Hewlett Packard
Enterprise

HPE iLO 6 1.59 User Guide

Part Number: 30-7A345B12-016
Published: April 2024
Edition: 1

HPE iLO 6 1.59 User Guide

Abstract

This guide provides information about configuring, updating, and operating supported HPE ProLiant servers using the HPE iLO 6 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 6.

Part Number: 30-7A345B12-016
Published: April 2024
Edition: 1

Notices

Acknowledgments

Revision history

Part Number	Publication date	Edition	Summary of changes
30-7A345B12-016	April 2024	1	Updated information in the following sections: • Connecting to HPE Compute Ops Management
30-7A345B12-015	March 2024	1	Updated information in the following sections: • Configuring Compute Ops Management • Viewing the iLO Virtual Serial Port log

Part Number	Publication date	Edition	Summary of changes
30-7A345B12-014	February 2024	1	Updated information in the following sections: • Viewing storage information • iLO encryption settings • Prerequisites for initiating the One-button secure erase process • iLO backup and restore
30-7A345B12-013	January 2024	1	Support for a configuration that enables the disabling of all weak ciphers and key lengths for SSH and TLS interfaces in Production security mode.
30-7A345B12-012	December 2023	1	• Updates to Enabling the Production security states topic • Updates to iLO LDevID topic • Updates to Websites topic
30-7A345B12-011	November 2023	1	• Minor edits for RIBCL deprecation note • Added Rest Alerts 6125 and 6126
30-7A345B12-010	October 2023	1	iLO 6 1.53 release updates • Enabling and Disabling a user account • Updates for IPMI server management section • Updates for SSL cipher and MAC support section
30-7A345B12-009	September 2023	1	iLO 6 1.52 release updates • Updates to Unsupported features on HPE ProLiant RL3xx Gen 11 platform • Updates for Authorizing a new SSH key by using the web interface
30-7A345B12-008	August 2023	1	iLO 6 1.51 release updates • Updates for the Directory page to mention LDAP and Two Factor Authentication are mutually exclusive • Updated details for supported MAC for Production mode • Update to mention RL3xx platforms do not support IPMI over KCS
30-7A345B12-007	July 2023	1	iLO 6 1.50 release updates • Updates for Mail page to add support for Two Factor Authentication • Updates for Directory page to add support for Two Factor Authentication • Updates for Installing the iLO directory support software • Update for Firmware page for display Intel CPU CFR • Update for Network Access Settings page for IPMI over KCS
30-7A345B12-006	June 2023	1	iLO 6 1.45 release updates
30-7A345B12-005	May 2023	1	iLO 6 1.40 release updates
30-7A345B12-004	April 2023	1	iLO 6 1.35 is the combined release of iLO 6 for Gen11 Intel, AMD, and Ampere Platforms.
30-7A345B12-003	March 2023	1	iLO 6 1.30 is the combined release of iLO 6 for Gen11 Intel and AMD Platforms.

Part Number	Publication date	Edition	Summary of changes
30-7A345B12-002	January 2023	1	iLO 6 1.20 is the initial release of iLO 6 for Gen 11 Intel Platforms. iLO 6 1.20 supports Gen11 AMD platform also.
30-7A345B12-001a	January 2023	1	Updates to the front matter
30-7A345B12-001	December 2022	1	iLO 6 1.10 is the initial release of iLO 6 for Gen11 AMD platforms.

Table of contents

iLO

iLO 6 is a remote server management processor embedded on the system boards of supported HPE servers and 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.

Subtopics

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**—You can upload the log to HPE InfoSight for Servers to view the log data or create a support case for servers under a valid warranty or support contract. For more information, see the HPE InfoSight for Servers documentation at the following website: **https://www.hpe.com/support/infosight-servers-docs**.
- **Agentless Management**—With Agentless Management, 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.
- **Firmware management**—Manage firmware updates by using the iLO firmware features, including the iLO Repository, install sets, and the installation queue.
- **Firmware verification and recovery**—Run scheduled or on-demand firmware verification scans and configure recovery actions to implement when an issue is detected.
- **iLO backup and restore**—Back up the iLO configuration and then restore it on a system with the same hardware configuration.
- **iLO Federation management**—Use the iLO Federation features to discover and manage multiple servers at a time.
- **iLO interface controls**—For enhanced security, enable or disable selected iLO interfaces and features.
- **iLO RESTful API and RESTful Interface Tool (iLOREST)**—iLO 6 includes the iLO RESTful API, which is Redfish API conformant.
- **iLO Service Port**—Use a supported USB Ethernet adapter to connect a client to the iLO Service Port to access the server directly. Hewlett Packard Enterprise recommends the HPE USB to Ethernet Adapter (part number Q7Y55A). You can also connect a USB key to download the Active Health System Log.

- **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.
- **IPMI**—The iLO firmware provides server management based on the IPMI version 2.0 specification.
- **Learn more links**—Troubleshooting information for supported events is available on the Integrated Management Log page.
- **One-button secure erase**—Securely decommission a server or prepare it for another use.
- **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.
- **Secure recovery**—Validates the iLO firmware when power is applied. If the firmware is invalid, the iLO firmware is flashed automatically (iLO Standard license).

  Validates the system ROM during server startup. If valid system ROM is not detected, the server is prevented from booting. Recovery options include: Swapping the active and redundant ROM, and initiating a firmware verification scan and recovery action. The iLO Advanced license is required for scheduled firmware verification scans and automated recovery.
- **Security log**—View a record of the security events recorded by the iLO firmware.
- **Security dashboard**—View the status of important security features and evaluate your configuration for potential risks. When a risk is detected, you can view details and advice for how to improve system security.
- **Security states**—Configure a security state that fits your environment. iLO supports the Production security state (default) and higher security states such as High Security, FIPS, and CNSA.
- **Server health monitoring**—iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. It also monitors installed firmware and software versions and the status of other monitored subsystems and devices.
- **System diagnostics**—Diagnose a system by booting to safe mode or Intelligent Diagnostics mode. You can restore the default manufacturing settings or the default system settings.
- **Two-factor authentication**—Two-factor authentication is supported with Kerberos and CAC smart card authentication. You can also setup Two Factor Authentication for Microsoft Active Directory login users.
- **User access**—Use local or directory-based user accounts to log in to iLO. You can use CAC smart card authentication with local or directory-based accounts.
- Virtual NIC—Access iLO securely from the host OS.
- **Virtual media**—Remotely mount high performance Virtual Media devices to the server.
- Workload advisor—View selected server workload characteristics. You can view and configure recommended performance tuning settings based on the monitored data.
- **Workload matching**—Enables the use of preconfigured workload profiles to fine-tune server resources.

Unsupported features on HPE ProLiant RL3xx Gen 11 (Ampere based) platform

iLO 6 v1.05 is supported on Ampere (RL300) based platform. (iLO 6 v1.10, v.1.20, and v1.30 based firmware is not compatible with Ampere (RL300) based platforms).

iLO 6 v1.35 or later versions are single firmware images applicable across Intel, AMD, and Ampere based platforms.

NOTE:

On HPE ProLiant RL300 Gen 11 platforms, for upgrading iLO 6 v1.05 to iLO 6 v1.35 or later, follow the below steps:

1. Update System ROM from v 1.12 to v1.20 or later from iLO 6 user interface.
2. Update iLO 6 1.05 to iLO 6 v1.35 or later

In case System ROM is not updated as mentioned in Step1 and if the iLO version is v1.35 or later, the system will not boot.

In such case of system halt at boot with System ROM v1.12, the recovery mechanism is either to downgrade System ROM to v1.10 or upgrade to v1.20 from iLO 6 user interface.

The Ampere based platforms (HPE ProLiant RL3xx Gen 11) support most of the iLO 6 firmware features with the following exceptions:

Unsupported OS	Unsupported options	Products not supporting RL300	Unsupported features
• MS Windows Server • SUSE Linux Enterprise Server • VMWare	• SR and MR Storage Controllers • Intel VROC • SATA and SAS drives (SSD and HDD) • Server Platform Services (SPS) firmware • HPE Smart Options (including Smart Array Encryption, Software RAID, and HPE SmartMemory) • TPM 1.0 • Intel PMEM support • Restore Last Power State	• HPE OneView • HPE InfoSight for Servers • iLO Amplifier Pack • Intelligent Provisioning (IP) • Service Pack for ProLiant (SPP) • iLO Scripting and Command Line Toolkit (RIBCL) • SIM • Smart Update Manager (SUM) and Smart Updated Tool (SUM)	• One Button Secure Erase • FIPS and CNSA security states • iLO Federation • IPMItool in-band interface • Platform Level Data Model (PLDM) based firmware updates • Power Capping • Insight Remote Support • Workload Profiles • Workload Advisor • Serial Over LAN Console • Shared Network Port configuration • Processor Jitter control • Power Regulator Mode • HPE Performance Telemetry • Secure Protocol and Data Model (SPDM) • Insight Remote Support • Enterprise Secure Key Manager (ESKM) • On Demand scan • WakeOnLAN • Generating NMI

For more information on getting started and using HPE ProLiant RL3xx Gen 11 platforms, go to: **https://www.hpe.com/info/rl300gen11-docs**.

iLO web interface

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

More information

iLO web interface overview

ROM-based configuration utility

You can use the iLO 6 Configuration Utility in the UEFI System Utilities to configure network parameters, global settings, and user accounts.

The iLO 6 Configuration Utility is designed for the initial iLO setup, and is not intended for continued iLO administration. You can start the utility when the server is booted, and you can run it remotely with the Remote Console.

You can configure iLO to require users to log in when they access the iLO 6 Configuration Utility, or you can disable the utility for all users. These settings can be configured on the Access Settings page. Disabling the iLO 6 Configuration Utility prevents reconfiguration from the host unless the system maintenance switch is set to disable iLO security.

To access the iLO 6 Configuration Utility, press F9 during POST to start the UEFI System Utilities. Click System Configuration, and then click iLO 6 Configuration Utility.

More information

Configuring iLO access settings

iLO RESTful API

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

To learn more about the iLO RESTful API, see the Hewlett Packard Enterprise website (**https://www.hpe.com/support/restfulinterface/docs**).

For specific information about automating tasks using the iLO RESTful API, see libraries and sample code at **https://www.hpe.com/info/redfish**.

For more information, watch the **Redfish & How it works with HPE Server Management** video.

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.

HPE ProLiant RL3xx Gen 11 platforms do not support iLO Scripting and Command Line Toolkit (RIBCL).

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**.

iLO Amplifier Pack does not support HPE ProLiant RL3xx Gen 11 platforms.

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**.

HPE InfoSight for Servers do not support HPE ProLiant RL3xx Gen 11 platforms.

Setting up iLO

Subtopics

Preparing to set up iLO

About this task

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

Subtopics

iLO network connection options

NIC teaming with Shared Network Port configurations

iLO IP address acquisition

iLO access security

iLO configuration tools

Other iLO configuration tools

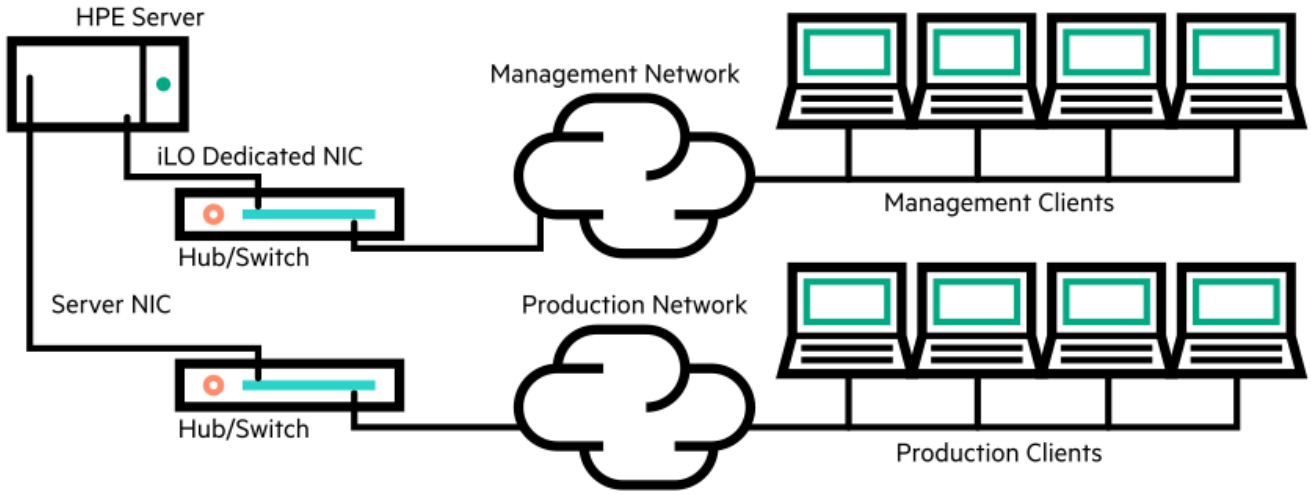
iLO network connection options

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

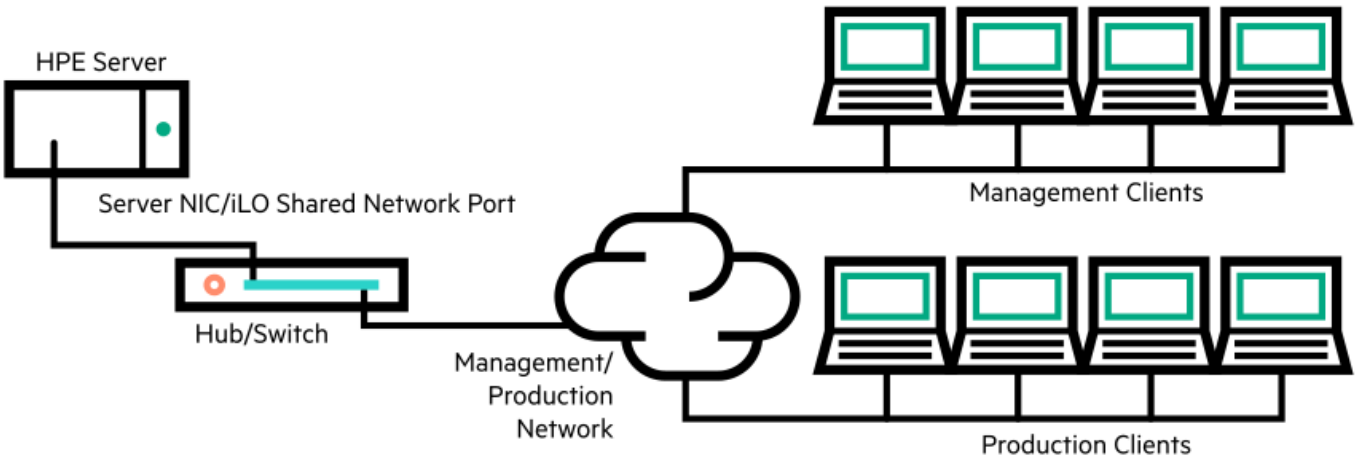
In this configuration, both the NIC and the iLO port are connected to the production network. In iLO, this type of connection is called the Shared Network Port configuration. Certain Hewlett Packard Enterprise embedded NICs and add-on cards provide this capability. This connection enables access to iLO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



iLO network enablement module

Some servers require an optional iLO network enablement module to add support for remote management through a dedicated management network (default) or a shared network connection. If an iLO network enablement module is not installed, iLO access is supported only through host-based (in-band) access methods. Some examples of the supported host-based access methods include the iLO RESTful API, UEFI System Utilities, iLO Service Port (if available), and the Virtual NIC.

To review the network connections your server supports, see the server user guide.

NIC teaming with Shared Network Port configurations

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

Subtopics

NIC teaming constraints

Hewlett Packard Enterprise NIC teaming modes

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 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 the iLO 6 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.

CAC smart card authentication

You can configure common access smart cards together with local accounts and directory services to manage iLO user access.

More information

Directory authentication and authorization settings in iLO
iLO user accounts
CAC Smartcard Authentication
Configuring iLO access settings

iLO configuration tools

iLO supports various interfaces for configuration and operation. The primary interfaces discussed in this guide include the following:

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.

ROM-based setup

Use the iLO 6 Configuration Utility when the system environment does not use DHCP, DNS, or WINS.

Other iLO configuration tools

iLO configuration options discussed in other guides include the following:

Intelligent Provisioning

To start Intelligent Provisioning, press F10 during POST.

You can also access Always On Intelligent Provisioning through the iLO web interface. For more information, see the Intelligent Provisioning user guide.

HPE ProLiant RL3xx Gen 11 platforms do not support Intelligent Provisioning.

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 the following website: **https://www.hpe.com/info/redfish**.

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.

HPE OneView does not support HPE ProLiant RL3xx Gen 11 platforms.

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 to set up 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 RIBCL 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.
- **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.

NOTE:

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

iLO sample scripts are available at Hewlett Packard Enterprise **website** .

Initial setup steps

About this task

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

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 Adding user accounts (iLO 6 Configuration Utility).
5. If necessary, install the iLO drivers.
6. (Optional) Install an iLO license.

   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: **https://www.hpe.com/support/ilo-docs**.

Connecting iLO to the network

About this task

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.

More information

iLO network connection options

iLO setup with the iLO 6 Configuration Utility

Hewlett Packard Enterprise recommends using the iLO 6 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.

Subtopics

Configuring a static IP address (iLO 6 Configuration Utility)

Managing local user accounts with the iLO 6 Configuration Utility

Configuring a static IP address (iLO 6 Configuration Utility)

About this task

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.

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. Click System Configuration.

5. Click iLO 6 Configuration Utility.
6. Disable DHCP:
   a. Click Network Options.
   b. Select OFF in the DHCP Enable menu.

      The IP Address, Subnet Mask, and Gateway IP Address boxes become editable. When DHCP Enable is set to ON, you cannot edit these values.
7. Enter values in the IP Address, Subnet Mask, and Gateway IP Address boxes.
8. To save the changes and exit, press F12.

   The iLO 6 Configuration Utility prompts you to confirm that you want to save the pending configuration changes.
9. To save and exit, click Yes - Save Changes.

   The iLO 6 Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.
10. Click OK.

    iLO resets, and the iLO session is automatically ended. You can reconnect in approximately 30 seconds.
11. Resume the normal boot process:
    a. Start the iLO remote console.

       The iLO 6 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, click Exit and resume system boot.

Managing local user accounts with the iLO 6 Configuration Utility

Subtopics

Adding user accounts (iLO 6 Configuration Utility)

Editing user accounts (iLO 6 Configuration Utility)

Removing user accounts (iLO 6 Configuration Utility)

Adding user accounts (iLO 6 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. Click System Configuration, click iLO 6 Configuration Utility, click User Management, and then click Add User.
5. Select the privileges for the new user.

   To assign a privilege, select YES in the menu next to the privilege name. To remove a privilege, select NO.

The Login privilege is assigned to every user by default, so it is not listed in the iLO 6 Configuration Utility.

You cannot assign the Recovery Set privilege through the iLO 6 Configuration Utility, so it is not available in the list.

6. Enter the user name and login name in the New User Name and Login Name boxes.
7. Enter the password.
   a. Move the cursor to the Password box, and then press Enter.

      The Enter your new password box opens.

   b. Type the password, and then press Enter.

      The Confirm your new password box opens.

   c. Type the password again to confirm, and then press Enter.

   The iLO 6 Configuration Utility confirms the new account creation.
8. To close the confirmation dialog box, click OK.
9. Create as many user accounts as needed, and then press F12 to save the changes and exit the system utilities.
10. When prompted to confirm the changes, click Yes - Save Changes to exit the utility and resume the boot process.

