO mobile app.

   The list of all iLO systems displayed.

2. (Optional) To view only the iLO systems in the Favorites list, tap Favorites.

3. (Optional) To view the iLO systems you have accessed, tap History

4. (Optional) To change the list order, tap Edit, and then drag the horizontal bar icon.

Starting the remote console

Prerequisites

The remote console is not in use.

Procedure

1. Tap an iLO system on the Select iLO page.
2. Tap Remote Console.
3. If prompted, enter the iLO login credentials.

Remote console usage

The iLO mobile app displays the server console in full screen mode with a virtual mouse and keyboard.

The remote console features are available from the status bar. You can tap once with two fingers to show or hide the status bar.

- To access the keyboard, tap the keyboard icon.
- To access the iLO web interface, tap the server health icon. This icon represents the server health, and might be gray, green, yellow, or red.

  When you start the web interface, no additional login is required.

  To return to the remote console, tap X.
- To access the virtual media feature, tap the CD/DVD-ROM icon.
- To access the virtual power switch, tap the power button icon.
- To disconnect from iLO, tap X.

  If you are idle for a specified amount of time, iLO will disconnect your session. You can configure the time limit in the iLO web interface.

Mobile app keyboard usage

- Tapping the following keys is equivalent to pressing and holding down the key: Ctrl, Alt, Shift.
- Tapping the Home (Windows) key on Windows systems opens the Start menu.
- Use the iLO mobile app keyboard functionality to enter special key commands not available on the standard keyboard.

  For example, to enter Ctrl+Alt+Del, tap Ctrl and Alt, and then tap Del.

Supported remote console gestures

- **Click or left-click**—Tap.
- **Show or hide the status bar** —Tap once with two fingers.
- **Left mouse button double-click** —Double-tap.
- **Right-click**—Tap and hold for 1 second.
- **Select and drag**—Touch and hold, then drag the selected item.
- **Zoom in or out**—Pinch the screen.
- **Pan**—Drag with two fingers.

Launching a script stored on a web server

Procedure

1. Tap an iLO system on the iLO list page.
2. Tap Scripting.

   Saved scripts are listed in the Select Script window.
3. (Optional) Add a script.
   a. Tap the plus symbol (+) icon.

      The app prompts you to enter the full URL for an iLO RIBCL script.
   b. Enter the URL, and then tap Done to return to the Select Script page.
4. On the Select Script page, tap a script URL in the list.

   If you saved the iLO login information when you added the system to the mobile app, the app uses the saved credentials. If you did not save the iLO login credentials, the app uses the login credentials provided in the XML script.

   The app prompts you to confirm that you want to run the script.
5. Tap Run.

   The script progress and results are displayed.

Starting the iLO web interface

Procedure

1. Tap an iLO system on the iLO list page.
2. Tap Home Page.
3. When you are finished using the web interface, tap the Back button to disconnect from iLO.

Clearing the iLO mobile app history

Procedure

1. Tap History to view the list of iLO systems accessed through the mobile app.
2. Tap Clear.
3. When prompted to confirm the request, tap Yes.

iLO mobile app feedback

Send feedback about the iLO mobile app to **iLO@hpe.com**.

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/**.

Procedure

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 ROM-based configuration utility starts.

5. Configure the following settings:

   - Disable EMS and BIOS Serial Console.
   - Set the Virtual Serial Port to `COM 2`.

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.

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 use the server video adapter to display 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.

Procedure

Use one of the following methods to access the Preboot Health Summary:

- Press the UID button on the server.

  CAUTION:

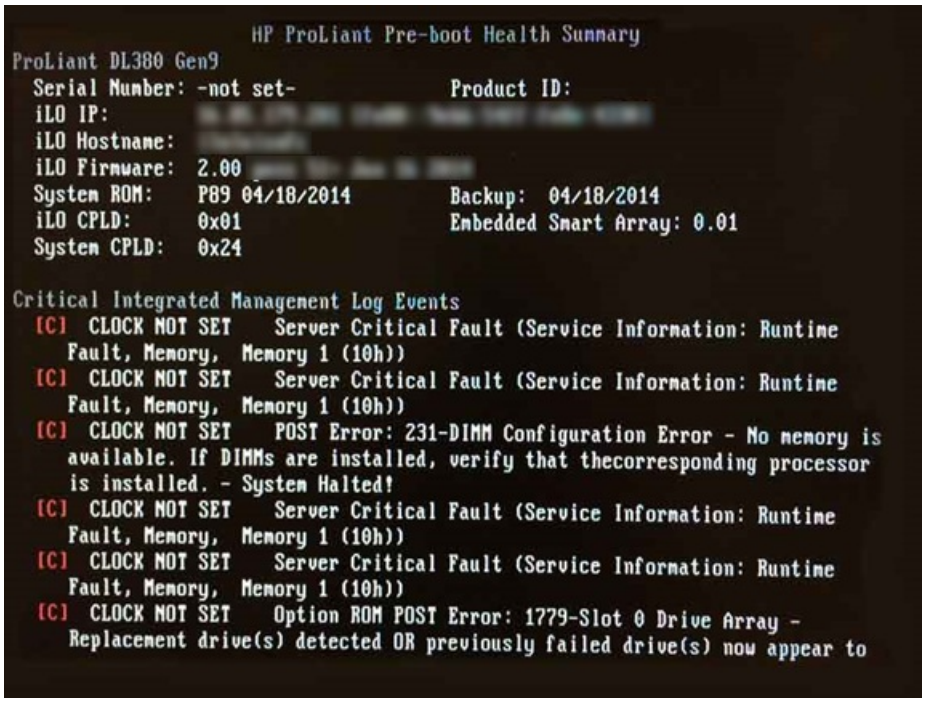
  To use this feature, press and release the UID button. Holding it down at any time for more than 5 seconds initiates a graceful iLO reboot or a hardware iLO reboot. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

- 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 is displayed until:

- The server is powered on.
- The UID state is changed to UID OFF.
- An SUV connector is removed.
- An iLO reboot completes.

Preboot Health Summary details

- 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.
- 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: https://www.hpe.com/support/hpesc.

Incorrect time stamp on iLO Event Log entries

Symptom

iLO Event Log entries have an incorrect date or time.

Cause

An SNTP setting is configured incorrectly.

Action

Verify that the NTP server addresses and time zone are correct.

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

- Verify that the user account exists and has the Login privilege.
- Change the user account password. Any user with the Administer User Accounts privilege can change the account password. If a login attempt fails after the password change, delete the invalid user account, and then add it again.
- 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 create a new administrator user account.
  - Use HPONCFG to create an administrator account. For more information, see the iLO scripting and command-line guide.

iLO management port not accessible by name

Symptom

The iLO management port is not accessible by name.

Cause

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. The environment is not configured to support accessing the iLO management port by name.

Action

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 is configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the required IP addresses.
- The iLO management port has a valid route to the WINS or DDNS server.
- The clients used to access the iLO management port are configured to use the same DDNS server where the IP address of the 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.

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

Set the SSL encryption level of your browser 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 iLO NIC teaming guidelines.

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.

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

- Use the ROM-based system utility to confirm that the NIC is enabled, and to verify the assigned IP address and subnet mask.

  For more information, see the ROM-based system utility documentation.
- 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. 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

Remove the self-signed certificate from the browser certificate store.

The self-signed certificate has iLO in the certificate name, and the Issued By value includes the text Default Issuer.

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.

See the browser documentation for more information about working with certificates.

Unable to connect to iLO IP address

Symptom

Cannot connect to iLO through the iLO IP address.

Cause

The web browser is configured to use a proxy server.

Action

To connect to iLO without using the proxy server, add iLO to the list of proxy server exceptions.

See the browser documentation for instructions.

iLO TCP/IP communication fails

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.

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 Certificates.
4. Click View Certificates.
5. Click the Servers tab, and then delete any certificates related to iLO.
6. Click the Others tab, and then delete any certificates related to iLO.
7. Click OK.
8. Start Firefox and connect to iLO.

Solution 2

Cause

The installed certificate contains the same serial number as another certificate issued by the certificate authority.

Action

1. Close Firefox.
2. Navigate to the Firefox `AppData` folder, and then delete all the `*.db` files in all the Firefox directories.