More information

iLO user account privileges
iLO user account options
Password guidelines

Editing user accounts (iLO 6 Configuration Utility)

About this task

NOTE: When the system is in Power On Self-Test (POST) state, Hewlett Packard Enterprise recommends NOT to perform a configuration change on iLO that would result in a reset of iLO. Making such a configuration change during POST may lead iLO to reset the factory defaults settings.

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. Click System Configuration, click iLO 6 Configuration Utility, click User Management, and then click Edit/Remove User.
5. In the Action menu for the user you want to edit or remove, select Edit.

   The account properties are displayed.
6. Update the Login Name.
7. Update the Password.
   a. Move the cursor to the Password box, and then press Enter.

      The Enter your new password box opens.

   b. Type the password, and then press Enter.

      The Confirm your new password box opens.

c. Type the password again to confirm, and then press Enter.

8. Modify the user account privileges.

   To assign a privilege, select YES in the menu next to the privilege name. To remove a privilege, select NO.

   The Login privilege is assigned to every user by default, so it is not available in the iLO 6 Configuration Utility.

   You cannot assign the Recovery Set privilege through the iLO 6 Configuration Utility, so it is not available in the list.

9. Update as many user accounts as needed, and then press F12 to save the changes and exit the system utilities.
10. When prompted to confirm the changes, click Yes - Save Changes to exit the utility and resume the boot process.

Removing user accounts (iLO 6 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 System Utilities start.

4. Click System Configuration, click iLO 6 Configuration Utility, click User Management, and then click Edit/Remove User.
5. In the Action menu for the user you want to remove, select Delete.

   The user name is marked to be deleted when you save the changes on this page.

6. If needed, mark other user accounts to delete, and then press F12 to save the changes and exit the system utilities.
7. When prompted to confirm the changes, click Yes - Save Changes 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.

More information

Supported browsers
Using the iLO web interface

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.

More information

Editing local user accounts
Password guidelines

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 or a common default password. The password type is defined at the factory, and it depends on the SKU numbers included in the server order.

  The common default password SKU number is P08040-B21. For more information, see the iLO QuickSpec document at the following website: **https://www.hpe.com/info/quickspecs**.
- **DNS name**—ILOXXXXXXXXXXXX, 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 driver support

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 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

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

- iLO 6 Channel Interface Driver for Windows—This driver is required for the Agentless Management Service, HPONCFG, firmware flash components, and other utilities to communicate with iLO. SUM uses this driver to inventory the firmware on a system. Install this driver in all configurations.
- iLO 6 Automatic Server Recovery Driver—This driver manages the ASR hardware timer, which will reset the server in the event of an operating system crash or lockup.

Linux

When you use Linux with iLO, the following driver is available: `hpilo` 1.5.0 and later.

This driver manages agent and tool application access to iLO.

`hpilo` is part of the Linux kernel for all the server operating systems supported by this version of the iLO firmware.

`hpilo` is loaded automatically at startup.

VMware

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.

HPE ProLiant RL3xx Gen 11 platforms do not support Windows, SUSE Linux Enterprise Server, or VMware.

Installing the iLO drivers

Procedure

1. Obtain the iLO drivers for your OS.
   - **For Windows**—**Download the SPP** or download the drivers from the Hewlett Packard Enterprise Support Center: **https://www.hpe.com/support/ilo6**.
   - **For VMware**—**Download the SPP** or download the driver from the vibsdepot section of the Hewlett Packard Enterprise Software Delivery Repository website: **https://www.hpe.com/support/SDR-Linux**.

   NOTE:
   The iLO driver is included in the Linux distribution for both Red Hat Enterprise Linux and SUSE Linux Enterprise Server.

2. Install the drivers.
   - If you downloaded the drivers from the Hewlett Packard Enterprise Support Center, follow the installation instructions provided with the software.
   - If you downloaded the SPP, follow the instructions in the SPP documentation: **https://www.hpe.com/info/spp/documentation**.

   Service Pack for ProLiant (SPP) does not support HPE ProLiant RL3xx Gen 11 platforms.

Using the iLO web interface

Subtopics

Supported browsers

Browser requirements

Logging in to the iLO web interface

Cookie sharing between browser instances and iLO

iLO web interface overview

Starting a remote management tool from the login page

Changing the language from the login page

Supported browsers

HPE iLO 6 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 6.

Browser requirements

- JavaScript—iLO uses client-side JavaScript extensively.
- 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 1.2 or TLS 1.3 in the browser.

Logging in to the iLO web interface

Procedure

1. Enter `https://<iLO host name or IP address>`.

   When you access the iLO web interface, you must use HTTPS (HTTP exchanged over an SSL encrypted session).

   The iLO login page opens.

   - If a login security banner is configured, the banner text is displayed in the NOTICE section.
   - If the Health LED status is Degraded or Critical, the Health LED icon is displayed next to the iLO host name.
   - If the iLO health status is Degraded, and the Anonymous Data access option is enabled, iLO displays the health status and a description of the issue on the login page. Self-test failures that could compromise security are not displayed in the description.
2. Enter a directory or local account login name and password, and then click Log In.

   If iLO is configured for Kerberos network authentication, the Zero Sign In button is displayed below the Log In button. You can use the Zero Sign In button to log in without entering a user name and password.

   If iLO is configured for CAC Smartcard Authentication, the Log in with Smartcard button is displayed below the Log In button. You can connect a smart card, and then click the Log in with Smartcard button. Do not enter a login name and password when you use CAC Smartcard Authentication.
3. For Microsoft Active Directory users, on successful validation of user credentials, if Two Factor Authentication is enabled, OTP login screen appears. Enter the OTP received to the email address configured on the LDAP server.

More information

iLO default DNS name and user account
CAC Smartcard Authentication
Configuring the Login Security Banner

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 on the Session List page.

For example, when User1 logs in, the web server builds the initial frames view, with User1 listed as the active user, menu items in the navigation pane, and page data in the 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 on the Session List 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.

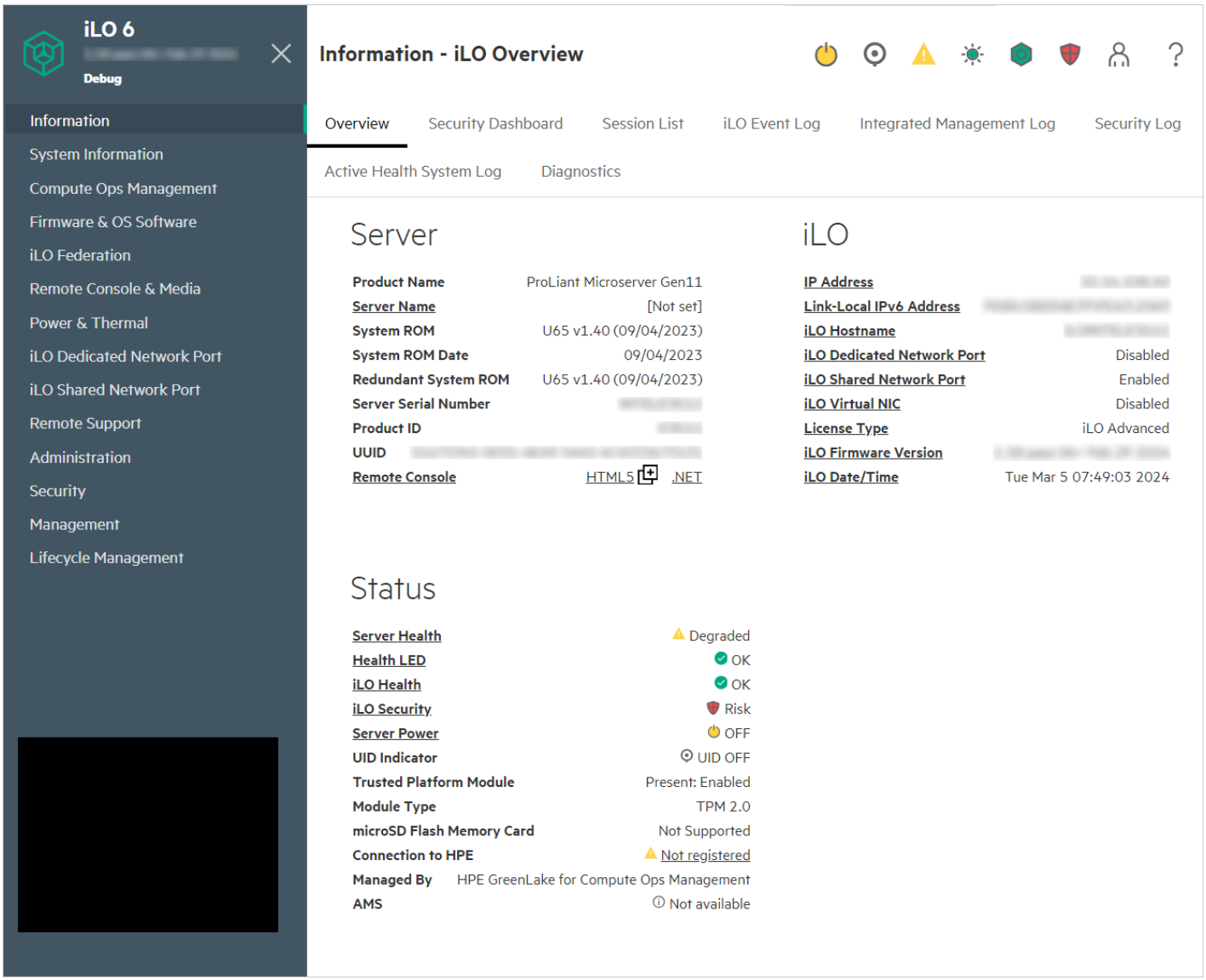
You can force the browser to refresh and reveal your true identity by pressing F5, selecting View > Refresh, or clicking the Refresh button.

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 with a navigation tree. To use the web interface, click an item in the navigation tree, and then click the name of the tab you want to view.



The following options are available in the navigation tree only if your server type or configuration supports them:

- When a remote management tool is used with iLO, the <Remote Management Tool Name> option is included.

Subtopics

iLO control icons

iLO navigation pane

iLO navigation pane remote console thumbnail

iLO control icons

When you log in to the iLO web interface, the iLO controls are available from any iLO page. You can click the iLO control icons to access

product features or information.

- Power icon—Use this icon to access the virtual power button features.

  The color of this icon varies based on the current power status.

- UID icon—Use this icon to turn the UID LED on and off.

  The color of this icon varies based on the current UID LED status.

- Language—Use this icon to select a language for the current iLO web interface session.

  Use the Settings option to view or modify the language settings.

  This icon is available only if one or more language packs are installed.

- Health LED icon—Indicates the system LED status. The color of this icon varies based on the current system LED status.
- Server Health icon—Use this icon to view the server health status summary. You can click the icon to view the health status for the server fans, temperature sensors, and other monitored subsystems.

  For most health status values in the list, you can click the status to view more information.

  This icon varies depending on the summarized server health status.

- iLO Health icon—Use this icon to view the iLO health status. The possible values are OK or Warning.
- Security icon—This icon shows the iLO security status, which is based on the combined results from the Security Dashboard page. The possible values are OK, Ignored, and Risk.

  You can click this icon to navigate to the Security Dashboard page.

  The color of this icon varies based on the security status.

- User icon—This icon supports the following actions:
  - Use the Logout option to log out of the current iLO web interface session.
  - Use the Sessions option to view the active iLO sessions.
  - Use the Settings option to view or modify iLO user accounts on the User Administration page.

    You can also click the name of the current session user to navigate to the User Administration page.

- Help icon—Use this icon to view online help for the current iLO web interface page.

  TIP:

  To navigate back or forward in the online help, press Alt+Left Arrow or Alt+Right Arrow.

- More icon—This icon is displayed on the Firmware & OS Software page when the browser window is too small to show the full page.

  Use this icon to access the Update Firmware option, Upload to iLO Repository option, and the Add to Queue option.

iLO navigation pane

iLO has a collapsible navigation pane that you can show or hide.

- To hide the navigation pane, click .

  When you hide the navigation pane, your preference is saved in a cookie, and it remains persistent when you:

  - View different pages.
  - Resize or refresh the browser window.

- Log in and out.

- To show the navigation pane when it is hidden, click  .

iLO navigation pane remote console thumbnail

The navigation pane shows a thumbnail of the remote console.

- To start a remote console, click the thumbnail and select a console option from the menu.
- When you run the HTML5 IRC in docked mode, the static remote console thumbnail changes to display the active remote console session.
- For servers with monitors: You can wake up a monitor that is in sleep mode by clicking the remote console thumbnail, and then selecting Wake-Up Monitor.