   The `AppData` folder is typically in the following location: `C:\\Users\<user name>\AppData\Local\Mozilla\Firefox\`

Security warning when navigating to iLO web interface with Internet Explorer

Symptom

When you navigate to the iLO web interface with Microsoft Internet Explorer, a security warning related to the website certificate is displayed.

Solution 1

Action

1. Depending on your version of Internet Explorer, do one of the following:
   - Click Continue to this website (not recommended).
   - Click More information, and then click the Go on to the webpage (not recommended) link.
2. Log in to iLO.

   When you use this solution, the text Certificate error is displayed in the browser address bar when you view the iLO web interface.

Solution 2

Action

1. Log in to iLO.
2. Navigate to the Administration > Security > SSL Certificate page.
3. Obtain and import an SSL certificate.
4. Reset iLO.

Certificate error when navigating to iLO web interface with Edge

Symptom

When you navigate to the iLO web interface with Microsoft Edge, the browser displays a message that says `This site is not secure`.

Solution 1

Action

1. Click Details.
2. Click Go on to the webpage.
3. Log in to iLO.

Solution 2

Action

1. Navigate to the Administration > Security > SSL Certificate page.
2. Obtain and import an SSL certificate.
3. Reset iLO.

Security warning when navigating to iLO web interface with Chrome

Symptom

When you navigate to the iLO web interface with Google Chrome, a security warning related to the website certificate is displayed.

Solution 1

Action

1. Click Advanced.
2. Click Proceed to *iLO host name* (unsafe).
3. Log in to iLO.

   When you use this solution, the text Not secure is displayed in the browser address bar when you view the iLO web interface and online help.

Solution 2

Action

1. Log in to iLO.
2. Navigate to the Administration > Security > SSL Certificate page.
3. Obtain and import an SSL certificate.
4. Reset iLO.

Security warning when navigating to iLO web interface with Firefox

Symptom

When you navigate to the iLO web interface with Mozilla Firefox, a security warning related to the website certificate is displayed.

Solution 1

Action

1. Click Advanced.
2. Click Accept the Risk and Continue.
3. Log in to iLO.

   When you use this solution, a warning icon is displayed in the browser address bar when you view the iLO web interface and online help.

Solution 2

Action

1. Log in to iLO.
2. Navigate to the Administration > Security > SSL Certificate page.
3. Obtain and import an SSL certificate.
4. Reset iLO.

iLO login page displays a Website Certified by an Unknown Authority message

Cause

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.
   a. 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.
   b. 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 login credentials to that imposter when you log in. Contact the administrator. To cancel the connection, exit the certificate window, and then click No or Cancel.
2. After verifying the items in the previous step, choose from the following options:
   - Accept the certificate temporarily for this session.
   - Accept the certificate permanently.
   - Stop now and import a certificate into your browser from a file provided by an administrator.

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. To confirm this cause, try to connect to iLO from the Safari browser on your iOS device.

Action

- 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 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. Configure a VPN on your device, 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.

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.

Running an XML script with iLO fails

Symptom

When you run an XML script against iLO, the session does not start or terminates unexpectedly.

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.

A certificate warning is displayed when you try to open the iLO online help in Microsoft Edge (legacy)

Symptom

A certificate error is displayed when you try to access the iLO online help in Microsoft Edge (legacy).

Cause

In Microsoft Edge (legacy) version 42 or later, your decision to trust an untrusted site certificate no longer applies to all windows within that site. Popup windows opened from links on the site, such as help topic windows, will prompt you to reauthorize the use of an untrusted certificate.

Action

Try the following solutions:

- Install a trusted certificate.
- Click the Details link, and then click Go on to the webpage to continue.

  This action will be required each time you access an online help page.
- Use a different browser.

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 file stored in iLO does not match the Active Directory key.
- iLO is configured for an incorrect 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.

Solution 3

Cause

There is a problem with the directory user account. Possible problems follow:

- 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.

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

Configure the browser to support Kerberos login.

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, 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

- Verify that the full DN of the user object exists in the directory.

  This information appears after the first `CN=` in the DN.

- Verify that 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.

A directory user account does not log out after the directory timeout expires

Symptom

A directory user is not logged out after the amount of time configured for the directory login timeout passes.