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.
   ```

   The name of the remote management tool is a link.

2. Click the remote management tool link.

More information

iLO and remote management tools

Changing the language from the login page

Prerequisites

A language pack is installed.

About this task

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.

Procedure

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

More information

Language packs

Viewing iLO information and logs

Subtopics

Viewing iLO overview information

Using the Security Dashboard

Managing iLO sessions

iLO Event Log

Integrated Management Log

Security Log

Active Health System

Viewing iLO overview information

Procedure

Click Information in the navigation tree.

The iLO Overview page displays high-level details about the server and the iLO subsystem, as well as links to commonly used features.

Subtopics

Server details

iLO details

Status details

Server details

Product Name

The product with which this iLO processor is integrated.

Server Name

The server name defined by the host OS.

To navigate to the Access Settings page, click the Server Name link.

Operating System

The server OS and version.

OS information is displayed when the Agentless Management Service (AMS) is installed and running and the OS is available. It is not displayed when the server is powered off.

System ROM

The version of the active system ROM.

System ROM Date

The date of the active system ROM.

Redundant System ROM

The version of the redundant system ROM. If a system ROM update fails or is rolled back, the redundant system ROM is used. This value is displayed only if the system supports redundant system ROM.

HPE ProLiant RL3xx Gen 11 platforms do not support Redundant System ROM.

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 OS 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.

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 OS 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.

Remote Console

Allows you to start a remote console for remote, out-of-band communication with the server console.

If the Remote Console option is disabled on the Access Settings page, the value Disabled is displayed.

If the current user is not assigned the Remote Console privilege, the value Unavailable is displayed.

To navigate to the iLO Integrated Remote Console page, click the Remote Console link.

More information

Starting the HTML5 IRC from the Overview page
Starting the .NET IRC from the overview page

iLO details

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.

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.

To navigate to the Network General Settings page, click the iLO Hostname link.

iLO Dedicated Network Port

The network interface status (enabled or disabled). If the server does not support this option, this value is not displayed.

To navigate to the Network Summary page, click the network interface name link.

iLO Shared Network Port

The network interface status (enabled or disabled). If the server does not support this option, this value is not displayed.

To navigate to the Network Summary page, click the network interface name link.

iLO Virtual NIC

The iLO Virtual NIC section displays the IP address to use when you connect to iLO through the Virtual NIC.

To navigate to the Access Settings page, where you can configure this feature, click iLO Virtual NIC.

License Type

The level of licensed iLO firmware functionality.

To navigate to the Licensing page, click the License Type link.

iLO Firmware Version

The version and date of the installed iLO firmware.

To navigate to the Installed Firmware page, click the iLO Firmware Version link.

iLO Date/Time

The internal clock of the iLO subsystem.

To navigate to the SNTP Settings page, click the iLO Date/Time link.

Status details

Server 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 server health status. The possible values are OK, Degraded, and Critical.

The server health is a roll up of individual subsystems. The subsystems are:

- Processor
- Memory
- BIOS or hardware health
- Network
- Storage
- Power supply
- Power supply redundancy
- Fans
- Fan redundancy
- Liquid cooling
- Liquid cooling redundancy
- Temperature
- Smart storage battery

Server health is the aggregate health of the subsystems. The highest severity of the subsystems is indicated as server health.

If the redundancy factor is Failed, the severity considered for calculation of server health will be Warning for the redundancy factor.

To navigate to the Health Summary page, click the Server Health link.

Health LED

Indicates the system LED status. It is the operational status of the server. The possible values are OK, Degraded, and Critical.

To navigate to the Integrated Management Log page, click the Health LED 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.

iLO Security

The iLO security status, which is based on the combined results from the Security Dashboard page. The possible values are OK, Ignored, and Risk.

To navigate to the Security Dashboard page, click the iLO Security link.

Server Power

The server power state (ON or OFF).

To access the virtual power button features, click the Server Power icon.

To navigate to the Server Power page, click the Server Power link.

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.

If the iLO Service Port is in use, the UID BLINK status includes the Service Port status. The possible values are UID BLINK (Service Port Busy), UID BLINK (Service Port Error), and UID BLINK (Service Port Finished).

To turn the UID LED on or off, click the UID Indicator icon, click the UID control at the top of the iLO web interface.

When the UID is blinking, and then it stops blinking, the status reverts to the previous value (UID ON or UID OFF). If a new state is selected when 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.

Platform RAS Policy

The configured platform Resiliency and Serviceability (RAS) policy.

The possible values follow:

- Firmware First (default)—The BIOS monitors corrected errors and logs an event when action is required for a corrected error. In this configuration, the OS does not monitor and log corrected errors.
- OS First—Corrected errors are unmasked to the OS and the OS controls the logging policy.

NOTE:
Corrected errors are an expected and natural occurrence. No action is required based on the logging of corrected errors unless the BIOS has also logged an event.

You can configure this setting by navigating to System Configuration > BIOS/Platform Configuration (RBSU) > Advanced Options in the UEFI System Utilities. Hewlett Packard Enterprise recommends using the default setting.

HPE ProLiant RL3xx Gen 11 platforms do not support Platform RAS Policy.

Trusted Platform Module or Trusted Module

The status of the TPM or TM socket or module.

The possible values are Not Supported, Not Present, or Present-Enabled.

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.

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.

microSD Flash Memory Card

The status of the internal SD card. If present, the SD card capacity is displayed.

Access Panel Status

The state of the access panel. The possible states are OK (the access panel is installed) and Intrusion (the access panel is open).

Connection to HPE

This section shows the remote support registration status for supported servers.

The possible status values follow:

- Registered to Remote Support—The server is registered.
- 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.

AMS

Agentless Management feature runs on the iLO hardware, independent of the operating system and processor. 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.

To collect information from devices and components that cannot communicate directly with iLO, install the Agentless Management Service (AMS). This section shows the status of AMS.

More information is not available for the Agentless Management Service (AMS).

The possible values are OK or Not available.

Managed By

This section shows the external manager which is used to manage the system. The possible values are:

- HPE OneView—Indicates that the system is managed by HPE OneView.
- HPE GreenLake for Compute Ops Management —Indicates that the system is managed by HPE GreenLake for Compute Ops Management

NOTE:

- The system can be managed by either HPE OneView or HPE GreenLake for Compute Ops Management.
- Managed By information is displayed only if the system is managed by any of the external managers.

More information

HPE embedded remote support

Using the Security Dashboard

Prerequisites

Configure iLO Settings privilege for configuring the Ignore option.

About this task

The Security Dashboard page displays the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. Use the dashboard to evaluate your configuration for potential risks. When a risk is detected, you can view details and advice for how to improve system security.

Procedure

1. Click Information in the navigation tree, and then click the Security Dashboard 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. Review the Security Dashboard table for detected risks.

   If a security feature is listed with Risk status, click the status value to view additional information. The additional information includes details about the risk and possible solutions.
4. (Optional) Configure the Ignore option for security features.
   - The Ignore option is disabled by default.
   - When you enable the Ignore option for a security feature, the status for that feature is ignored when iLO determines the Overall Security Status. Ignoring a security feature status does not change the Status value in the Security Dashboard table.

   When you change the Ignore value for a security feature, iLO recalculates the Overall Security Status.

Subtopics

Security Dashboard details

Risk details

Causes of security risk status

Security Dashboard details

Overall Security Status

- OK—iLO did not detect any security risks associated with the monitored security features.
- Risk—iLO detected a potential security risk associated with one or more monitored security features.
- Ignored—iLO detected a potential security risk associated with one or more monitored security features. All of the affected features are set to be excluded from the Overall Security Status.

  This status is also displayed on the Overview page and in the iLO controls.

Security State

The configured security state. The possible values are:

- Production
- High Security
- FIPS
- CNSA
- Synergy Security Mode

HPE ProLiant RL3xx Gen 11 platforms do not support FIPS and CNSA security states.

Server Configuration Lock

The configured Server Configuration Lock setting. This feature alerts the administrator to activities such as device substitution or addition, hardware removal, Secure Boot changes, and firmware installations. You can configure this feature in the UEFI System Utilities or by using the iLO RESTful API.

To view Server Configuration Lock information on the Security Dashboard page, your environment must meet the following requirements:

- The server was rebooted after the security state was changed from Production to a higher security state.
- A license that includes Server Configuration Lock is installed.

Security Dashboard table

- Security Parameter—The name of the monitored security feature.

  For features that you can configure in the iLO web interface, click the link in this column to navigate to the related web interface page.
- Status—The security status of the monitored security feature.
  -  OK—iLO did not detect a security risk associated with this feature.
  -  Risk—iLO detected a potential security risk associated with this feature.
- State—The current state of the monitored security feature. The possible values are:
  - Enabled—The feature is enabled.
  - Disabled—The feature is disabled.
  - Insufficient—The feature is enabled but the recommended configuration is not used.
  - Off—The feature is set to Off.
  - On—The feature is set to On.
  - OK—The feature complies with the iLO security recommendations.
  - Failed—The feature reported a failure.
  - Repaired—The feature reported a failure that was repaired.
  - True—The feature is in use.
  - False—The feature is not in use.
- Ignore—This column displays a switch that allows you to set a feature to be ignored. When you enable the Ignore setting, the monitored feature is not included in the Overall Security Status value.

  Ignoring a feature does not change the Status value displayed in the Security Dashboard table.

More information

iLO security states

Risk details

When you view the risk details for a security feature on the Security Dashboard page, the following information is available:

- Description—An explanation of why the security feature is in Risk status.
- Recommended Action—A recommended solution.

  This value is not displayed when the Ignore option is enabled.
- Ignored—The date and time that the Ignore option was enabled.
- Ignored by—The name of the user who enabled the Ignore option.

Causes of security risk status

The following security features are monitored on the Security Dashboard page. If a server does not support a feature, it is not listed.

Access Panel Status

The chassis intrusion detection connector reported that the access panel status is Intrusion.

This feature is available only on servers that are configured for chassis intrusion detection.

Hewlett Packard Enterprise recommends auditing the events recorded in the IML and iLO Event log, and checking surveillance video for any physical intrusion activity on the server.

Authentication Failure Logging

iLO is not configured to log authentication failures.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Default SSL Certificate In Use

The iLO default self-signed certificate is in use.

Hewlett Packard Enterprise recommends configuring a trusted certificate on the SSL Certificate Customization page.

IPMI/DCMI Over LAN

The IPMI/DCMI over LAN feature is enabled, which exposes the server to known IPMI security vulnerabilities.

Hewlett Packard Enterprise recommends disabling this feature on the Access Settings page.

Last Firmware Scan Result

The last firmware verification test failed. A firmware component is corrupted or its integrity is compromised.

Hewlett Packard Enterprise recommends updating the affected firmware component to a verified image.

To use this feature, you must install a license. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/ilo-docs**.

Minimum Password Length

The minimum password length is less than the recommended length, which makes the server vulnerable to dictionary attacks.

Hewlett Packard Enterprise recommends setting this value to 8 (default) or greater on the Access Settings page.

Password Complexity

iLO is not configured to enforce the password complexity guidelines, which makes the server vulnerable to dictionary attacks.

You can enable this feature on the Access Settings page.

Require Host Authentication

The Require Host Authentication feature is disabled and iLO is configured to use the High Security security state. When this feature is disabled, iLO credentials are not required when you use host-based configuration utilities to access the management processor.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Require Login for iLO RBSU

iLO is not configured to require login credentials to access the iLO configuration options in the UEFI System Utilities. This configuration allows unauthenticated access to the iLO configuration during system boot.

Hewlett Packard Enterprise recommends enabling this feature on the Access Settings page.

Secure Boot

The UEFI Secure Boot option is disabled. In this configuration, the UEFI system firmware skips validation for the boot loader, Option ROM firmware, and other system software executables for trusted signatures. It breaks the chain of trust established by iLO from power-on.

Hewlett Packard Enterprise recommends enabling this feature.

For more information, see the UEFI System Utilities documentation.

Security Override Switch

The server Security Override Switch (also called the System Maintenance Switch) is enabled. This configuration is a risk because login authentication is not required when the Security Override Switch is enabled.

Hewlett Packard Enterprise recommends disabling this feature.

SNMPv1 Request

SNMPv1 Request is enabled. This configuration allows iLO to receive SNMPv1 requests. Enabling SNMPv1 Request increases the system vulnerability to attack.

Hewlett Packard Enterprise recommends disabling this feature on the SNMP Settings page.

Global Component Integrity

SPDM authentication is enabled. This configuration allows iLO to authenticate all applicable components in the server using SPDM. Disabling Global Component Integrity in the Access Settings page will change the iLO security status to risk.

If the Global Component Integrity is disabled, iLO does not validate the components for SPDM authentication and even the SPDM supported cards will be reported as `Not Supported`.

You can enable this feature on the Access Settings page.

More information

Configuring iLO access settings
Reasons to disable iLO security
Firmware verification

Managing iLO sessions

Prerequisites

Administer User Accounts privilege

Procedure

1. Navigate to the Information page, and then click the Session List tab.

   The Session List page displays information about the active iLO sessions.

2. (Optional) To disconnect a session, click the check box next to it, and then click Disconnect session.

   iLO prompts you to confirm that you want to disconnect the selected session.

3. Click Yes, disconnect.

Session list details

iLO displays the following details in the Current Session and Session List (*Total number of active sessions*) tables:

- User—The iLO user account name.

  Regular user accounts are displayed in the format *User: user account name*. Service accounts are displayed in the format *Service User: user account name*.

- IP—The IP address of the computer used to log in to iLO.
- Login Time—The date and time that the iLO session started.
- Access Time—The date and time that iLO was last active in the session.
- Expires—The date and time that the session will end automatically.
- Source—The session source (for example, remote console, web interface, ROM-based setup utility, iLO RESTful API, or SSH).
- Privilege icons (current user only)—The privileges assigned to the current user account. A checkmark icon indicates that a privilege is

enabled. An X icon indicates that a privilege is disabled.

More information

iLO user accounts

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.

Subtopics

Viewing the event log

Saving the event log to a CSV file

Clearing the event log

Viewing the event log

Procedure

1. Click Information in the navigation tree, and then click the iLO Event Log tab.
2. (Optional) Use the sort, search, and filter features to customize the log view.
3. (Optional) To refresh the event list, click .
4. (Optional) To view the event details pane, click an event.

Subtopics

Event log view controls

Event log details

Event log icons

Event log event pane details

Event log view controls

Sorting events

To sort the log table by a column, click the column heading.

To change the display to ascending or descending order, click the column heading again or click the arrow icon next to the column.

Refreshing the event list

To refresh the list of log entries, click  .

Searching for an event

To search for events based on dates, event ID, or description text, click  , and then enter text in the search box.

Event filters

To access the log filters, click  .

- To filter by severity, select a severity level from the Severity menu.
- To filter by category, select a value in the Category menu.
- To change the displayed date and time for events, select a value in the Time menu. Choose from the following:
  - Show Default—Display UTC time.
  - Show Local Time—Display the iLO web interface client time.
  - Show ISO Time—Display UTC time in ISO 8601 format.
- To filter by the last update date, select a value in the Last Update menu.
- To set the filters back to the default values, click Reset filters.

Event log details

When you view the event log, the total number of recorded events is displayed above the Filter Logs icon.

When log filters are applied, the number of events that meet the filter criteria is displayed below the filter icon.

The following details are displayed for each event:

- ID—The event ID number. Events are numbered in the order in which they are generated.

  By default, the log 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.
- Description—The description provides the 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 log.
- 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, the value `[NOT SET]` is displayed.
- Count—The number of times this event has occurred (if supported).

  In general, important events generate a log entry each time they occur. They are not consolidated into one log entry.

  When less important events are repeated, they are consolidated into one log entry, and iLO updates the Count and Last Update values.

  Each event type has a defined interval that determines whether repeated events are consolidated or a new event is logged.
- Category—The event category. For example, Administration, Configuration, or Security.

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.

Event log event pane details

- 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.
- Event Class—A unique identifier for the event class.

  This value is displayed in hexadecimal format.
- Event Code—A unique identifier for an event in an event class.

  This value is displayed in hexadecimal format.
- Recommended Action—A short description of the recommended action for a failure condition.

  NOTE:

  The Recommended Action text is static. It is not removed or updated when the event status changes. If corrective action is complete, you can ignore the recommended action.

Saving the event log to a CSV file

Procedure

1. Click Information in the navigation tree, and then click the iLO Event Log tab.
2. Click CSV.

   The CSV Output window is displayed.
3. Click Save, and then follow the browser prompts to save or open the file.

Clearing the event log

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Information in the navigation tree, and then click the iLO Event Log tab.
2. Click .

iLO prompts you to confirm the request.

3. Click Yes, clear.

   The log is cleared of all previously logged information. This action is recorded in the event 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 drivers. Logged events include server-specific information such as health and status information, firmware updates, 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.

Subtopics

Examples of IML event types

- Fan actions and status
- Power supply actions and status
- Temperature status and automatic shutdown actions
- Drive failure
- Firmware flash actions
- Smart Storage Energy Pack status
- Network actions and status

Viewing the IML

Procedure

1. Click Information in the navigation tree, and then click the Integrated Management Log tab.
2. (Optional) Use the sort, search, and filter features to customize the log view.

3. (Optional) To refresh the event list, click .
4. (Optional) To view the event details pane, click an event.

Subtopics

IML view controls

Sorting events

To sort the log table by a column, click the column heading.

To change the display to ascending or descending order, click the column heading again or click the arrow icon next to the column.

Refreshing the event list

To refresh the list of log entries, click .

Searching for an event

To search for events based on dates, event IDs, or description text, click , and then enter text in the search box.

Event filters

To access the log filters, click .

- To filter by severity, select a severity level from the Severity list.
- To filter by class, select a class from the Class list.
- To filter by category, select a value in the Category list.
- To change the displayed date and time for events, select a value in the Time menu. Choose from the following:
  - Show Default—Display UTC time.
  - Show Local Time—Display the iLO web interface client time.
  - Show ISO Time—Display UTC time in ISO 8601 format.
- To filter by the Last Update date, select a value in the Last Update menu.
- To set the filters back to the default values, click Reset filters.

IML details

When you view the IML, the total number of recorded events is displayed above the Filter Logs icon.

When log filters are applied, the number of events that meet the filter criteria is displayed below the filter icon.

The following details are displayed for each event:

- **Repairable events**—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. This check box is used 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 log 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, UEFI, environment, or system revision.
- Description—The description provides the 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.
- 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, the value `[NOT SET]` is displayed.
- Count—The number of times this event has occurred (if supported).

  In general, important events generate a log entry each time they occur. They are not consolidated into one log entry.

  When less important events are repeated, they are consolidated into one log entry, and iLO updates the Count and Last Update values.

  Each event type has a defined interval that determines whether repeated events are consolidated or a new event is logged.
- Category—The event category. For example, Hardware, Firmware, or Administration.

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.

IML event pane details

- 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.
- Event Class—A unique identifier for the event class.

  This value is displayed in hexadecimal format.
- Event Code—A unique identifier for an event within an event class.

  This value is displayed in hexadecimal format.
- Learn More— Click the link displayed here to access troubleshooting information for supported events.
- Recommended Action—A short description of the recommended action for a failure condition.

NOTE:

The Recommended Action text is static. It is not removed or updated when the event status changes. If corrective action is complete or an event shows Repaired status, you can ignore the recommended action.

Marking an IML entry as repaired

Prerequisites

Configure iLO Settings privilege

About this task

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

Procedure

1. Investigate and repair the issue.
2. Click Information in the navigation tree, and then click the Integrated Management Log tab.
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 .

   The iLO web interface refreshes, and the selected log entry status changes to Repaired.

Adding a maintenance note to the IML

Prerequisites

Configure iLO Settings privilege

About this task

Use maintenance notes to create log entries about activities such as:

- Upgrades
- System backups
- Periodic system maintenance
- Software installations

Procedure

1. Click Information in the navigation tree, and then click the Integrated Management Log tab.
2. Click .

   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

Procedure

1. Click Information in the navigation tree, and then click the Integrated Management Log tab.
2. Click  .

   The CSV Output window is displayed.
3. Click Save, and then follow the browser prompts to save or open the file.

Clearing the IML

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Information in the navigation tree, and then click the Integrated Management Log tab.
2. Click  .

   iLO prompts you to confirm the request.
3. Click Yes, clear.

   The log is cleared of all previously logged information. This action is recorded in the IML.

Security Log

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

Examples of the logged events include changes to the security configuration and security compliance issues. Other logged events include hardware intrusion, maintenance, and denial of service.

The security log provides a focused view of all recorded security events. Some of the same events are also included in the iLO event log or IML.

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

Viewing the security log

Procedure

1. Click Information in the navigation tree, and then click the Security Log tab.
2. (Optional) Use the sort, search, and filter features to customize the log view.
3. (Optional) To refresh the event list, click  .
4. (Optional) To view the event details pane, click an event.

Security log view controls

Sorting events

To sort the log table by a column, click the column heading.

To change the display to ascending or descending order, click the column heading again or click the arrow icon next to the column.

Refreshing the event list

To refresh the list of log entries, click .

Searching for an event

To search for events based on dates, event IDs, or description text, click , and then enter text in the search box.

Event filters

To access the log filters, click .

- To filter by severity, select a severity level from the Severity list.
- To filter by class, select a class from the Class list.
- To filter by category, select a value in the Category list.
- To change the displayed date and time for events, select a value in the Time menu. Choose from the following:
  - Show Default—Display UTC time.
  - Show Local Time—Display the iLO web interface client time.
  - Show ISO Time—Display UTC time in ISO 8601 format.
- To filter by the Last Update date, select a value in the Last Update menu.
- To set the filters back to the default values, click Reset filters.

Security log details

When you view the security log, the total number of recorded events is displayed above the Filter Logs icon.

When log filters are applied, the number of events that meet the filter criteria is displayed below the filter icon.

The following details are displayed for each event:

- ID—The event ID number. Events are numbered in the order in which they are generated.

  By default, the log 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, UEFI, environment, or system revision.
- Description—The description provides the 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.
- 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, the value `[NOT SET]` is displayed.
- Count—The number of times this event has occurred (if supported).

  In general, important events generate a log entry each time they occur. They are not consolidated into one log entry.

  When less important events are repeated, they are consolidated into one log entry, and iLO updates the Count and Last Update values.

  Each event type has a defined interval that determines whether repeated events are consolidated or a new event is logged.
- Category—The event category. For example, Security, Maintenance, or Configuration.

Security log 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.

Security log event pane details

- 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, the value `[NOT SET]` is displayed.
- Event Class—A unique identifier for the event class.

  This value is displayed in hexadecimal format.
- Event Code—A unique identifier for an event in an event class.

  This value is displayed in hexadecimal format.
- Recommended Action—A short description of the recommended action for a failure condition.

> **NOTE:**
>
> The Recommended Action text is static. It is not removed or updated when the event status changes. If corrective action is complete, you can ignore the recommended action.

Saving the security log to a CSV file

Procedure

1. Click Information in the navigation tree, and then click the Security Log tab.
2. Click CSV.

   The CSV Output window is displayed.
3. Click Save, and then follow the browser prompts to save or open the file.

Clearing the security log

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Information in the navigation tree, and then click the Security Log tab.
2. Click the trash icon.

   iLO prompts you to confirm the request.
3. Click Yes, clear.

   The log is cleared of all previously logged information. This action is recorded in the security log.

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

Subtopics

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 Active Health System Log, you may optionally append your contact information. When you 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 **https://www.hpe.com/info/privacy**.

You can upload the log to HPE InfoSight for Servers to view the log data or create a support case for servers under a valid warranty or

support contract. For more information, see the HPE InfoSight for Servers documentation at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

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.
- **iLO Service Port**—Download the log by connecting a USB flash drive to the iLO Service Port on the front of the server.
- **cURL utility**—Download the log by using the cURL command-line tool.
- **Intelligent Provisioning**—For instructions, see the Intelligent Provisioning user guide.
- **iLO RESTful API and RESTful Interface Tool**—For more information, see **https://www.hpe.com/support/restfulinterface/docs**.

More information

Downloading the Active Health System Log for a date range
Downloading the entire Active Health System Log
Downloading the Active Health System Log by using cURL
Downloading the Active Health System Log through the iLO Service Port
Downloading the Active Health System log (iLOREST)

Downloading the Active Health System Log for a date range

Procedure

1. In the iLO UI, click Information in the navigation tree, and then click the Active Health System Log tab.

   The Active Health System Log is inaccessible when a download of the log is in progress.

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.

   To reset the range to the default values, click ↩.

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 your service technician.

   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 HPE InfoSight for Servers.

   You can access the Analyze Logs page in HPE InfoSight for Servers by selecting Infrastructure > Analyze Logs under the Compute heading.

   For more information, see the HPE InfoSight for Servers User Guide at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

Downloading the entire Active Health System Log

About this task

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. Click Information in the navigation tree, and then click the Active Health System Log tab.

   The Active Health System Log is inaccessible when a download of the log is in progress.
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 your service technician.

   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 HPE InfoSight for Servers.

   You can access the Analyze Logs page in HPE InfoSight for Servers by selecting Infrastructure > Analyze Logs under the Compute heading.

For more information, see the HPE InfoSight for Servers User Guide at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

Downloading the Active Health System Log by using cURL

About this task

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 your service technician.

   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 log file to HPE InfoSight for Servers to view the log data or create a support case for servers under a valid warranty or support contract.

For more information, see the HPE InfoSight for Servers documentation at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

Subtopics

cURL command usage with iLO

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 log file to HPE InfoSight for Servers to view the log data or create a support case for servers under a valid warranty or support contract.

   For more information, see the HPE InfoSight for Servers documentation at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

Subtopics

iLOREST serverlog command usage

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

Prerequisites

- Configure iLO Settings privilege
- Enable Active Health System Logging is enabled in the Show Advanced Settings section of the Active Health System Log page.

About this task

If the log file is corrupted, or if you want to clear and restart logging, clear the Active Health System Log.

Procedure

1. Click Information in the navigation tree, and then click the Active Health System Log tab.

   The Active Health System Log is inaccessible when a download of the log is in progress.
2. Click Show Advanced Settings.
3. Scroll to the Clear Log section, and then click Clear.
4. When prompted to confirm the request, click Yes, clear.

   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 and system diagnostics

About this task

HPE ProLiant RL3xx Gen 11 platforms do not support the following features or options:

- Generating NMI
- Power Capping
- Booting to system safe mode
- Booting to Intelligent Diagnostics mode

Subtopics

Viewing iLO self-test results

iLO reboot (reset)

Reimaging an appliance

System diagnostics

Viewing iLO self-test results

About this task

The iLO Self-Test Results section displays the results of internal iLO diagnostic tests, including the test name, status, and notes.

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.

If a status is not reported for a test, the test is not listed.

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics 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.

Subtopics

iLO self-test details

iLO self-test types

iLO self-test details

iLO Health

The iLO health status, which is based on the combined results of the iLO diagnostic self-tests.

Self-Test

The tested function.

Status

The test status.

- Pass—The test was successful.
- Degraded—The test detected a problem. A reboot, firmware or software update, or service might be required.

  If a self-test reports this status, check the IML for additional information.

  For Secure Element degraded status, perform AC power cycle and check the status of Secure Element. If the problem persists, contact Support with the AHS and Notes details.
- Informational—Supplemental data about the tested system is provided in the Notes column.

Notes

A test might include supplemental information in the Notes column.

For some tests, this column displays the versions of other system programmable logic, such as the System Board PAL or the Power Management Controller.

iLO self-test types

The tests that are run are system-dependent. Not all tests are run on all systems. The possible tests include:

- Cryptographic—Tests security features.
- NVRAM data—Tests the subsystem that retains nonvolatile configuration data, logs, and settings.
- Embedded Flash—Tests the state of the system that can store configuration, provisioning, and service information.
- Host ROM—Checks the BIOS to determine whether it is out-of-date compared to the management processor.
- Supported Host—Checks the management processor firmware to determine whether it is out of date for the server hardware.
- Power Management Controller—Tests functions related to power measurement, power capping, and power management.
- CPLD—Tests the programmable hardware in the server.
- EEPROM—Tests the hardware that stores basic iLO properties that are assigned during the manufacturing process.
- Secure Element—Tests the hardware that stores basic iLO properties that are assigned during the manufacturing process.

  Based on the supported platform Secured Element or EEPROM entries are shown.
- **ASIC Fuses**—Compares a known data pattern against expected data manufactured into the iLO chip to make sure that the chip was manufactured properly and that operating settings meet tolerances.

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.

Subtopics

iLO reboot (reset) methods

Rebooting (resetting) the iLO processor with the web interface

Rebooting (resetting) iLO with the iLO 6 Configuration Utility

Performing a graceful iLO reboot with the server UID button

Performing a hardware iLO reboot with the server UID button

iLO reboot (reset) methods

iLO web interface

Use the Reset button on the Diagnostics page.

iLO 6 Configuration Utility

Use the iLO 6 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 6 Scripting and Command Line Guide.

IPMI

For more information, see the HPE iLO 6 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) the iLO processor with the web interface

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics tab.
2. Click Reset.

   iLO prompts you to confirm the request.

   If the server is in the Power On Self-Test (POST) process, iLO warns you that a reset may cause unexpected behavior like resetting iLO to the factory defaults settings. A system reboot may be required after the iLO reset is complete.
3. Click Yes, reset iLO.

   iLO resets and closes your browser connection.

Rebooting (resetting) iLO with the iLO 6 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, click System Configuration, and then click iLO 6 Configuration Utility.
5. Select Yes in the Reset iLO menu.

   The iLO 6 Configuration Utility prompts you to confirm the reset.
6. Click OK.
7. iLO resets and all active connections are ended. If you are managing iLO remotely, the remote console session is automatically ended.

   When you reset iLO, the iLO 6 Configuration Utility is not available again until the next server reboot.
8. 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 open from the previous session.

b. Press Esc until the main menu is displayed.

c. Click Exit and resume system boot.

d. When prompted to confirm the request, click OK to exit the utility and resume the normal boot process.

Performing a graceful iLO reboot with the server UID button

About this task

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

About this task

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 secure recovery or iLO network failed flash recovery features. 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.

Reimaging an appliance

Prerequisites

- Login privilege
- Remote Console privilege
- Virtual Power and Reset privilege

- Virtual Media privilege

About this task

You can use iLO to initiate the reimage process for supported appliances when you cannot access the appliance hardware directly.

> **WARNING:**
> When you reimage an appliance, it will be offline until the reimage process is complete.

Procedure

1. Use the iLO virtual media feature to connect a USB device that contains an appliance software image.

   The image must include the HPE OneView software.
2. Click Information in the navigation tree, and then click the Diagnostics tab.
3. Click Reimage.

   iLO prompts you to confirm the request.
4. Click Yes, reimage the appliance.

More information

Using a virtual drive (physical drive on a client PC)

System diagnostics

The following system diagnostics features are available. Feature support depends on your server model and iLO version. Features that are not supported on a server are not displayed on the Diagnostics page.

- Generate an NMI
- Restore the default manufacturing settings
- Restore the default system settings
- Save UEFI serial debug messages to the Active Health System

> **IMPORTANT:**
> Do not initiate more than one system diagnostics operation at the same time. Running more than one operation at the same time might cause unexpected results.

Subtopics

Generating an NMI

Booting to system safe mode

Booting to Intelligent Diagnostics mode

Restoring the default manufacturing settings

Restoring the default system settings

Saving UEFI serial debug messages to the Active Health System Log during POST

Generating an NMI

Prerequisites

Virtual Power and Reset privilege

About this task

The Generate NMI feature enables you to stop the operating system for debugging.

This feature is useful when a system does not boot and hangs in a pre-OS state (for example, during POST). Using an NMI enables the system ROM exception handler to run and capture a trace of the code that caused the issue.

HPE ProLiant RL3xx platforms do not support NMI generation.

> **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 button only in extreme cases in which the OS is not functioning correctly and an experienced support organization has recommended an NMI.

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics tab.
2. Click Show System Diagnostics.
3. Click Generate NMI.

   iLO prompts you to confirm the request.

   > **CAUTION:**
   > Generating an NMI might cause data loss and data corruption.

4. Click Yes, proceed.

   iLO confirms that the NMI was sent.

Booting to system safe mode

Prerequisites

- Host BIOS privilege
- Virtual Power and Reset privilege
- Configure iLO Settings privilege
- The server platform supports this feature.
- The server is powered off.

About this task

Use the System Safe Mode option to boot the system with a minimum configuration to check if a boot processor is operating correctly. All other PCIe devices are removed from the configuration quickly and safely.

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics tab.
2. Click Show System Diagnostics.
3. Click Boot to Safe Mode.

   iLO prompts you to confirm the request.

4. Click Yes, proceed.

   A successful server boot in safe mode indicates that the boot processor is operating correctly.

   The results of this action are recorded in the IML.

Booting to Intelligent Diagnostics mode

Prerequisites

- Host BIOS privilege
- Virtual Power and Reset privilege
- Configure iLO Settings privilege
- The server platform supports this feature.
- The server is powered off.

About this task

When you enter Intelligent Diagnostics mode on a supported system, the system can automatically diagnose a boot failure during POST.

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics tab.
2. Click Show System Diagnostics.
3. Click Boot to Intelligent Diagnostics Mode.

   iLO prompts you to confirm the request.

4. Click Yes, proceed.

   iLO notifies you that the system is in Intelligent Diagnostics mode.

   The server begins a sequence of reboots to determine the cause of the boot failure. When a cause is identified, the affected device is disabled, and the boot process resumes.

   NOTE:

   This process might take a long time to complete. Multiple server reboots might be required to isolate and identify the cause of the boot failure. After you enter Intelligent Diagnostics mode, allow the process to complete without interruption.

   To monitor the status, check the server POST screen.

   The results of this action are recorded in the IML.

5. If an issue was detected, take the necessary steps to resolve the issue.

Restoring the default manufacturing settings

Prerequisites

- Host BIOS privilege
- Virtual Power and Reset privilege

- Configure iLO Settings privilege
- The server platform supports this feature.
- The server is powered off.

About this task

Use the Restore Default Manufacturing Settings option to reset all BIOS configuration settings to their default manufacturing values.

This process deletes all UEFI nonvolatile variables, such as boot configuration, Secure Boot security keys (if Secure Boot is enabled), and configured date and time settings.

To use an option that retains some UEFI settings, consider the Restoring Default System Settings option.

When you use this feature, the iLO IP address and iLO settings stored in the nonvolatile memory are retained.

Procedure

1. (Optional) Set the Save User Defaults option to Yes, Save in the UEFI System Utilities.

   When enabled, this option causes the current BIOS settings to be used as the default settings when you restore the default manufacturing settings.

   For more information, see the UEFI System Utilities user guide.
2. Click Information in the navigation tree, and then click the Diagnostics tab.
3. Click Show System Diagnostics.
4. Click Restore Default Manufacturing Settings.

   iLO prompts you to confirm the request, and warns you that previously configured settings, including Secure Boot settings, will be reset to the default values.
5. Click Yes, proceed.

   The UEFI nonvolatile variables are reset to the default values, and the server restarts.

   To monitor the status, check the server POST screen.

   The results of this action are recorded in the IML.

Restoring the default system settings

Prerequisites

- Host BIOS privilege
- Virtual Power and Reset privilege
- Configure iLO Settings privilege
- The server platform supports this feature.
- The server is powered off.

About this task

Use the Restore Default System Settings option to reset all BIOS configuration settings to their default values and restart the server.

Selecting this option resets all platform settings except:

- Secure boot BIOS settings
- Date and time settings
- Primary and redundant ROM selection (if supported)

- Other entities, such as option cards or iLO, that must be individually reset.

  When you use this feature, the iLO IP address and iLO settings stored in the nonvolatile memory are retained.

Procedure

1. (Optional) Set the Save User Defaults option to Yes, Save in the UEFI System Utilities.

   When enabled, this option causes the current BIOS settings to be used as the default settings when you restore the default system settings.

   For more information, see the UEFI System Utilities user guide.
2. Click Information in the navigation tree, and then click the Diagnostics tab.
3. Click Show System Diagnostics.
4. Click Restore Default System Settings.

   iLO prompts you to confirm the request, and warns you that previously configured settings will be reset to the default values.
5. Click Yes, proceed.

   The BIOS configuration settings are reset to the default values, and the server restarts.

   To monitor the status, check the server POST screen.

   The results of this action are recorded in the IML.

Saving UEFI serial debug messages to the Active Health System Log during POST

Prerequisites

- The server is in the Power On Self-Test (POST) state.

About this task

During normal server operation, UEFI serial log messages are automatically saved to the Active Health System Log. These messages can be helpful when the Active Health System Log is used for troubleshooting. If a server stalls or fails to boot, UEFI serial debug messages are not sent automatically. Use this procedure to manually save UEFI serial debug messages to the Active Health System Log one time. To save the UEFI serial debug messages again, repeat this procedure.

This feature is available only during server POST. After POST is complete, the Capture button is unavailable.

Procedure

1. Click Information in the navigation tree, and then click the Diagnostics tab.
2. Click Capture.

   iLO notifies you that the UEFI serial debug messages were saved to the Active Health System Log.

Viewing general system information

Subtopics

Viewing health summary information

About this task

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. Click System Information in the navigation tree.
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.

   When you click a fan or liquid cooling module value on a system with liquid cooling modules, the Power & Thermal page opens and displays the Fans & Cooling Modules tab. If liquid cooling modules are not present or supported, then the tab is called Fans.

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

Subtopics

Redundancy status

Redundancy status is displayed for the following:

- Fan Redundancy
- Power

  Based on the power domains available in the system, the redundancy status appears. If the system has multiple power domains, the System redundancy and GPU redundancy status are displayed. (This option is available only for supported servers).
- Liquid Cooling Redundancy (supported servers only)

Subsystem and device status

Summarized status information is displayed for the following:

- Agentless Management Service
- BIOS/Hardware Health
- Fans
- Liquid Cooling (supported servers only)
- Memory
- Network
- Power Supplies (nonblade servers only)

  Based on the power supply domains available in the system, the System domain and GPU domain appear (This option is available only for supported servers).
- Processors
- Storage
- Temperatures
- Smart Storage Energy Pack (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.
- Critical—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.
- 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 processor information

About this task

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

Click System Information in the navigation tree, and then click the Processors tab.

Subtopics

Processor details

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

About this task

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. Click System Information in the navigation tree, and then click the Memory tab.

   The Memory page displays details for the following:

   - Advanced Memory Protection (AMP)
   - Memory Summary
   - Physical Memory
   - High Bandwidth Memory

2. (Optional) By default, empty memory slots are hidden in the Physical Memory table. To view empty memory slots, click show empty memory slots. When empty memory slots are displayed, click hide empty memory slots to hide them.

   This option is not displayed if there are no empty slots.

3. (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.

4. (Optional) To view additional memory details, select a memory module.

   The Memory Details pane is displayed.

Subtopics

Advanced Memory Protection details

Advanced memory protection is available only in supported platforms.

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.
- A3DC—The system is protected by AMP in the A3DC mode.
- Degraded A3DC—The system is protected by AMP in the A3DC 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.
- A3DC—The system is configured for AMP with the A3DC engine.

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.
- A3DC—The system can be configured for A3DC AMP.
- 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.

Memory Type

The type of memory

Total Memory Slots

The number of memory module slots.

Total Memory

The capacity of the memory, including memory recognized by the OS and memory used for spare, mirrored, or XOR configurations.

Operating Frequency

The frequency at which the memory operates.

Physical Memory Details

The Physical Memory Details section shows the physical 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.

Socket Locator

The slot or processor on which the memory module is installed.

Status

The memory module status and whether the module is in use. Possible values follow:

- Added But Unused—The DIMM was added and it is unused.
- Configuration Error—There is a configuration error in the DIMM.
- Degraded—The DIMM status is degraded.
- Does Not Match—The DIMM type does not match.
- Expected but Missing —The DIMM is expected, but it is missing.
- Good, In Use—The DIMM is functioning properly and it is in use.
- Good, Partially in Use—The DIMM is functioning properly and it is partially in use.
- Map Out Error—The DIMM is mapped out because of a training failure.
- Map Out Configuration —The DIMM is mapped out because of a configuration error.
- Not Present—The DIMM is not present.
- Not Supported—The DIMM is not supported.
- Other—The DIMM status does not fit any of the standard status definitions.
- Present, Spare—The DIMM is present and it is used as a spare.
- Present, Unused—The DIMM is present and it is unused.
- Unknown—The DIMM status is unknown.
- Upgraded but Unused —The DIMM was upgraded and it is unused.

Size

The memory module size.

Max Supported Frequency

The maximum frequency supported by the memory module.

Technology

The memory module technology. Possible values follow:

- Unknown—Memory technology cannot be determined.
- N/A—Memory module not present.
- SDRAM (Synchronous DRAM)
- RDIMM (Registered memory module)
- UDIMM (Unregistered memory module)
- LRDIMM (Load-reduced memory module)

Subtopics

Memory Details pane (physical memory)

Memory Details pane (physical memory)

Manufacturer

The memory module manufacturer.

Part Number

The memory module part number.

This value is displayed only for HPE memory modules.

Serial Number

The memory module serial number.

This value is not displayed for empty memory slots.

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.
- DDR5
- N/A—Memory module is not present.

Ranks

The number of ranks in the memory module.

Error Correction

The type of error correction used by the memory module.

Data Width Bits

The memory module data width in bits.

Bus Width Bits

The memory module bus width in bits.

Channel

The channel number in which the memory module is connected.

Memory Controller

The memory controller number.

CPU Socket

The memory module socket number.

Memory Slot

The memory module slot number.

State

The memory state.

Vendor

The memory vendor name. If the vendor name is not available, the value N/A is displayed.

Vendor ID

The memory vendor ID.

Armed

The current backup-ready status of the NVDIMM-N, if available.

Last Operation

The status of the last operation (NVDIMMs only).

Media Life

The percentage of media life left (NVDIMMs only).

High Bandwidth Memory details

The High Bandwidth Memory details section shows the high bandwidth memory modules present on the processor that were installed. High bandwidth memory allows normal system boot without DDR5 DIMMs. High bandwidth memory is available only on supported platforms.

Socket Locator

The processor on which the memory module is present.

Size

The memory module size.

Max Supported Frequency

The maximum frequency supported by the memory module.

Technology

The memory module technology. Possible values are:

- Synchronous
- N/A—Memory module not present.

Subtopics

High Bandwidth Memory modes

Memory Details pane (High bandwidth memory)

High Bandwidth Memory modes

This section shows the different memory modes in High bandwidth memory.

The available modes are:

- HBM Only—Memory summary lists only High bandwidth memory records. High bandwidth memory section shows both memory mode and memory details. The Physical memory section is hidden.
- Flat—Memory summary lists both High bandwidth memory and DIMM records. High bandwidth memory section shows memory mode and memory details.
- Cache—Memory summary lists only DIMM records. High bandwidth memory section shows only the memory mode and memory details are hidden.

Memory Details pane (High bandwidth memory)

Manufacturer

The memory module manufacturer.

Type

The type of memory installed. Possible values are:

- HBM
- N/A—Memory module is not present.

Ranks

The number of ranks in the memory module.

Error Correction

The type of error correction used by the memory module.

Data Width Bits

The memory module data width in bits.

Bus Width Bits

The memory module bus width in bits.

Viewing network information

About this task

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. Click System Information in the navigation tree, and then click the Network 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 expand or collapse the information on this page, click Expand All or Collapse All, respectively.

Subtopics

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.

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:
  - The default status is OK and the link status is displayed in iLO, if Ethernet cable is connected to network switch when system boot up.
  - iLO displays the status Unknown, if Ethernet cable is not connected to network switch when system boot up. The status will display when Ethernet cable is connected after system boot.
  - 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 OK.
  - 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.

NOTE: For complex NICs (NICs with multiple port functions like Ethernet, FCoE, and iSCSI) the adapter status indicates the status of physical ports and status of the functions running on that ports. If the functions running on any of the ports is not configured by switch or if the Fibre Channel fabric is down, the status of the adapter may indicate DEGRADED even though the status of individual physical port is OK.

Port

The configured network port. This value is displayed for system NICs (embedded and stand-up) only.

MAC Address

The port MAC address.

Status

The port status.

Possible values include OK, Failed, and Unknown, and Link Down.

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 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

About this task

HPE ProLiant RL3xx Gen 11 platforms do not support Workload performance Advisor.

The Device Inventory page displays information about devices installed in the server. 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.

For older adapters that do not comply with industry-standard management specifications, the Agentless Management Service (AMS) is required for obtaining the adapter firmware version, part number, serial number, and status.

Redfish DeviceDiscovery must reach `vMainDeviceDiscoveryComplete` state to display device inventory after host or iLO reboot.

For adapters that support the Field Replaceable Unit (FRU) EEPROM, iLO obtains static adapter details such as the product name and part number. These values are formatted according to the IPMI Platform Management FRU Information Storage Definition specification.

Procedure

1. Click System Information in the navigation tree, and then click the Device Inventory tab.
2. (Optional) By default, empty slots are hidden in the Device Inventory table. To view empty slots, click show empty slots. When empty slots are displayed, click hide empty slots to hide them.

   This option is not displayed if there are no empty slots.
3. (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.
4. (Optional) To view additional slot details, click a device in the table.

   The Slot Details pane is displayed.

Subtopics

Device Inventory details

Slot Details pane

Device status values

Configuring MCTP discovery

Initiating an MCTP factory reset

More information

Agentless Management and AMS

Device Inventory details

- MCTP Discovery—Whether this feature is enabled or disabled for the server.
- Location—The device install location.
- Product Name—The device product name.

Typically, iLO obtains this value from the FRU EEPROM (Product Info Area Format region, Product Name value).

For some adapters, this value is obtained through a proprietary adapter interface.

- Product Version—The device product version.

  Typically, iLO obtains this value from the FRU EEPROM (Product Info Area Format region, Product Version value).

  For some adapters, this value is obtained through a proprietary adapter interface.

- Firmware Version—The installed adapter firmware version.

  There are multiple methods iLO can use to obtain this adapter-specific information.

  For adapters that support the UEFI Device Driver interfaces, UEFI is the primary method for obtaining this value.

- Component Integrity Status—The SPDM authentication status of the device.

- Status—The device status value.

  The value Unknown might mean that:

  - iLO has not completed initialization for the device.
  - The device is not capable of providing status (for example, legacy chipset SAS/SATA controllers).
  - Agentless Management and the Agentless Management Service do not provide information about this device.

  For information about network adapter unknown status values, see the Network Information page documentation.

  For information about storage device unknown status values, see the Storage Information page documentation.

More information

Configuring MCTP discovery
Viewing network information
Viewing storage information

Slot Details pane

When you click a row in the Device Inventory table, more information is displayed in the Slot Details pane.

The displayed values depend on the selected device type. Some device types do not display all the listed values.

- SKU Number—The adapter vendor's primary part number.

  Typically, iLO obtains this value from the FRU EEPROM (Product Info Area Format region, Product Part/Model Number value).

  Various is displayed when the part number depends on internal graphics devices that differ by server model.

  N/A is displayed for backplanes connected to storage controllers.

- Part Number—The adapter vendor's spare part number (if available).

  If the adapter vendor's spare part number is not available, iLO obtains this value from the FRU EEPROM (Board Info Area Format region, Board Part Number value).

  N/A is displayed for backplanes connected to storage controllers.

- Serial Number—The adapter serial number.

  Typically, iLO obtains this value from the FRU EEPROM (Product Info Area Format region, Product Serial Number value).

  N/A is typically displayed for embedded devices.

- MCTP Status—Whether MCTP Discovery is enabled or disabled.

- Slot details
  - Type—The slot type, for example, PCIe, MXM, SATA, or another industry-standard slot type.
  - Bus Width—The slot bus width.
  - Length—The slot length.
  - Characteristics—Information about the slot, for example, voltage or other support information.

  For more information about the slot detail values, see System Slots (Type 9) in the System Management BIOS (SMBIOS) Reference Specification.
- Segment (PCIe devices only)—The PCI segment assigned by the BIOS during PCI configuration. For all other device types, FFh or N/A is displayed.
- Bus (PCIe devices only)—The PCI bus assigned by the BIOS during PCI configuration. For all other device types, FFh or N/A is displayed.
- Device (PCIe devices only)—The PCI device assigned by the BIOS during PCI configuration. For all other device types, FFh or N/A is displayed.
- Function (PCIe devices only)—The PCI function assigned by the BIOS during PCI configuration. For all other device types, FFh or N/A is displayed.
- Bifurcated Device Peer Instance —Bifurcation details of the devices which support bifurcation. Bifurcated Device Peer Instance indicates if the device is bifurcated and the instance of the bifurcation.

More information

Configuring MCTP discovery

Device status values

The Device Inventory page uses the following status values:

- Enabled—The device is enabled and the health status is OK.
- No Supporting CPU—The CPU that supports the device slot is not installed.
- N/A—The device is not installed.
- Enabled—The device is enabled and the health status is Critical.
- Enabled—The device is enabled and the health status is Warning.
- Unknown—The iLO firmware has not received data about the device status.
- Disabled—The device is disabled.
- Not Supported—Device does not support Security Protocol and Data Model (SPDM) authentication.
- Success—SPDM authentication of the device is successful.
- Failed—SPDM authentication of the device has failed.

Configuring MCTP discovery

Prerequisites

Configure iLO Settings privilege

About this task

MCTP is the industry standard technology iLO uses to communicate directly to options installed in the server. MCTP discovery is enabled by default. For troubleshooting of a problematic option, you can disable MCTP discovery for a server or an individual adapter. For example, if an adapter is not working, you could temporarily disable MCTP discovery to allow server operations to continue while you investigate the problem. When you disable MCTP discovery, the only way to enable it again is to perform an MCTP factory reset. An MCTP factory reset enables MCTP discovery on the server and all adapter slots.

Disabling MCTP discovery for the server automatically disables it for all adapter slots.

Hewlett Packard Enterprise recommends that you do not disable MCTP discovery unless this action is recommended by support personnel.

WARNING:

- If you disable MCTP discovery on a server managed by HPE OneView, disabled devices will be inaccessible to HPE OneView.
- When MCTP discovery is disabled for a server, iLO does not monitor or display status information for the following components: Embedded NICs, Smart Array, memory, CPU, and option adapters.
- When MCTP discovery is disabled, the Performance Settings, Performance Monitoring, and Workload Performance Advisor pages are unavailable.

Procedure

1. Click System Information in the navigation tree, and then click the Device Inventory tab.
2. Click Discovery.

   The Discovery Settings page opens.
3. To disable MCTP discovery for the server and all adapter slots, set MCTP Discovery to disabled.
4. To disable MCTP discovery on selected adapter slots, set one or more MCTP options in the Devices table to disabled.
5. Click Apply.

   iLO notifies you that an MCTP factory reset is required to re-enable MCTP discovery.
6. Click OK.

Initiating an MCTP factory reset

Prerequisites

Configure iLO Settings privilege

About this task

If MCTP discovery is disabled for a server or the adapter slots in a server, the only way to re-enable it is to perform an MCTP factory reset. This procedure does not reset iLO or the server.

Procedure

1. Click System Information in the navigation tree, and then click the Device Inventory tab.
2. Click Discovery.

   The Discovery Settings page opens.
3. Click MCTP Factory Reset.

   iLO warns you that an MCTP factory reset will enable MCTP on all devices, and prompts you to confirm the request.
4. Click Yes.

   An MCTP factory reset is initiated.

When the process is complete, MCTP discovery is enabled on all devices.

Viewing storage information

About this task

If the server is powered off, the system status information on the Storage Information page is current as of the last power off. Status information is updated only when the server is powered on and POST is complete.

To view a full set of data on the Storage Information 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.

Redfish DeviceDiscovery must reach `vMainDeviceDiscoveryComplete` state to display device inventory after host or iLO reboot.

Fibre Channel adapters are not listed on this page. To view information about Fibre Channel adapters, click System Information in the navigation tree, and then click the Network tab.

Procedure

1. Click System Information in the navigation tree, and then click the Storage tab.

   Storage Information page appears.

2. (Optional) To view component details, click a listed component from the Entity table.

   Details pane opens and displays additional information.

   NOTE: Language translation capability is not applicable to details pane.

3. (Optional) To change the physical drive indicator LED status for an NVMe or SATA drive, click the drive indicator LED icon .

   This feature is available on supported servers only.

   The Configure iLO Settings privilege is required to use this feature.

   You can change the LED status to ON or OFF.

4. (Optional) To power an NVMe or SATA drive on or off, use the Drive Power Button feature.

   This feature is available on supported servers only.

   The Configure iLO Settings privilege is required to use this feature.

Subtopics

Supported storage components

Supported storage products

Storage details

Status values and definitions

Managing drive power

More information

Viewing network information

Supported storage components

The Storage Information page displays the Entity, Count, and Health Summary information about the following storage components:

- Storage Controllers, Volumes, Storage Enclosures, Drives, Switches, and Ports.

  iLO can monitor 256 physical drives total and 256 volumes total.

- Hewlett Packard Enterprise and third-party storage controllers that manage direct-attached storage, and the attached physical drives.

  The following direct-attached storage types are supported: SATA, NVMe, and RDE-enabled devices. The information displayed depends on the storage type.

Supported storage products

- HPE ML/DL Server M.2 SSD Enablement Kit
- HPE Dual 8GB MicroSD EM USB Kit (Windows only)
- NVMe drives
- HPE NS204i-t Gen10 Plus Boot Controller
- HPE SR932i-p Gen11 Controller
- HPE SR416ie-m Gen11 Controller
- HPE E208e-p SR Gen10 Controller
- HPE MR416i-p Gen10 Plus Controller
- HPE MR216i-p Gen10 Plus Controller
- HPE MR416i-p Gen11 Controller
- HPE MR416i-o Gen11 Controller
- HPE MR408i-o Gen11 Controller
- HPE MR216i-p Gen11 Controller
- HPE MR216i-o Gen11 Controller
- AHCI SATA controllers
- Intel VROC 8.0

HPE ProLiant RL3xx Gen 11 platforms support only NVMe drives.

Storage details

The Storage Information page displays the following details about Smart Array and direct-attached storage.

NOTE:
The information displayed depends on the storage type. Some storage types do not include all the listed properties.

Subtopics

Storage Controllers

Volumes

Storage Enclosures

Drives

Storage Controllers

The Storage Controllers section displays the following details for each controller.

- Name
- Location—The controller location in the server.
- Status— A combination of the controller hardware health and the current state of the controller. The displayed value indicates a status icon (OK, Critical, or Warning), and text that provide more information.

  For more information on health and current state values and definitions, see Status values and definitions.
- Enclosures

When you select a controller, the Details pane opens and displays more information. Also, the Enclosure Chassis and **Volumes** details appears.

Enclosure Chassis

The Enclosure Chassis section displays the following for each enclosure.

- Location
- Status
- Drives
- Total Ports

When you select an enclosure, the associated **Drives**, Switches, and Ports appears.

Switches

The Switches section displays the following for each switch.

- Model
- Status
- Firmware Version

Ports

The Ports section displays the following for each port.

- Port Number
- Location
- Status
- Current Speed
- Active Width

NOTE: The Maximum link rate per lane (GT/s) mentioned in the Drive backplane naming convention is different from the Current Speed or Max Speed displayed for Ports.

For more information on Drive backplane naming, see **HPE ProLiant DL345 Gen11 Server User Guide**.

Volumes

The Volumes section displays the following details for each volume.

- Name
- Status — For more information on health and current state values and definitions, see Status values and definitions.
- Capacity
- RAID Type
- Drives
- Spares

Volumes must be configured through the Smart Storage Administrator software before they can be displayed on this page.

When you select a volume, the Details pane opens and displays more information. Also, the associated **Drives** appears.

Storage Enclosures

The Storage Enclosures section displays the following details for each enclosure. The enclosure information is available based on the controller capability to share the details of the enclosure.

- Name
- Location—The enclosure port and box numbers.
- Status— For more information on health and current state values and definitions, see Status values and definitions.
- Type
- Switches

Some enclosures do not include all the listed properties, and some storage configurations do not include drive enclosures.

When you select an enclosure, the Details pane opens and displays more information. Also, the associated **Drives**, **Switches**, and **Ports** appears.

Drives

The Drives section displays the following details for each drive.

- Location— Drive port, box, and bay numbers
- Status — For more information on health and current state values and definitions, see Status values and definitions.
- Capacity
- Type
- Media Life

When you select a drive, the Details pane opens and displays more information.

The Details pane also displays the following details about the selected drive.

- Indicator LED—The LED status (on or off). You can click  to change the LED status. This feature is available on NVMe and SATA drives.

The configure iLO Settings privilege is required to use this feature.

- Drive Power—The current drive power state (on, off, or starting).

  You can use the Power On or Power Off buttons to control Drive Power for NVMe and SATA drives.

Status values and definitions

The possible health values are:

- OK — Indicates Normal
- Critical — A critical condition exists that requires immediate attention.
- Warning — A condition exists that requires attention.

The possible state values are:

- Enabled — The device is enabled.
- Disabled — The device is disabled.
- In Test — The device is undergoing testing.
- Quiesced — The device is enabled but processes only a restricted set of command.
- Standby Offline — The device is enabled, but awaiting an external action to activate it.
- Standby Spare — The device is part of a redundancy set and is awaiting a failover or other external action to activate it.
- Starting — The device is starting.
- Unavailable Offline — The device is present but cannot be used.
- Updating — The device is updating and may be unavailable or degraded.
- Absent — The device is not present or not detected.
- Deferring — The device will not process any commands but will queue new requests.

Managing drive power

Prerequisites

- Configure iLO Settings privilege
- The server configuration supports managing drive power.

About this task

When you select a supported drive, the Drive Power Button section in the Details pane displays the current drive power state. The possible values are ON, OFF, and Starting.

You can use the Drive Power Button options to power a drive on or off.

The power off option works only with supported drive firmware.

For the list of compatible drives, see **https://ssd.hpe.com/recommendation**.

The power on option (hot-plug) is not supported on standard IDE controllers. Cold boot the system to recover the drive. See the drive specifications to determine whether a drive supports these power reset features.

Procedure

1. Click System Information in the navigation tree, and then click the Storage tab.
2. Select a drive.

   The Details pane opens.
3. Click the Power On or Power Off button.
4. When prompted to confirm the request, click OK.

Subtopics

Drive power button options

Drive power button options

- Power On—Power on the drive immediately.
- Power Off—Power off the drive immediately. Using this option results in a nongraceful shutdown.

Viewing and managing firmware and software

Subtopics

Firmware updates

iLO firmware and software management features

Viewing installed firmware information

Replacing the active system ROM with the redundant system ROM

Updating iLO or server firmware by using the flash firmware feature

Viewing software information

Maintenance windows

iLO Repository

Install sets

Installation queue

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.

Subtopics

Online firmware update

Offline firmware update

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 drivers are required for in-band firmware updates.

During a host-based firmware update, if iLO is set to the Production security state, it does not verify user credentials or privileges. The host-based utilities require a root (Linux and VMware) or Administrator (Windows) login.

When iLO is configured to use the High Security, FIPS, or CNSA security states, user credentials are required.

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 on a system that uses the Production security state, any user can update firmware with an out-of-band method. If the system is configured to use a higher security state, user credentials are required.

Subtopics

In-band firmware update methods

Out-of-band firmware update methods

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.

This option is supported when iLO is configured to use the Production security state.

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.

When you use HPONCFG 6.0.0 or later with iLO 6 1.10 or later, an error message is displayed if your user account lacks the required user privileges.

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.

Subtopics

Offline firmware update methods

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.

You can use SUM together with iLO to access the iLO Repository and manage install sets and the installation queue.

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.

iLO firmware and software management features

iLO supports the following firmware and software management features:

- Viewing installed firmware.
- Replacing the active system ROM with the redundant system ROM.
- Using the Update Firmware controls to install firmware on the local managed server.

  You can also use the Update Firmware controls to install an iLO language pack.
- Viewing installed software.
- Managing maintenance windows. You can apply maintenance windows to tasks that you add to the installation queue.
- Using the Group Firmware Update feature to install firmware on multiple servers in an iLO Federation group.
- Accessing the iLO with integrated Smart Update features. This version of iLO supports the following actions:

- View and manage the components in the iLO Repository.
- Add components from the iLO Repository to the installation queue.
- View and remove install sets and add them to the installation queue.

  Use SUM to configure install sets. For more information, see the SUM documentation.
- View the System Recovery Set or use the iLO RESTful API to create one.
- View and manage tasks in the installation queue.

  The best practice is to use SUM to manage the installation queue. For more information, see the SUM documentation.

You can access the Update Firmware, Upload to iLO Repository, and Add to Queue controls from all tabs on the Firmware & OS Software page.

For more information, see the **Firmware Updates** video.

Viewing installed firmware information

Procedure

1. Click Firmware & OS Software in the navigation tree.

   The Installed Firmware 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.

   NOTE: If a component is updated using smart component through a host system, then you might have to reset iLO or the host to view the updated firmware.

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.

Subtopics

Firmware types

Firmware details

Firmware types

The firmware types listed on the Installed Firmware page vary based on the server or chassis 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 Energy Pack
- TPM or TM firmware

- SAS Programmable Logic Device
- System Programmable Logic Device
- Intelligent Provisioning
- Networking adapters
- NVMe Backplane firmware
- Drive firmware
- Power Supply firmware
- Embedded Video Controller
- Language packs
- CPU MEZZ Programmable Logic Device (This firmware type is displayed only for supported platforms)
- Secondary System Programmable Logic Device (This firmware type is displayed only for supported platforms)
- Intel CPU Fault Resilience (CFR) (This firmware type is displayed only for supported platforms)

Firmware details

The Installed Firmware 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.

Replacing the active system ROM with the redundant system ROM

Prerequisites

- Host BIOS privilege
- The server supports redundant system ROM.

Procedure

1. Click Firmware & OS Software in the navigation tree.
2. On the Installed Firmware page, click next to the Redundant System ROM details.

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

   The change will take effect after the next server reboot.

   A server reboot initiated from iLO requires the Virtual Power and Reset privilege.

Updating iLO or server firmware by using the flash firmware feature

Prerequisites

- The Configure iLO Settings privilege is required for flashing firmware and storing components in the iLO Repository.
- The Recovery Set privilege is required for making an optional update to the System Recovery Set after a successful firmware update.
- If you want to use the Update Recovery Set feature, a System Recovery Set must exist and contain the component you want to update.

About this task

You can update firmware from any network client by using the iLO web interface. A signed file is required.

IMPORTANT:

Update Firmware option does not work for firmware packages which must be updated using UEFI or Runtime Agent.

To update such packages using iLO, you must add the packages to the iLO repository using the Upload to iLO Repository option. The packages are automatically picked up for installation during POST.

Procedure

1. Obtain a server firmware or iLO firmware file.
2. If you will update the Server Platform Services (SPS) firmware, power off the server, and then wait 30 seconds.

   The SPS firmware cannot be updated when the server OS is running.
3. Click Firmware & OS Software in the navigation tree, and then click Update Firmware.

   If the Update Firmware option is not displayed, click the ellipsis icon in the top-right corner of the iLO web interface, then click Update Firmware.
4. Select the Local file or Remote file option.
5. Depending on the option you selected, do one of the following:
   - Depending on the browser you use, click Browse or Choose File in the Local file box, and then specify the location of the firmware component.
   - In the Remote file URL box, enter the URL for a firmware component on an accessible web server.

   a. (Optional) To configure Enhanced Download Performance, click Enhanced Download Performance link.

      The **Access Settings** page is displayed. You can configure the settings on the Access Settings page.

      For more information on the option, see the help on the Access Settings page.

      NOTE: Enhanced Download Performance link is not displayed, if it is already enabled.
6. (Optional) To save a copy of the component to the iLO Repository, select the Also store in iLO Repository check box.
7. (Optional) If a version of the component you selected in step 5 exists in the System Recovery Set, select the Update Recovery Set check box to replace the existing component with the selected component.

   Selecting this option replaces the component, even if the version in the System Recovery Set is newer.

   If there is no System Recovery Set, or you are not assigned the required privilege for this action, then this option is not displayed.

   When you select this option, the Also store in iLO Repository option is selected automatically, because the System Recovery set is stored in the iLO Repository.
8. On servers with an installed TPM or TM, suspend or back up software that stores information on the TPM or TM, then select the Confirm TPM override check box.

   Drive encryption software is an example of software that stores information on the TPM or TM.

   CAUTION: 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.

9. To start the update process, click Flash.

   Depending on the server configuration, 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.

10. Click OK.

    IMPORTANT:

    Do not boot or reboot the server during a PLDM firmware update because this action might cause the server to go into standby mode for approximately 20 minutes before starting up.

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

    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.

11. For iLO firmware updates only: To start working with the new firmware, clear your browser cache, and then log in to iLO.