Cause

The iLO Idle Connection Timeout value is set to **Infinite** which keeps the iLO session from timing out. When the iLO session is active, the iLO firmware queries the directory periodically for user permissions. This query keeps the directory connection active, and prevents a user from being logged out based on the directory timeout settings.

Action

- Log out when you are finished using iLO.
- 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 in the `ktpass` command is formatted correctly.

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`

OpenLDAP authentication fails when configured with nested groups or posixgroups

Symptom

OpenLDAP authentication fails when the directory is configured with nested groups or posixgroups.

Cause

iLO does not support nested groups or posixgroups with OpenLDAP.

Action

Configure iLO with a group in which the LDAP user has a direct membership. Make sure the OpenLDAP directory group has an objectClass of the type groupOfNames.

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.

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

- Verify that the DNS server configured in iLO is correct.
- Verify that the directory server FQDN is correct.
- As a troubleshooting tool, use an IP address instead of the FQDN.
- 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

- Check to see if a firewall is active on the directory server.
- 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

- Verify that the configured directory server is the correct host.
- 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).
- 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

- 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

- Verify that the directory server allows anonymous binding.
- If you entered a user name in the test boxes, verify that the credentials are correct.
- 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`.
- Verify that the specified user is allowed to log in and is enabled.

Directory Administrator Login test reports a failure

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

- Verify that the user credentials were entered correctly.
- Try using other user name formats; for example, `user@domain.com`, `DOMAIN\username, username` (called Display Name in Active Directory), or `userlogin`.
- Verify that the specified user is allowed to log in and is enabled.
- 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

- Verify that the specified user name is part of the specified directory group.
- 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

- Verify that the LDAP FQDN of the LOM object is correct.
- Update the HPE Extended Schema and snap-ins in the directory server by using the HPLOMIG software.

Remote Console issues

The following sections discuss troubleshooting Remote Console issues.

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.

Caps Lock out of sync between Remote Console and client keyboard

Symptom

When you log in to the Remote Console, the Caps Lock setting is out of sync with the client keyboard.

Action

- In the .NET IRC or Java IRC: Select Keyboard > Caps Lock.
- In the HTML5 IRC: Click , and then click the virtual CAPS key.

Num Lock out of sync between Remote Console and client keyboard

Symptom

In a regular or shared Remote Console session, the Num Lock setting is out of sync with the client keyboard.

Action

- In the .NET IRC or Java IRC: Select Keyboard > Num Lock.
- In the HTML5 IRC: Click , and then click the virtual NUM key.

Session leader does not receive connection request when .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.

Keystrokes repeat unintentionally during 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.

The exact name of these settings varies depending on the OS you are using. For more information about changing the typematic delay and rate, see your OS documentation.

Cursor cannot reach Remote Console window corners

Symptom

The cursor cannot be moved to the corners of the Remote Console window.

Action

Right-click and drag the cursor outside the Remote Console window, and then drag it back inside.

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.

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.

File not present after copy from server to virtual media USB key

Symptom

If you copy files from a target server to an iLO virtual media USB key, the files are not visible in Windows Explorer on the client computer.

Cause

A user on a client computer cannot use Windows Explorer to view file changes on an iLO virtual media USB key.

Windows Explorer keeps a cached copy of the files on the USB key. The 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.
3. Connect the USB key by selecting it in the Virtual Drives menu.
4. Make file changes to the connected device (copy, delete, and so on).
5. To ensure that all data is updated on the device, unmount the device from the target server.
6. Use the remote console Virtual Devices menu to disconnect the USB key.

   Do not use Windows Explorer to refresh the contents of the USB key.
7. Use the Safely Remove Hardware feature to eject the USB key from the client computer.
8. Remove the USB key from the client computer.

   When you connect the USB key to any computer, the file changes will be visible in Windows Explorer.