12. For server firmware updates only: If the firmware type requires powering on or rebooting the server or initiating a system reset, take the appropriate action.
13. (Optional) To confirm that the new firmware is active, check the firmware version on the Installed Firmware page.

    You can also check the iLO firmware version on the Overview page.

Subtopics

Obtaining the iLO firmware image file

Obtaining supported server firmware image files

Requirements for firmware update to take effect

Supported firmware types

Daily firmware flash limit

More information

Obtaining the iLO firmware image file
Obtaining supported server firmware image files
Requirements for firmware update to take effect
Installing language packs with the flash firmware feature
System Recovery Set

Obtaining the iLO firmware image file

About this task

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: **https://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:
     - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`

   The name of the iLO firmware image file is similar to `iLO6_<yyy>.bin`, where `<yyy>` represents the firmware version.

Obtaining supported server firmware image files

Procedure

1. Navigate to the following website: **https://www.hpe.com/support/hpesc**.
2. To locate and download an Online 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:
   a. For Linux components, depending on the file format, enter one of the following commands:
      - `#rpm2cpio <firmware_file_name>.rpm | cpio -id`
   b. (Optional) If you are working with Server Platform Services (SPS) firmware component, locate the `<firmware_file_name>.zip` file, and extract the binary file.

Subtopics

Server firmware file type details

Server firmware file type details

- When you update the system ROM, you must use a signed image or the signed ROMPAQ image:
  - Signed image example:

    http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash
  - Signed ROMPAQ image example:

    http://<server.example.com>/<wwwroot>/CPQPJ0612.A48
- The Power Management Controller 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`.
- The Server Platform Services (SPS) firmware files use the file extension `.bin`.
- Language Pack files use the extension `.lpk`.

Requirements for firmware update to take effect

Depending on the firmware type, additional action might be required for the update to take effect.

- iLO firmware or language pack—These firmware types take effect after an automatically triggered iLO reset.
- System ROM (BIOS)—Requires a server reboot.
- System Programmable Logic Device (CPLD)—Requires a server reboot.

  NOTE:

  A server reboot after a CPLD firmware update is converted to a server AC power cycle. iLO will reset as part of the AC power cycle.

- 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.

- Server Platform Services (SPS)—These firmware types require that you power off the server before installation. The changes take effect after you power on the server.

Supported firmware types

Many firmware update types are supported, depending on the server platform. Some common examples follow:

- iLO
- System ROM/BIOS
- Power Management Controller
- System Programmable Logic Device (CPLD)
- Backplane
- Server Platform Services (SPS)
- Language Packs
- Third-party firmware packages

  Platform Level Data Model (PLDM) firmware packages are supported if the Accept 3rd Party Firmware Update Packages option is enabled on the Access Settings page.

  HPE ProLiant RL3xx Gen 11 platforms do not support PLDM.

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.

Daily firmware flash limit

To protect the iLO and server hardware from repeated flashing attacks, iLO limits the number of times per day that you can flash each supported firmware type. The limit is 20, which includes both successful and failed firmware flash activities. The firmware flash count is

reset every 24 hours, or 24 hours after a successful firmware update. The firmware flash limit applies to firmware updates initiated through any application or interface.

The firmware flash count is stored in the nonvolatile memory. If the flash limit is exceeded, the firmware cannot be flashed, and the software notifies you that you must try again later.

When a firmware update fails, an event is logged in the iLO event log.

Flash limit process example

1. At 10 a.m. on Monday, the BIOS firmware is flashed for the first time since the previous Friday.
2. During the firmware flash, iLO checks the BIOS firmware flash limit time stamp.

   In this example, the last firmware flash is more than 24 hours ago, and the firmware flash count is reset to 1.
3. Later on Monday, the BIOS firmware is flashed 19 more times.

   Each flash activity increments the flash count to a total of 20.
4. Before leaving work on Monday, the BIOS firmware is flashed again, and the update fails, due to the flash limit.

   This failure persists until the next morning at 10 a.m., when the flash count is reset.

Viewing software information

Prerequisites

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

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Software tab.
2. (Optional) To update the software information data, click .

   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 to update the page with the latest information.
3. (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.

HPE Software details

This section lists all the HPE software on the managed server. The list includes Hewlett Packard Enterprise and Hewlett Packard Enterprise-recommended third-party software that was added manually or by using the SPP.

- Name—The name of the software.
- Version—The software version.

  The versions of the displayed firmware components indicate the firmware versions available in the firmware flash components that are saved on the local OS. The displayed version might not match the firmware running on the server.
- Description—A description of the software.

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.
- Path—The file path of the software.

Installed Software details

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

Maintenance windows

A maintenance window is a configured time period that applies to an installation task.

You can create a maintenance window:

- On the Maintenance Windows tab.
- When you add a task to the installation queue.

Adding a maintenance window

Prerequisites

Configure iLO Settings privilege

About this task

iLO supports a maximum of eight maintenance windows.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Maintenance Windows.
2. Click +.

   iLO prompts you to enter the maintenance window information.
3. Enter a name in the Name box.
4. Enter a description in the Description box.
5. Enter the maintenance window start and end times in the From and To boxes.
   a. Click in the From box.

      A calendar is displayed.
   b. Select a start date and time, and then click Done.
   c. Click in the To box.

      A calendar is displayed.
   d. Select the end date and time, and then click Done.

   Enter the date and time based on the local time on the client you are using to manage iLO.

   The equivalent UTC value is displayed above the date and time you entered.

   If you enter a To value that occurs before the start time of an existing task, iLO prompts you to enter a different value. The installation queue is a first-in, first-out list of tasks, and you cannot create a maintenance window that will expire before an existing task will run.
6. Click Add.

   The maintenance window is added.

Editing a maintenance window

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Maintenance Windows.
2. Click  .

   iLO prompts you to update the maintenance window information.
3. Update the maintenance window name in the Name box.
4. Update the description in the Description box.
5. Update the maintenance window start and end times in the From and To boxes.
   a. Click  in the From box.

      A calendar is displayed.
   b. Select a start date and time, and then click Done.
   c. Click  in the To box.

      A calendar is displayed.
   d. Select the end date and time, and then click Done.

   Enter the date and time based on the local time on the client you are using to manage iLO.

   The equivalent UTC value is displayed above the date and time you entered.

   If you enter a To value that occurs before the start time of an existing task, iLO prompts you to enter a different value. The installation queue is a first-in, first-out list of tasks, and you cannot create a maintenance window that will expire before an existing task will run.
6. Click OK.

   The maintenance window is updated.

Removing a maintenance window

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Maintenance Windows.
2. Click  next to the maintenance window you want to remove.

   iLO prompts you to confirm that you want to remove the maintenance window.
3. Click Yes, remove.

   The maintenance window is removed.

   All tasks associated with the removed maintenance window are canceled.

Removing all maintenance windows

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Maintenance Windows.
2. Click Remove all.

   iLO prompts you to confirm that you want to remove all maintenance windows.

3. Click Yes, remove all.

   The maintenance windows are removed.

   All tasks associated with the removed maintenance windows are canceled.

Viewing maintenance windows

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Maintenance Windows.
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) Click an individual maintenance window to view detailed information.

Maintenance window summary details

The Maintenance Windows tab displays the iLO Date/Time and the following details about each configured maintenance window:

- Name—The user-defined name for the maintenance window.
- Start time—The maintenance window start time (UTC).
- End time—The maintenance window end time (UTC).

Maintenance windows are automatically deleted 24 hours after they expire.

Individual Maintenance Window details

When you click an individual maintenance window, the following details are displayed:

- Name—The user-defined name for the maintenance window.
- Start—The maintenance window start time (UTC).
- End—The maintenance window end time (UTC).
- Description—A description of the maintenance window.

iLO Repository

The iLO Repository is a secure storage area in the nonvolatile flash memory embedded on the system board. The nonvolatile flash memory is 1 gigabyte in size and is called the iLO NAND. Use SUM or iLO to manage signed software and firmware components in the iLO Repository.

iLO, the UEFI BIOS, SUM, and other client software can retrieve these components and apply them to supported servers. Use SUM to organize the stored components into install sets and SUM or iLO to manage the installation queue.

To learn more about how iLO, SUM, and the BIOS software work together to manage software and firmware, see the **SUM documentation**.

HPE ProLiant RL3xx Gen 11 platforms do not support SUM.

Adding a component to the iLO Repository

Prerequisites

- The Configure iLO Settings privilege is required for uploading files to the iLO Repository.
- The Recovery Set privilege is required for making an optional update to the System Recovery Set after you upload a file to the iLO Repository.
- If you want to use the Update Recovery Set feature, a System Recovery Set must exist and contain the component you want to update.

About this task

Use the Upload to iLO Repository pane to add components to the iLO Repository. The Upload to iLO Repository pane is available whenever you view a tab on the Firmware & OS Software page.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Upload to iLO Repository.

   If the browser window is a small size, and the Upload to iLO Repository option is not displayed, click the ellipsis icon in the top right corner of the iLO web interface, then click Upload to iLO Repository.

2. Select the Local file or Remote file option.

3. Depending on the option you selected, do one of the following:

   - In the Local file box, click Browse or Choose File (depending on your browser), and then specify the location of the firmware component.
   - In the Remote file URL box, enter the URL for a firmware component on an accessible web server.

   a. (Optional) To configure Enhanced Download Performance, click Enhanced Download Performance link.

      The **Access Settings** page is displayed. You can configure the settings on the Access Settings page.

      For more information on the option, see the help on the Access Settings page.

      NOTE: Enhanced Download Performance link is not displayed, if it is already enabled.

4. For firmware components specified by multiple files only: Select the I have a component signature file check box.

5. If you selected the check box in step 4, do one of the following:

   - In the Local signature file box, click Browse or Choose File (depending on your browser), and then specify the location of the component signature file.
   - In the Remote signature file URL box, enter the URL for a component signature file on an accessible web server.

6. (Optional) If a version of the component you selected in step 3 exists in the System Recovery Set, select the Update Recovery Set check box to replace the existing component with the selected component.

   Selecting this option replaces the component, even if the version in the System Recovery Set is newer.

   If there is no System Recovery Set, or you are not assigned the required privilege for this action, then this option is not displayed.

7. Click Upload.

   iLO notifies you that uploading a component with the same name as an existing component will replace the existing component.

8. Click OK.

   The upload starts. The upload status is displayed at the top of the iLO web interface.

More information

Obtaining the iLO firmware image file
Obtaining supported server firmware image files
System Recovery Set

Installing a component from the iLO Repository

Prerequisites

Configure iLO Settings privilege

About this task

You can add a component to the installation queue from the iLO Repository page.

When you add a component to the installation queue, a task is added to the end of the queue. After other queued tasks are complete, the

added component is installed when the software that initiates updates for the component type detects the installation request. To determine the software that can initiate an update, check the component details on the iLO Repository and Installation Queue pages.

If a previously queued task is waiting to start or finish, a new task might be delayed indefinitely. For example, if a queued component is installable by the UEFI BIOS, a server restart is required before installation can start. If the server is not restarted, the tasks that follow in the queue are delayed indefinitely.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click iLO Repository.
2. Click  next to the component you want to install.

   The Install Component pane opens and prompts you to confirm the request.

   While adding the Firmware package 2.0 from the repository to the `install queue` through iLO web interface, iLO creates multiple tasks based on the package `UpdatableBy` field values, ex, BMC, and UEFI. Then iLO creates tasks for BMC and UEFI. If there are no devices `UpdatableBy` the BMC or UEFI, either of the tasks becomes in exception state. You must manually clear the task to execute the remaining tasks in the queue.
3. (Optional) If you want to specify an installation schedule, select the Set schedule window check box.
   a. Select a method for defining the schedule.
      - Select Use maintenance window (default) to choose a maintenance window you configured on the Maintenance Windows page.

        To add a maintenance window, click New to navigate to the Maintenance Windows page. Create a maintenance window, and then restart this procedure.
      - Select Specify time window to enter a schedule now.

   b. Depending on the method you selected, do one of the following:
      - If you selected Use maintenance window, select a value in the Maintenance window list.
      - If you selected Specify time window, enter the schedule details.
4. Click Yes, add to the end of the queue .

   If the installation queue is empty, and iLO can initiate the component installation, the button is labeled Yes, install now.

   The update is initiated after existing queued tasks finish and the software that initiates installation for the selected component type detects a pending installation.

   If the installation queue is empty and iLO can initiate the update, the update begins immediately.

More information

Adding a component to the iLO Repository
Viewing iLO Repository summary and component details
Viewing the installation queue
Daily firmware flash limit
Obtaining the iLO firmware image file
Obtaining supported server firmware image files

Entering time window details when installing a component

Prerequisites

Configure iLO Settings privilege

About this task

Use this procedure to enter the schedule when Specify Time Window is selected.

Procedure

1. Click  in the From box.

   A calendar is displayed.

2. Select a start date and time, and then click Done.

   The selected date and time are displayed in the From box.

3. Click in the To box.

   A calendar is displayed.

4. Select an end date and time, and then click Done.

   This value sets the expiration date and time for the tasks in the install set.

   The selected date and time are displayed in the To box.

Removing a component from the iLO Repository

Prerequisites

- Configure iLO Settings privilege
- The component is not in an install set.
- The component is not part of a queued task.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the iLO Repository tab.
2. Click .

   iLO prompts you to confirm the request.

3. Click Yes, remove.

   The component is removed.

Removing all components from the iLO Repository

Prerequisites

- Configure iLO Settings privilege
- The components are not in an install set.
- The components are not part of a queued task.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the iLO Repository tab.
2. Click Remove all.

   iLO prompts you to confirm the request.

3. Click Yes, remove all.

   The components are removed.

Viewing iLO Repository summary and component details

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the iLO Repository 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 view detailed component information, click an individual component.

iLO Repository storage details

The Summary section of the iLO Repository page displays the following details about the iLO Repository storage use:

- Capacity—Total iLO Repository storage capacity
- In use—Used storage
- Free space—Available iLO Repository storage
- Components—Number of saved components in the iLO Repository

iLO Repository contents

The Contents section of the iLO Repository page displays the following details about each firmware or software component:

- Name
- Version

iLO Repository individual component details

When you click an individual component, the following details are displayed:

- Name—Component name
- Version—Component version
- File name—Component file name
- Size—Component size
- Uploaded—Upload date and time
- Installable by—The software that can initiate an update with the component.
- In use by install set or task? —Whether the component is part of an install set or queued task.

  When a component is part of an install set or queued task, you can click the install set or task name link to view the install set details or queued task details.

Install sets

An install set is a group of components that can be applied to supported servers with a single command. SUM determines what to install on a server and creates an install set that is copied to iLO. You can view existing install sets on the Install Sets page in the iLO web interface.

Saving an install set when you deploy from SUM keeps all the components on the iLO system for later use. For example, you could use the saved components to restore or roll back a component version without needing to find the original SPP.

To learn more about how iLO, SUM, and the BIOS software work together to manage software and firmware, see the **SUM documentation**.

HPE ProLiant RL3xx Gen 11 platforms do not support SUM and Intelligent Provisioning.

Installing an install set

Prerequisites

- Configure iLO Settings privilege
- No components in the install set are queued as part of another installation task.

About this task

You can add an install set to the installation queue from the Install Sets page.

When you add an install set to the installation queue, iLO adds a task for each component or command in the install set. The new tasks are

added to the end of the queue.

Components in the queue are installed after other queued tasks are complete, and when the software that initiates updates for the component type detects the installation request. To determine the software that can initiate an update, check the component details on the iLO Repository and Installation Queue pages.

If a previously queued component is waiting to start or finish, a new task might be delayed indefinitely. For example, if a queued component is installable by the UEFI BIOS, a server restart is required before installation can start. If the server is not restarted, the tasks that follow in the queue are delayed indefinitely.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Install Sets.
2. Click next to the install set you want to install.

   The Install Components pane opens and prompts you to confirm the request.
3. (Optional) If you want to specify a schedule for installation, select the Set schedule window check box.
   a. Select a method for defining the schedule.
      - Select Use maintenance window (default) to choose a maintenance window you configured on the Maintenance Windows page.

        To add a maintenance window, click New to navigate to the Maintenance Windows page. Create a maintenance window, and then restart this procedure.
      - Select Specify time window to enter a schedule now.

   b. Depending on the method you selected, do one of the following:
      - If you selected Use maintenance window, select a value in the Maintenance window list.
      - If you selected Specify time window, enter the schedule details.
4. (Optional) If there are existing queued tasks, select the Clear installation queue check box if you want to remove them.

   When there are existing tasks, iLO displays the number of queued tasks and notifies you that the install set contents will be added to the end of the queue.

   This check box is not displayed when the queue is empty and iLO can initiate the updates in the install set.

   This check box is disabled when the queue is empty and iLO cannot initiate the updates in the install set.
5. Click Yes, add to the end of the queue .

   If you selected the check box in step 4 or the queue was already empty, and iLO can initiate the updates in the install set, the button label is Yes, install now.

   The updates are initiated after existing queued tasks finish and the software that initiates installation for the selected component types detects a pending installation.

   If the installation queue is empty and iLO can initiate the requested updates, the updates begin immediately.

More information

Viewing the installation queue

Entering time window details when installing an install set

Prerequisites

Configure iLO Settings privilege

About this task

Use this procedure to enter the schedule when Specify Time Window is selected.

Procedure

1. Click in the From box.

A calendar is displayed.

2. Select a start date and time, and then click Done.

   The selected date and time are displayed in the From box.

3. Click in the To box.

   A calendar is displayed.

4. Select an end date and time, and then click Done.

   This value sets the expiration date and time for the tasks in the install set.

   The selected date and time are displayed in the To box.

Removing an install set

Prerequisites

- Configure iLO Settings privilege for unprotected install sets.
- Configure iLO Settings privilege and Recovery Set privilege for removing the protected install set.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Install Sets.
2. Click next to the install set that you want to remove.

   iLO prompts you to confirm the request.

3. Click Yes, remove.

   The install set is removed.

Removing all install sets

Prerequisites

- Configure iLO Settings privilege
- The Recovery Set privilege is required for including the System Recovery Set in a request to remove all install sets.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Install Sets tab.
2. Click Remove all.

   iLO prompts you to confirm the request.

3. (Optional) If a System Recovery Set exists, select the Also remove protected Recovery Set check box if you want to remove the Recovery Set.

   This option is not displayed if your user account is not assigned the Recovery Set privilege.

4. Click Yes, remove all.

   The install sets are removed.

Viewing install sets

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Install Sets 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) Click an install set to view detailed information.

Install set summary details

The Install Sets tab displays the following details about each install set:

- Name—The install set name.
- Components/Commands—The components and commands in the install set. Version information is included for all components.

You can use the install set icons to add an install set to the installation queue or to delete an install set. The protected install set is displayed with a lock icon.

More information

Installing an install set
Removing an install set

Individual install set details

When you click an individual install set, the following details are displayed:

- Name—The install set name.
- Created—The creation date and time.
- Description—A description of the install set.
- Component/Commands—The components and commands in the install set. Version information is included for all components.

  When an install set contains components, you can click the component name link to view the component details in the iLO Repository.
- System Recovery Set?—Indicates whether the install set is designated as the System Recovery Set.

  The System Recovery Set is used for runtime firmware recovery operations. Only one System Recovery Set can exist at a time.

System Recovery Set

By default, a System Recovery Set is included with every server. User accounts with the **Recovery Set** privilege can configure this install set. Only one System Recovery Set can exist at a time.

The following firmware components are included in the default System Recovery Set for Intel servers:

- System ROM (BIOS)
- iLO firmware
- System Programmable Logic Device (CPLD)
- Server Platform Services (SPS) Firmware
- Server Platform Services Full Recovery Image

The following firmware components are included in the default System Recovery Set for AMD servers:

- System ROM (BIOS)
- iLO firmware
- System Programmable Logic Device (CPLD)

If the default System Recovery Set is deleted:

- A user with the Recovery Set privilege can use the iLO RESTful API and the RESTful Interface Tool to create a System Recovery Set from components stored in the iLO Repository.
- A user with the Recovery Set privilege can use SUM to create an install set, and then designate it as the System Recovery Set by using the iLO RESTful API.

More information

Creating a System Recovery Set

Creating a System Recovery Set

Prerequisites

- Recovery Set privilege
- A System Recovery Set does not exist on the server.
- The RESTful Interface Tool is installed.

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

About this task

If the System Recovery Set is deleted, you can use the iLO RESTful API and RESTful Interface Tool to create a new set from components stored in the iLO Repository.

NOTE: To simply replace an individual component in an existing System Recovery Set, you can add the component to the iLO Repository, and select the Update Recovery Set check box.

Procedure

1. Download the firmware components that you want to include in the System Recovery Set.

   The System Recovery Set typically includes the following components:

   - iLO firmware
   - System ROM/BIOS
   - System Programmable Logic Device (CPLD)
   - Server Platform Services (SPS)
2. Extract the required files from the downloaded components.
3. Add the firmware components to the iLO Repository.
4. Open a text editor and create a file to define the System Recovery Set.

   This file includes a name and description, assigns the `IsRecovery` property, and lists the components to add. Add the components in the order in which they will be installed when the install set is used.

   Use the following example as a template. Your content might be different, depending on the component versions you downloaded.