Unable to boot to DOS using a USB key mounted with the Remote Console

Symptom

An error occurs when you try to boot to a DOS-bootable USB key that is mounted by using the 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
```

Cause

The Remote Console lacks sufficient privileges to access the boot sector of the USB key.

Action

- 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.

Remote Console hot key does not work in the HTML5 IRC

Symptom

Entering a Remote Console hot key in the HTML5 IRC does not work or produces unexpected results.

Cause

Your browser or client OS is mapped to use the key for something else.

For example, when you use Chrome, Ctrl+W closes the current tab.

Action

- Use a browser that does not use the same keyboard combination as your configured hot key.
- If your browser supports custom shortcuts, configure the browser to use a different keyboard combination.
- Configure a different hot key that does not conflict with your browser.
- Use the virtual CTRL key to enter the hot key command.
  1. Click , and then click and hold the virtual CTRL key.
  2. Type the rest of the keyboard combination on your client keyboard.

Pressing CTRL+ALT+DEL in the Remote Console affects only the client OS

Symptom

Pressing CTRL+ALT+DEL on the client keyboard affects the client OS and does not affect the server OS and Remote Console.

Action

- In the .NET IRC or Java IRC: Select Keyboard > CTRL-ALT-DEL.
- In the HTML5 IRC: Click , and then select CTRL+ALT+DEL.

Keyboard input has unexpected effects when using HTML5 IRC

Symptom

When using the HTML5 IRC, keyboard input has incorrect or unexpected results.

Cause

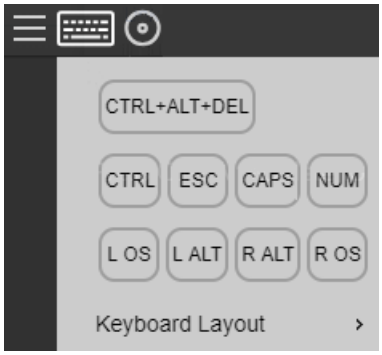
The key or keyboard combination you entered affected the client OS and the Remote Console, or only the client OS.

Action

- Define a Remote Console hot key for the keyboard combination you want to enter.
- Use the HTML5 IRC virtual keys to enter the keyboard action.
  - To press a virtual key, click , and then click a virtual key.
  - To enter a keyboard command with a virtual key, click , and then click and hold the virtual key. Type the rest of the keyboard command on your client keyboard.

    For example, to enter CTRL+W, click , click and hold the mouse on the virtual CTRL key, and then press W on your client keyboard.

  The following virtual keys are available:



  - CTRL—Control
  - ESC—Escape
  - CAPS—CapsLock
  - NUM—NumLock
  - L OS—Left OS-specific key
  - L ALT—Left ALT key
  - R ALT—Right ALT key
  - R OS—Right OS-specific key

.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. This situation causes the character to repeat continuously.

Action

Bring the Remote Console window to the front of your desktop by clicking the .NET IRC window.

.NET IRC becomes inactive or disconnects

Symptom

The .NET IRC becomes inactive or disconnects during periods of high activity. Console 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

- 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

- Reconnect to the .NET IRC and the Virtual Media.
- Reset 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 .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 .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.

.NET IRC takes a long time to verify application requirements (Internet Explorer)

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: Configure the proxy server settings.
6. Click OK to close the Local Area Network (LAN) Settings window.
7. Click OK to close the Internet Options window.
8. Close all browser windows.
9. Restart the browser, log in to iLO, and then start the .NET IRC.

.NET IRC displays a dialog box that says the application cannot be started (Internet Explorer)

Symptom

When you start the .NET IRC using Internet Explorer, the following message is displayed:

```
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
```

.

.NET IRC displays a dialog box that says the application cannot be started (new Microsoft Edge)

Symptom

When you start the .NET IRC using the new Microsoft Edge, the following message is displayed:

```
Cannot download the application. The application is missing required files. Contact
application vendor for assistance.
```

Cause

The browser is not configured to support ClickOnce.

> **WARNING:**
> This feature is available as an experimental Microsoft Edge browser feature. Use this experimental feature at your own risk. Before enabling this feature, read the Microsoft documentation to learn about the feature and any associated risks.

Action

1. In the new Microsoft Edge browser, navigate to `edge://flags`.
2. Search for `ClickOnce`.
3. Set ClickOnce Support to Enabled.

   Microsoft Edge notifies you that the changes take effect when you restart the browser.
4. Click Restart.

.NET IRC displays a dialog box that says the application is improperly formatted

Symptom

When you start the .NET IRC, the following message is displayed:

```
Cannot continue. The application is improperly formatted. Contact the application
vendor for assistance.
```

Cause

The client system you used to start the .NET IRC does not meet the minimum .NET Framework requirement.

In iLO 4 2.60 and later, the .NET IRC has a new SHA256 signing certificate. This certificate replaced the SHA1 signing certificates that were used for previous versions of the .NET IRC.

Version 4.5.1 or later of the .NET Framework is required to support the new certificate.

Action

Install .NET Framework 4.5.1 or later, and then retry the .NET IRC.

.NET IRC displays a security warning dialog box

Symptom

iLO displays the following security warning when you start the .NET IRC:

```
Your administrator has blocked this application because it potentially
poses a security risk to your computer.
```

Solution 1

Cause

The network administrator blocked ClickOnce applications from launching.

Action

Check with the system administrator for instructions.

Possible solutions include:

- Updating the network configuration to allow ClickOnce applications to launch.
- Using a different remote console such as the HTML5 console or a Java-based console.

Solution 2

Cause

A system update or application installation changed the .NET Framework security setting in the registry.

Action

1. Start the registry editor.

   CAUTION:

   Use the Registry Editor at your own risk and back up the registry before you modify it. If you use the Registry Editor incorrectly, serious issues might occur that could require reinstallation of the OS. For more information, see the Microsoft Knowledge Base Article 256986: Windows registry information for advanced users.

2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Security\TrustManager\PromptingLevel`.
3. Ensure that the `LocalIntranet` and `Internet` values are set to the default values (enabled).

.NET IRC cannot be shared

Symptom

When you try to join a shared .NET IRC session, the Unable to connect dialog box is displayed with the following message:

```
Unable to connect to shared IRC. This might be due to a firewall blocking port
<Remote Console Port number>.
```

Action

- Make sure that there is a communication path 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.

The .NET IRC will not start in the legacy version of Microsoft Edge

Symptom

When you start the .NET IRC in Microsoft Edge version 42 or later, the application fails to start. A Blocked content icon is displayed in the address bar.

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. In this configuration, the iLO web interface uses HTTPS, and the web interface starts the remote console by using HTTP. Microsoft Edge version 42 or later blocks the redirection and displays a Blocked content icon.

Action

Try one of the following solutions:

- Install a trusted certificate and enable the IRC Requires a Trusted Certificate in iLO setting on the Remote Console > Security page.
- Click the Blocked content icon in the address bar, and then click See all content.

  This action will authorize the blocked content for the current session.
- Use Internet Explorer to run the .NET IRC.
- Use the Standalone IRC.

  You can download the Standalone IRC from the following website: **http://www.hpe.com/support/ilo4**.
- Use the iLO mobile app.

The .NET IRC will not start in the new Microsoft Edge

Symptom

When you start the .NET IRC in the new Microsoft Edge, the application fails to start. No error message is displayed.

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. In this configuration, the iLO web interface uses HTTPS, and the web interface starts the remote console by using HTTP. The new Microsoft Edge blocks the redirection.

Action

Try one of the following solutions:

- Configure the browser to allow the connection.

  1. In the browser, navigate to `edge://settings/content/insecureContent`.
  2. Click Add.

     The Add a site window opens.
  3. Add the server hostname or IP address, and then click Add.

- Use Internet Explorer to run the .NET IRC.
- Use the Standalone IRC.

  You can download the Standalone IRC from the following website: **http://www.hpe.com/support/ilo4**.
- Use the iLO mobile app.

Mouse or keyboard does not work in the Integrated Remote Console

Symptom

The mouse or keyboard does not work in the Integrated Remote Console.

Solution 1

Action

For the .NET IRC or Java IRC (Java Web Start or Java Applet):

1. Close the Remote Console.
2. Navigate to the Power Settings page.
3. Clear the Enable persistent mouse and keyboard check box, and then click Apply.
4. Start the Remote Console.

Solution 2

Action

For the .NET IRC or Java IRC (Java Web Start or Java Applet):

Right-click and drag the cursor outside the Remote Console window, and then drag it back inside.

Solution 3

Action

For the Java IRC (Java Applet):

1. Close the browser window and exit the 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.

   Viewing your changes before you click Apply might reset the Runtime Parameters dialog box, causing your edits to be lost.
7. Start the browser and log in to iLO.
8. Start the Java IRC again.

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.

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

- 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.

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.

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

- 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 disable 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.

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. Log in to iLO with an account that has the Configure iLO Settings privilege.
2. Navigate to the Information > Diagnostics page.
3. Click Reset.

   Clicking Reset does not make any configuration changes, but it terminates any active connections to iLO and completes any firmware updates in progress.
4. 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 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.
   - For ProLiant Gen8 servers with iLO firmware earlier than 1.30: Navigate to the Remote Support > Data Collections page, and then click Send Data Collection. If you do not send Data Collection information manually, the server name is updated after the next automatic transmission. Data Collection information is automatically transmitted every 30 days.
3. If you had an active Insight Online session when you performed step 1, click the refresh button to update the Insight Online view with the server name.

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 operating system and the Agentless Management Service (AMS) were not running when the server was registered for remote support. In this situation, iLO cannot determine which OS is installed. To update the OS information, iLO must acquire the OS information from AMS.

Action

1. Verify the following:
   - A supported version of the iLO firmware 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 **https://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 Data Collections page in the iLO web interface.

   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 the previous step, click the refresh button.

   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.

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

- 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.

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

- 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.

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

- 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 iLOFederation 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.

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

- Verify that the iLO Client Applications use IPv6 first check box is not selected on the iLO Dedicated Network Port - IPv6 or page.

Firmware 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.

iLO firmware update error

Symptom

iLO notifies you that the last attempt to update the firmware was unsuccessful.

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

When an iLO firmware update is initiated, the update does not start and one of the following symptoms occurs:

- The firmware update status remains at 1%.
- The message `Checking HP Secure Digital Signature` is displayed.

Solution 1

Cause

The iLO web interface stopped responding.

Action

1. Refresh the browser window.
2. Retry the iLO firmware update.

Solution 2

Cause

The iLO firmware update process cannot make progress because other processes are consuming all available processing time.

Action

1. Shut down the server OS.
2. Disconnect the power cable from the server.
3. Wait for a few seconds and then reconnect the power cable.
4. Retry the iLO firmware update before starting the server OS.

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 that supports these features.

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 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 drivers must be installed.

Action

Install the iLO drivers.

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 > SNMP Settings page.

Server name 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 obtain the host name and update it on the iLO web interface page.

Action

- To update the server name, load the Insight Management Agents.
- Set iLO to the factory default settings.

  NOTE:

  This procedure clears all iLO configuration information, not just the server name.

- 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.

Action

1. Verify that AMS is installed.
2. Restart AMS.
3. Reset iLO.

OS installation from a Virtual Media device fails on a server that uses theiLO Shared Network Port

Symptom

An OS installation fails when you use a Virtual Media device to install the OS on a server that uses the Shared Network Port.

Cause

When the Shared Network Port is enabled, the iLO network connection depends on the server NIC. 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. The amount of time that iLO is unreachable depends on the NIC firmware. If the unreachable state is too long, the Virtual Media client stops trying to communicate with iLO and disconnects the session.

Action

- Retry the installation.
- Install the OS from physical media connected directly to the server.

Websites

iLO

http://www.hpe.com/info/ilo

iLO 4 Information Library

http://www.hpe.com/info/ilo-docs

iLO 4 Support

http://www.hpe.com/support/ilo4

iLO mobile app

http://www.hpe.com/info/ilo

Active Health System Viewer

http://www.hpe.com/servers/ahsv

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

SUM

http://www.hpe.com/info/sum-docs

SPP

http://www.hpe.com/info/spp/documentation

Intelligent Provisioning

http://www.hpe.com/info/intelligentprovisioning/docs

iLO RESTful API and RESTful Interface Tool

http://www.hpe.com/info/restfulinterface/docs

Remote Support

http://www.hpe.com/info/insightremotesupport/docs

HPE OneView

http://www.hpe.com/info/oneview/docs

OA

http://www.hpe.com/support/oa/docs

HPE SIM

http://www.hpe.com/info/insightmanagement/sim/docs

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  https://www.hpe.com/info/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  https://www.hpe.com/support/downloads

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter
- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

  https://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Pointnext Tech Care

https://www.hpe.com/services/techcare

HPE Complete Care

https://www.hpe.com/services/completecare

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.

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (located at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. All document information is captured by the process.