```
{
    "Description": "Essential system firmware components",
    "IsRecovery": true,
    "Name": "System Recovery Set",
    "Sequence": [
        {
             "Command": "ApplyUpdate",
             "Filename": "ilo6_110.bin",
             "Name": "System Recovery Set item (iLO 6)",
             "UpdatableBy": [
                 "Bmc"
             ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "A55_1.10_10_14_2022.signed.flash",
            "Name": "System Recovery Set item (System ROM)",
            "UpdatableBy": [
```

```
                "Bmc"
            ]
        },
        {
            "Command": "ApplyUpdate",
            "Filename": "CPLD_DL385_DL365_gen11_v0A0A_full_signed.vme",
            "Name": "System Recovery Set item (System Programmable Logic Device)",
            "UpdatableBy": [
                "Bmc"
            ]
        }

    ]
}
```

5. Save the file as a JSON file. For example, system_recovery_set.json.
6. Start the RESTful Interface Tool.

   To view help content about working with install sets, enter `ilorest installset -help`.

   For more information, see the following website: **https://www.hpe.com/support/restfulinterface/docs**.
7. Enter the command to create the System Recovery Set:

```
C:\WINDOWS\system32>ilorest installset add <JSON file location>\<JSON file name>
-u <iLO login name> -p <iLO password> --url=<iLO hostname or IP address>
```

8. (Optional) To view the install set you created, enter the following command:

```
ilorest installset -u <iLO login name> -p <iLO password> --url=<iLO hostname or IP address>
```

   The install sets on the server are displayed along with the components they contain.

More information

Obtaining the iLO firmware image file
Obtaining supported server firmware image files
Adding a component to the iLO Repository

Installation queue

The installation queue is an ordered list of components and commands that were added to the queue individually or as parts of an install set. You can add tasks to the queue by using the following methods:

- Use the iLO Add to Queue pane.
- Click + on the Installation Queue page.
- Click on the iLO Repository page.
- Use SUM.

HPE ProLiant RL3xx Gen 11 platforms do not support SUM.

Subtopics

Adding a task to the installation queue

Editing a task in the installation queue

Removing a task from the installation queue

Removing all tasks from the installation queue

Viewing the installation queue

More information

Adding a task to the installation queue
Installing a component from the iLO Repository

Adding a task to the installation queue

Prerequisites

- The Configure iLO Settings privilege is required for adding tasks to the installation queue.
- The Recovery Set privilege is required for making an optional update to the System Recovery Set after a queued update is completed successfully.
- If you want to use the Update Recovery Set feature, a System Recovery Set must exist and contain the component you want to update.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Installation Queue tab.
2. Click + or click Add to Queue.

   The Add to Queue pane is available whenever you view a tab on the Firmware & OS Software page. If the browser window is a small size, and the Add to Queue option is not displayed, click the ellipsis icon in the top right corner of the iLO web interface, then click Add to Queue.

   While adding the Firmware package 2.0 from the repository to the `install queue` through iLO web interface, iLO creates multiple tasks based on the package `UpdatableBy` field values, ex, BMC, and UEFI. Then iLO creates tasks for BMC and UEFI. If there are no devices `UpdatableBy` field values the BMC or UEFI, either of the tasks becomes in exception state. You must manually clear the task to execute the remaining tasks in the queue.

   iLO prompts you to add task information.
3. Enter a task name (up to 64 characters) in the Task name box.
4. Select a value in the Component/Command box.

   The list includes the following:

   - Components stored in the iLO Repository.
   - The Wait and Reset iLO commands.
5. If the Wait command is selected, enter the wait time in the Wait time (seconds) box.

   Valid values are from 1 to 3600 seconds.
6. (Optional) If you want to specify an installation schedule, select the Set schedule window check box.
   a. Select a method for defining the schedule.
      - Select Use maintenance window (default) to choose a maintenance window you configured on the Maintenance Windows page.

        To add a maintenance window, click New to navigate to the Maintenance Windows page. Create a maintenance window, and then restart this procedure.
      - Select Specify time window to enter a schedule now.
   b. Depending on the selected method, do one of the following:
      - If you selected Use maintenance window, select a value in the Maintenance window list.

- If you selected Specify time window, enter the schedule details.

7. (Optional) If you selected a component in step 4, and the component exists in the System Recovery Set, select the Update Recovery Set check box to replace the existing component with the selected component.

   Selecting this option replaces the component, even if the version in the System Recovery Set is newer.

   This option is not displayed if:

   - A command is selected.
   - There is no System Recovery Set.
   - Your user account is not assigned the required privilege.

8. If the server has a TPM or TM, suspend or back up any software that stores information on the TPM or TM, then select the Confirm TPM override check box.

   Drive encryption software is an example of software that stores information on the TPM or TM.

   > **CAUTION:** 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.

9. Click Add to Queue.

   iLO notifies you that the task was added to the end of the installation queue. This event is recorded in the iLO event log.

   If the task would expire before the start time of an existing task that precedes it in the queue, iLO notifies you that it cannot save the task. The installation queue is a first-in, first-out list of tasks, and you cannot create a task that will expire before an existing task will run.

   If you selected the Update Recovery Set check box, the component is updated after the task is initiated and completed successfully.

Subtopics

Commands that can be added to the installation queue

Entering time window details when queuing a task

How tasks in the installation queue are processed

More information

Adding a maintenance window
Entering time window details when queuing a task
Commands that can be added to the installation queue
System Recovery Set
How tasks in the installation queue are processed

Commands that can be added to the installation queue

Wait

Causes the installation queue to stop and wait for the configured amount of time (seconds). Valid values are from 1 second to 3600 seconds.

Reset iLO

Resets (reboots) iLO.

This command does not make any configuration changes, but ends all active connections to the iLO firmware.

Entering time window details when queuing a task

Prerequisites

Configure iLO Settings privilege

About this task

Use this procedure to enter the schedule when Specify Time Window is selected.

Procedure

1. Click in the From box.

   A calendar is displayed.

2. Select a start date and time, and then click Done.

   The selected date and time are displayed in the From box.

3. Click in the To box.

   A calendar is displayed.

4. Select an end date and time, and then click Done.

   This value sets the task expiration date and time.

   The selected date and time are displayed in the To box.

How tasks in the installation queue are processed

When you add a task to the installation queue:

- It is added to the end of the queue.
- If you added a command, the task is initiated after existing queued tasks finish.
- If you added a component, the task is initiated after:
  - Existing queued tasks finish.
  - The software that initiates installation for the selected component type detects a pending installation.

  If the installation queue is empty and iLO can initiate the update, the update begins immediately.

  To determine the software that can initiate an update, check the component details on the iLO Repository and Installation Queue pages.
- If a previously queued task is waiting to start or finish, a new task might be delayed indefinitely. For example, there might be a queued component waiting until the UEFI BIOS detects it during server POST. If the server is not restarted, the tasks that follow this task in the queue will remain on hold indefinitely.
- If the task expires before the start time of a task that precedes it in the installation queue, iLO will not save the task.
- If an update is not initiated within the specified time window, it expires. If the update expires, delete and then recreate the task, or edit the task.

More information

Viewing iLO Repository summary and component details
Viewing the installation queue

Editing a task in the installation queue

Prerequisites

- The Configure iLO Settings privilege is required for editing tasks in the installation queue.
- The Recovery Set privilege is required for making an optional update to the System Recovery Set after a queued update is completed successfully.
- If you want to use the Update Recovery Set feature, a System Recovery Set must exist and contain the component you want to update.
- The task you want to edit is in Pending status.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Installation Queue tab.
2. Click  next to the task you want to edit.

   iLO prompts you to update the task information.
3. To update the task name, enter a new name (up to 64 characters) in the Task name box.
4. Select a value in the Component or Command box.
   - If the original task is a component update, you can select only another component.
   - If the original task is a command, you can select only another command.
5. If the Wait command is selected, enter or update the wait time in the Wait time (seconds) box.

   Valid values are from 1 to 3600 seconds.
6. (Optional) If you want to specify or edit the installation schedule, select or clear the Set schedule window check box.
   a. If the Set schedule window check box is selected, select or update the method you want to use to define the schedule.
      - Select Use maintenance window (default) to choose a maintenance window you configured on the Maintenance Windows page.

        To add a maintenance window, click New to navigate to the Maintenance Windows page. Create a maintenance window, and then restart this procedure.
      - Select Specify time window to enter a schedule now.

   b. Depending on the selected method, do one of the following:
      - If Use maintenance window is selected, select or change the value in the Maintenance window list.
      - If Specify time window is selected, add or update the schedule details.
7. (Optional) If you selected a component in step 4, and the component exists in the System Recovery Set, select or clear the Update Recovery Set check box.

   When this option is enabled, the existing component in the System Recovery Set is replaced by the selected component when the task is complete.

   Selecting this option replaces the component, even if the version in the System Recovery Set is newer.

   This option is not displayed if:
   - A command is selected.
   - There is no System Recovery Set.
   - Your user account is not assigned the required privilege.
8. If the server has a TPM or TM, suspend or back up any software that stores information on the TPM or TM, then select the Confirm TPM override check box.

Drive encryption software is an example of software that stores information on the TPM or TM.

> **CAUTION:** 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.

9. Click OK.

   iLO notifies you that the task was updated.

   If the task would expire before the start time of a task that precedes it in the queue, iLO notifies you that it cannot save the task. The installation queue is a first-in, first-out list of tasks, and you cannot create a task that will expire before an existing task will run.

   If you selected the Update Recovery Set check box, the component is updated after the task is initiated and completed successfully.

More information

Adding a maintenance window
Entering time window details when queuing a task
Commands that can be added to the installation queue
System Recovery Set
How tasks in the installation queue are processed

Removing a task from the installation queue

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click Installation Queue.
2. Click the remove component icon .

   iLO prompts you to confirm the request.
3. Click Yes, remove.

   The component is removed.

Removing all tasks from the installation queue

Prerequisites

- Configure iLO Settings privilege
- The component is not in an install set.
- The component is not part of a queued task.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Installation Queue tab.
2. Click Remove all.

   iLO prompts you to confirm the request.
3. Click Yes, remove.

   The tasks are removed.

Viewing the installation queue

About this task

The Installation Queue page displays summary information for each queued task, and you can click an individual task for more information. The current iLO Date/Time value is displayed at the top of the page.

Procedure

1. Click Firmware & OS Software in the navigation tree, and then click the Installation Queue tab.
2. (Optional) To view detailed information, click an individual task.

Subtopics

Queued task summary details

Individual task details

Queued task summary details

State

Status of the task. The possible values follow:

- Pending—The task will run when the software that initiates updates for the component type detects the installation request.
- In progress—The task is being processed.
- Complete—The task completed successfully.
- Canceled—The task is associated with a canceled or expired maintenance window.
- Expired—The task is expired. Subsequent tasks will not run until this task is removed from the queue.
- Exception—The task could not complete. Subsequent tasks will not run until this task is removed from the queue.

Name

The task name.

Starts

The task start date and time (UTC). If the task is waiting for other tasks to complete, the value is After previous tasks are executed.

The value N/A is displayed for tasks that are in the following states: Complete, Expired, or Exception.

Expires

The task expiration date and time (UTC). If no expiration date is set, the value Never is displayed.

Individual task details

Name

The task name.

Command

If a command is selected, this value is the command name. For example, Wait or iLO Reset.

If a component is selected, the value Apply Update is displayed.

Component name

The component name, when a component from the iLO Repository is selected.

You can click the component name link to view the component details in the iLO Repository.

File name

The component file name, when a component from the iLO Repository is selected.

State

Task status. The possible values are Pending, In progress, Complete, Canceled, Expired, or Exception.

Wait time (seconds)

The wait time in seconds, if the task is a Wait command.

Result

Task results, if available. For example, The task completed successfully or The update failed with a component specific error. Retry the update after fixing the component error.

Installable by

The software that can initiate an update with the selected component. For example, iLO, **Smart Update Tool**, or UEFI BIOS.

Smart Update Tool (SUT) does not support HPE ProLiant RL3xx Gen 11 platforms.

Maintenance Window

The maintenance window name if the task is configured to run during a maintenance window.

Start time

The task start date and time (UTC).

- If a time window is specified, the start time is listed.
- If a maintenance window is selected, the maintenance window start time is listed.
- If a start time is not specified and the task state is Complete, Expired, or Exception, the value N/A is displayed.
- If a start time is not specified and the task state is InProgress or Pending:
  - The value Immediately after the associated updater checks is displayed when the task is first in the queue.
  - The value After previous tasks are executed is displayed if the task is not first in the queue.

Expiration

The task expiration date and time (UTC).

If a maintenance window is selected, the maintenance window end time is listed.

Update Recovery Set?

This value is displayed only when a component is selected. A value of Yes means that the queued component will replace the component in the System Recovery Set after the task is initiated and completed successfully.

Created by user with Recovery Set privilege?

This value is displayed only when a component is selected. A value of Yes indicates that the task was created by a user with the Recovery Set privilege.

This privilege is required for making an optional update to the System Recovery Set after a queued update is completed successfully.

This privilege is also required for firmware downgrades when the Downgrade Policy is set to the Downgrade requires Recovery Set privilege option.

Configuring and using iLO Federation

Subtopics

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 iLO Federation groups.

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 iLO Federation group is retrieved.

iLO supports the following features:

- Group health status—View server health and model information.
- Group virtual media—Connect URL-based media for access by a group of servers.
- Group power control—Manage the power status of a group of servers.
- Group firmware update—Update the firmware of a group of servers.
- Group license installation—Enter a license key to activate iLO licensed features on a group of servers.
- 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.

HPE ProLiant RL3xx Gen 11 platforms do not support iLO Federation.

Configuring iLO Federation

Subtopics

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.

iLO Federation network requirements

- (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, disable the iLO Client Applications use IPv6 first option on the IPv6 Settings 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.

Configuring the iLO Federation multicast options

Prerequisites

Configure iLO Settings privilege

About this task

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.

Procedure

1. Click iLO Federation in the navigation tree.

   The Setup tab is displayed.

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.

Subtopics

Multicast options

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

Subtopics

iLO Federation group characteristics

iLO Federation group memberships for local iLO systems

iLO Federation group memberships for a set of iLO systems

iLO Federation group privileges

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 RIBCL XML scripts to view and configure group memberships.

  For more information, see the iLO Federation user guide.
- You can use the iLO RESTful API to configure group memberships.

  For more information, see the iLO Federation user guide.
- Hewlett Packard Enterprise recommends installing the same version of the iLO firmware on iLO systems that are in the same iLO Federation group.

iLO Federation group memberships for local iLO systems

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

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

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

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

Group memberships for the local iLO system are configured on the iLO Federation page Setup tab.

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 a system is added to a group, the group can be granted the following privileges:

- Login— Group members can log in to iLO.
- Virtual Power and Reset—Group members can power-cycle or reset the host system. These activities interrupt the system availability.
- Virtual Media—Group members can use URL-based virtual media with the managed server.
- Configure iLO Settings—Group members can configure iLO settings and remotely update firmware.

In addition, the following privileges can also be granted to the group. However, the current iLO Federation feature set does not support actions that require them:

- Administer User Accounts—Supports actions that require the Administer User Accounts privilege.
- Remote Console—Supports actions that require the Remote Console privilege.
- Host BIOS—Supports actions that require the Host BIOS privilege.
- Host NIC—Supports actions that require the Host NIC privilege.
- Host Storage—Supports actions that require the Host Storage privilege.
- Recovery Set—Supports actions that require the Recovery Set privilege.

Managing iLO Federation group memberships (local iLO system)

Subtopics

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. Click iLO Federation in the navigation tree.

   The Setup tab is displayed.

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.

   If Password Complexity is enabled on the local iLO system, the group key must meet the password complexity requirements.
5. Select the privileges to assign to the group.

   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 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. Click iLO Federation in the navigation tree.

   The Setup tab displays the existing group memberships for the local iLO system.
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, select the Change Group Key check box, then 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.

   If Password Complexity is enabled on the local iLO system, the group key must meet the password complexity requirements.
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. Click iLO Federation in the navigation tree.

   The Setup tab shows the group memberships for the local iLO system.

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 Yes, delete.

Viewing iLO Federation group memberships (local iLO system)

Procedure

Click iLO Federation in the navigation tree.

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. Assigned privileges are displayed with a check mark icon and unassigned privileges are displayed with an X icon.

Adding iLO Federation group memberships (multiple iLO systems)

Subtopics

Adding a group based on an existing 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: **https://www.hpe.com/support/ilo-docs**.
- At least one iLO Federation group exists.

About this task

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.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Configuration tab.
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. Click Create Group on Affected Systems .

   The Create Group interface opens.

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.

   If Password Complexity is enabled on systems in the existing group, and the group key does not meet the password complexity requirements, those systems cannot be added to the new group.

   in the existing group, and the group key does not meet the password complexity requirements, those systems cannot be added to the new 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. Select the privileges to assign to the group.

   To select all available privileges, click the select all check box.

8. 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

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: **https://www.hpe.com/support/ilo-docs**.
- At least one iLO Federation group exists.

About this task

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.

Procedure

1. Create a set of systems by using the filters on the iLO Federation pages.
2. Click iLO Federation in the navigation tree, and then click the Group Configuration tab.

   The active filters are listed above the Affected Systems list.

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. Click Create Group on Affected Systems .
5. 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.
6. 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.

   If there are systems in the filtered list that have Password Complexity enabled, and the group key does not meet the password complexity requirements, those systems cannot be added to the new 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. Select the privileges to assign to the group.

   To select all available privileges, click the select all check box.
9. 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.

Using the iLO Federation features

Subtopics

Selected Group list

Exporting iLO Federation information to a CSV file

iLO Federation Multi-System view

Selected Group list

All of the iLO Federation pages except for Setup 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.

Subtopics

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

Prerequisites

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

About this task

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.

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.

Subtopics

Viewing server health and model information

Viewing servers with critical and degraded status

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. Click iLO Federation in the navigation tree, and then click the Multi-System View tab.
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.

Subtopics

Server health and model details

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. Click iLO Federation in the navigation tree, and then click the Multi-System View tab.
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.

Subtopics

Critical and degraded server status details

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

Prerequisites

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

About this task

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.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Multi-System Map tab.
2. Select a group from the Selected Group menu.

Subtopics

iLO peer details

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.
- Query Time (seconds)—When a timeout occurs, this value can be used to identify systems that are not responding quickly. This value applies to the most recent query.
- Node Count—When an error occurs, this value can indicate how much data might be missing. A value of zero indicates that the most recent query timed out. This value applies to the most recent query.
- 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 URL-based media for access by a group of servers.

- The following types of URL-based virtual media are supported: 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, and eject URL-based media, and you can boot from CD/DVD-ROM disk images. When you use URL-based 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.
- Before you use the virtual media feature, review the virtual media operating system considerations.

Subtopics

Connecting URL-based virtual media for groups

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: https://www.hpe.com/support/ilo-docs.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Virtual Media tab.
2. Select a group from the Selected Group menu.

   The URL-based media you connect will be available to all systems in the selected group.
3. Enter the disk image URL in the Virtual 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 will 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.
5. For virtual floppy devices only: Select the Read-Only check box if you want to connect the virtual media device with read-only permission.

   The Read-Only check box is enabled by default.
6. Click Insert Media.

   iLO displays the command results.

Viewing URL-based virtual media status for groups

Prerequisites

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

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Virtual Media tab.
2. (Optional) To filter the displayed information, click a Read-Only Status or an Image URL link.

Subtopics

URL-based virtual media details

URL-based virtual media details

When URL-based 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. Scripted Media is displayed when URL-based media is connected.
- Connected—Indicates whether a virtual media device is connected.
- Read-Only Status—Indicates whether the virtual media device is connected with Read-Only or Read/Write permission.
- Image URL—The URL that points to the connected URL-based media.

Virtual CD/DVD-ROM Status

- 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 URL-based media.

Ejecting a URL-based virtual media device

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: **https://www.hpe.com/support/ilo-docs**.
- Each member of the selected iLO Federation group has granted the Virtual Media privilege to the group.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Virtual Media tab.
2. Select a group from the Selected Group menu.

   The URL-based virtual media device that you eject will be disconnected from all the systems in the selected group.
3. Click Eject Media in the Virtual Floppy Status section or the Virtual CD/DVD-ROM Status section.

Servers affected by a group virtual media action

The Affected Systems section provides the following details about the servers affected when you initiate a group virtual media action:

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

Click Next or 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

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: **https://www.hpe.com/support/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.

About this task

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.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Power tab.
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 Yes, <action>.

   For example, if you clicked Reset, the button label is Yes, reset. The name of the button to click depends on the group power option that you initiated.

   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.

- 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.

- 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.

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

Configuring group power capping

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: **https://www.hpe.com/support/ilo-docs**.
- Each member of the selected iLO Federation group has granted the Configure iLO Settings privilege to the group.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

About this task

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Power Settings tab.
2. Select a group from the Selected Group menu.

   Changes you make on this page affect all systems in the selected group.
3. Set the Enable power capping option to enabled.
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, select BTU/hr in the Power Unit menu to change the display to BTU/hr. When values are displayed in BTU/hr, select 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 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 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 Advanced Power Manager

See the server specifications at https://www.hpe.com/info/quickspecs 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: https://www.hpe.com/support/ilo-docs.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Power Settings tab.
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)
- Power Management Controller
- System Programmable Logic Device (CPLD)
- NVMe Backplane Firmware
- Server Platform Services (SPS)
- Language packs

- Third-party firmware packages

  Platform Level Data Model (PLDM) firmware packages are supported if the Accept 3rd Party Firmware Update Packages option is enabled on the Access Settings page.

- GPU

  The following GPUs are supported:

  - NVIDIA A100 x4/x8 SXM4
  - AMD MI100 GPU

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.

Subtopics

Updating the firmware for multiple servers

Servers affected by a group firmware update

Viewing group firmware information

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: https://www.hpe.com/support/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: https://www.hpe.com/support/hpesc.
2. Save the firmware file to a web server.
3. Click iLO Federation in the navigation tree, and then click the Group Firmware Update tab.
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. If you will update the Server Platform Services (SPS) firmware, power off the servers you want to update, and then wait 30 seconds.

   The SPS firmware cannot be updated when the server OS is running.

7. 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 6_<yyy>.bin`, where `<yyy>` represents the firmware version.

   iLO prompts you to confirm the request.

8. Click Yes, update.

   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.

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.

Viewing group firmware information

Prerequisites

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

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Firmware Update tab.
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.

Subtopics

Firmware details

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.

Installing license keys (iLO Federation group)

Prerequisites

- Configure iLO Settings privilege
- Each member of the iLO Federation group has granted the Configure iLO Settings privilege to the group.
- Your iLO license is supported on the selected servers.
- You obtained an iLO license activation key that is authorized for the number of selected servers.
- The iLO configuration and the network configuration meet the prerequisites for using the iLO Federation features.

About this task

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.

Procedure

1. Click iLO Federation in the navigation tree, and then click the Group Licensing tab.
2. (Optional) To filter the list of affected systems, click a license type or status link.

   For example: 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 Status section to install licenses only on servers that are unlicensed.
3. Enter a 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.

   After you install a license key, only the last five digits are displayed in iLO. Hewlett Packard Enterprise recommends recording and saving your license key information in case it is needed later.
4. Click Install.

   iLO prompts you to confirm that you have read and accept the EULA.

   The EULA details are available in the License Pack option kit.
5. Click I agree.

   The license is installed and 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. Click iLO Federation in the navigation tree, and then click the Group Licensing tab.
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 an OS remotely, the remote console enables you to view and control the host server monitor throughout the installation process.

Integrated remote console (IRC) access options

You can access the following integrated 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. To use this console, your browser must support using ClickOnce to start a .NET application.

On 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.

Other remote console access options

The following remote console options are available from outside of the iLO web interface:

- **HTML5 standalone remote console**—Provides HTML5 remote console access through a supported browser, without going through the iLO web interface.
- **Standalone remote console (HPLOCONS)**—Provides 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 integrated remote console. Download HPLOCONS from the following website: **https://www.hpe.com/support/ilo6**.

Remote console usage considerations

- The integrated remote console is suitable for high-latency (modem) connections.
- Do not run the integrated remote console from its host operating system on the same server.
- When you log into a server through the remote console, Hewlett Packard Enterprise recommends that you log out before closing the console.
- When you finish using the remote console, close the window or click the browser Close button (X) to exit.
- The UID LED flashes when a remote console session is active.
- The Idle Connection Timeout specifies how long a user can be inactive before a remote console session ends automatically. This value does not affect remote console sessions when a virtual media device is connected.
- When the mouse is positioned over the remote console window, the console captures all keystrokes, regardless of whether the console window has focus.
- You can enable and disable the Remote Console feature on the Access Settings page.
- When you use the HTML5 remote console in standalone mode or new window mode, the remote console initially runs in an iLO web UI session. When remote console video starts, a dedicated remote console session starts. If the web UI session ends, your connection to the HTML5 console ends and you must reconnect to the remote console.

NOTE: If you are using shared network port, the remote console and virtual media may disconnect. For more information see, Shared network port consideration section in iLO 6 User Guide.

Subtopics

Viewing remote console access settings

Starting the integrated remote console

Integrated remote console features

Remote console hot keys

Configuring remote console security settings

More information

Configuring iLO access settings

Viewing remote console access settings

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console access settings in the General Information section.

2. (Optional) To navigate to the Access Settings page, where you can configure these settings, click the Remote Console Status link or the

Remote Console Port link.

Subtopics

Remote console access setting details

Remote console access setting details

Remote Console Status

The current remote console access setting (enabled or disabled).

When the remote console is disabled:

- You cannot access the graphical remote console or the text-based remote console.
- The configured remote console port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

To view this setting on the Access Settings page, click the Remote Console Status link.

Remote Console Port

The configured remote console port. The default value is 17990.

To view this setting on the Access Settings page, click the Remote Console Port link.

Starting the integrated remote console

Subtopics

Starting the HTML5 IRC

Starting the HTML5 IRC from the Overview page

Starting the HTML5 standalone remote console

HTML5 remote console modes

HTML5 remote console controls

Starting the .NET IRC

Starting the .NET IRC from the overview page

.NET IRC requirements

Acquiring the remote console

Joining a shared remote console session (.NET IRC only)

Viewing the remote console status bar

Starting the HTML5 IRC

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

About this task

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

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Start the HTML5 IRC by doing one of the following:

   - Click the HTML5 Console button.

     This option opens the console in the same browser window as the iLO web interface. You cannot move the console out of the browser window.

   - Click the New Window button.

     This option opens the console in a new window. You can move the window to a different position or monitor, or minimize it.

   The HTML5 IRC starts.

3. Use the remote console features.

4. (Optional) To view the HTML5 remote console online help, click the Menu icon , and then select Help.

More information

Configuring iLO access settings
HTML5 remote console controls

Starting the HTML5 IRC from the Overview page

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

About this task

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

Procedure

1. Click Information in the navigation tree, and then click the Overview tab.

2. Start the HTML5 IRC by doing one of the following:

   - Click the HTML5 link.

     This option opens the console in the same browser window as the iLO web interface. You cannot move the console out of the browser window.

   - Click .

     This option opens the console in a new window. You can move the window to a different position or monitor, or minimize it.

   The HTML5 IRC starts.

3. Use the remote console features.
4. (Optional) To view the HTML5 remote console online help, click the Menu icon , and then select Help.

More information

Configuring iLO access settings
HTML5 remote console controls

Starting the HTML5 standalone 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

About this task

Use this procedure to access the HTML5 remote console without first logging in to the iLO web interface.

Procedure

1. Open a browser window, and then navigate to the following webpage: `https://<iLO hostname or IP address>/irc.html`.

   The iLO HTML5 remote console login page opens.

   - If a login security banner is configured, the banner text is displayed in the NOTICE section.
   - If the iLO health status is Degraded, and the Anonymous Data access option is enabled, iLO displays the health status and a description of the issue on the login page. Self-test failures that could compromise security are not displayed in the description.
2. Enter a directory or local account login name and password, and then click Log In.

   If iLO is configured for Kerberos network authentication, the Zero Sign In button is displayed below the Log In button. You can use the Zero Sign In button to log in without entering a user name and password.

   If iLO is configured for CAC Smartcard Authentication, the Log in with Smartcard button is displayed below the Log In button. You can connect a smart card, and then click the Log in with Smartcard button. Do not enter a login name and password when you use CAC Smartcard Authentication.
3. Use the remote console features.
4. (Optional) To view the HTML5 remote console online help, click the Menu icon , and then select Help.

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. The supported viewing modes depend on the method that you use to start the console.

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.

This mode is available when you start the console by using the following methods:

- Click HTML5 on the iLO Overview page.

- Click HTML5 Console on the iLO Integrated Remote Console page.
- Click the iLO navigation pane remote console thumbnail, and then select HTML5 Console.

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

New window mode

The remote console is displayed in a window that you can move to a different position or monitor. You can also add it as a browser tab or minimize the window.

This mode is available when you start the console by using the following methods:

- Click  on the iLO Overview page.
- Click New Window on the iLO Integrated Remote Console page.

You can switch from this mode to full screen mode.

Docked mode

The remote console is displayed in a navigation pane thumbnail.

This mode is available when you start the console by using the following methods:

- Click HTML5 on the iLO Overview page.
- Click HTML5 Console on the iLO Integrated Remote Console page.
- Click the iLO navigation pane remote console thumbnail, and then select HTML5 Console.

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.

Standalone mode

When you use standalone mode, the remote console is displayed in a browser tab.

This mode is available when you start the console by using the following method:

- Navigate to the following webpage, and then log in: `https://<iLO hostname or IP address>/irc.html`.

You can switch from this mode to full screen mode.

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.
- Use the Info menu to view the iLO host name and the server name.
- Use the Help menu to view HTML5 console online help.

This icon is not available in docked mode.

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

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- 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 HPE iLO 6 Troubleshooting Guide.
- Pop-up blockers are disabled.

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

About this task

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

More information

Configuring iLO access settings
.NET IRC requirements

Starting the .NET IRC from the overview page

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- 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 HPE iLO 6 Troubleshooting Guide.
- Pop-up blockers are disabled.

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

About this task

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

Procedure

1. Click Information in the navigation tree, and then click the Overview tab.
2. Click the .NET link.
3. Use the remote console features.

More information

Configuring iLO access settings
.NET IRC requirements

.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**.

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.

Acquiring 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

About this task

If another user is working in the remote console, you can acquire it from that user.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

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.

More information

Configuring iLO access settings

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Click the .NET Console button.

   A message notifies you that the .NET remote console is already in use.

3. Click Share.

   The session leader receives your request to join a shared remote console session.

   If the session leader clicks Yes, you are granted access to the session with access to the keyboard and mouse.

Subtopics

Shared remote console (.NET IRC only)

More information

Configuring iLO access settings

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: **https://www.hpe.com/support/ilo-docs**.

- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

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.

4. (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.

Subtopics

Remote console status bar details

More information

Configuring iLO access settings

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

Subtopics

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

Subtopics

Sending a keyboard action with the HTML5 IRC

Sending a keyboard action with the .NET IRC

Sending a remote console hot key

Changing the keyboard layout in the HTML5 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

More information

Configuring iLO access settings

Sending a keyboard action with the .NET 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- Remote console hot keys are configured on the Hot Keys page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Start a remote console.
3. On your client keyboard, press the key combination for a configured remote console hot key.

More information

Configuring iLO access settings
Remote console hot keys
Creating remote console hot keys

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- 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. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

More information

Configuring iLO access settings

Virtual power IRC features

Subtopics

Using the remote console virtual power switch with the HTML5 IRC

Using the remote console virtual power switch with the .NET IRC

Virtual power button options

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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 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.
5. Click OK.

More information

Configuring iLO access settings

Using the remote console virtual power switch with the .NET 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
2. Start the .NET 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.

Subtopics

Using a virtual drive (physical drive on a client PC)

Using a local IMG or ISO file with the HTML5 IRC

Using a local IMG or ISO file with the .NET IRC

Using a virtual drive to install an OS and provide a required driver (.NET IRC)

Using a virtual drive to install an OS and provide a required driver (HTML5 IRC)

Using a URL-based image file with the HTML5 IRC

Using a URL-based image file with the .NET IRC

Using a virtual folder (HTML5 IRC)

Using a virtual folder (.NET IRC)

More information

iLO web interface virtual media options

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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- If you are using the remote console with Windows, you have Windows administrator rights, which are required for mounting a physical drive.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Start a remote console that supports this feature.

   In this release, the .NET IRC supports this feature.

3. Click the Virtual Drives menu, and then select a floppy disk, CD-ROM/DVD, or USB key drive connected to your client system.

   The activity LED will blink to show the virtual drive activity.

4. When you are finished using the virtual drive, disconnect it through the server OS.

   You can also disconnect a virtual drive from the Virtual Drives menu. Click Virtual Drives and clear the respective checkbox.

More information

Configuring iLO access settings
Virtual media considerations

Using a local IMG or ISO file with the HTML5 IRC

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

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. If your OS supports system notifications, a notification is displayed.

5. When you are finished using the local IMG or ISO file, disconnect it through the server OS.

   You can also disconnect the local IMG or ISO file by clicking , and then selecting *media type* > Force Eject Media.

More information

Configuring iLO access settings
Virtual media considerations

Using a local IMG or ISO file with the .NET IRC

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Start the .NET 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.

5. When you are finished using the local IMG or ISO file, disconnect it through the server OS.

   You can also disconnect the local IMG or ISO file by selecting Virtual Drives > *Connected virtual drive*.

More information

Configuring iLO access settings
Virtual media considerations

Using a virtual drive to install an OS and provide a required driver (.NET IRC)

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the Access Settings page.

- The Virtual Media feature is enabled on the Access Settings page.
- 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: **https://www.hpe.com/support/ilo-docs**.

About this task

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.

Procedure

1. Download and extract the required driver.

   You can obtain drivers from the SPP or download them from the following website: **https://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.
   - 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.

More information

Configuring iLO access settings
Virtual media considerations
Configuring the server boot mode
Using a local IMG or ISO file with the .NET IRC
Using a virtual folder (.NET IRC)

Using a virtual drive to install an OS and provide a required driver (HTML5 IRC)

Prerequisites

- Remote Console privilege
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- 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: **https://www.hpe.com/support/ilo-docs**.

About this task

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.

Procedure

1. Download and extract the required driver.

   You can obtain drivers from the SPP or download them from the following website: **https://www.hpe.com/support/hpesc**.
2. Copy the driver to a folder on the client where you will access the remote console.
3. Start the HTML5 remote console.
4. Mount the operating system ISO.
   a. Click the Virtual Media icon , and then select CD/DVD > Local *.iso file.

      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.

      The activity LED will blink to show the virtual drive activity. If your OS supports system notifications, a notification is displayed.
5. Drag and drop the folder that contains the required driver from your client computer into the HTML5 IRC window.

   The virtual folder is mounted on the server with the name iLO FOLDER.

   The activity LED will blink to show the virtual drive activity. If your OS supports system notifications, a notification is displayed.
6. Boot to the operating system ISO.
7. Follow the onscreen instructions until the operating system installer prompts you for the path to the driver.
8. When prompted for the driver location, enter the path to the virtual folder that contains the driver.
9. Follow the onscreen instructions to complete the operating system installation.
10. Install any additional required device drivers.

    You can obtain device drivers from the SPP.

Using a URL-based image 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- The image file you want to use is on a web server on the same network as iLO.

About this task

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
2. Start the HTML5 IRC.
3. Click the Virtual Media icon, and then select Floppy > Virtual Media URL or CD/DVD > Virtual Media URL.

   The remote console 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.
5. When you are finished using the image file, disconnect it through the server OS.

   You can also disconnect the image file by clicking, and then selecting *media type* > Force Eject Media.

More information

Configuring iLO access settings
Setting up IIS for scripted virtual media

Using a URL-based image file with the .NET 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- The image file you want to use is on a web server on the same network as iLO.

About this task

You can connect the following types of URL-based media: 1.44 MB floppy disk images (IMG) and CD/DVD-ROM images (ISO).

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

2. Start the .NET 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.
5. When you are finished using the image file, disconnect it through the server OS.

   You can also disconnect the image file by selecting Virtual Drives > *Connected virtual drive*.

More information

Configuring iLO access settings
Setting up IIS for scripted virtual media

Using a virtual folder (HTML5 IRC)

Prerequisites

- Remote Console privilege
- 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- The size of the folder you will mount as a virtual folder is 2 GB or less.
- You are using a browser that supports this feature.

About this task

In the HTML5 IRC, the virtual folder feature uses drag and drop to mount a virtual folder. There is a Virtual folder option when you click the Virtual Media icon . The Virtual folder option provides information about the feature. When a virtual folder is mounted, the Virtual folder menu option provides an option to unmount the virtual folder.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
2. Start the HTML5 remote console.
3. Drag and drop one or more folders or one or more selected files from the system running the remote console into the console window.

   The virtual folder is mounted on the server with the name iLO FOLDER.

   The activity LED will blink to show the virtual drive activity. If your OS supports system notifications, a notification is displayed.
4. When you are finished using the virtual folder, disconnect it through the server OS.

   You can also disconnect a virtual folder by clicking , and then selecting Virtual Folder > Force Eject Media.

Using a virtual folder (.NET 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: **https://www.hpe.com/support/ilo-docs**.
- The Remote Console feature is enabled on the Access Settings page.
- The Virtual Media feature is enabled on the Access Settings page.
- The size of the folder you will mount as a virtual folder is 2 GB or less.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

   The activity LED will blink to show the virtual drive activity.
5. When you are finished using the virtual folder, disconnect it through the server OS.

   You can also disconnect a virtual drive from the Virtual Drives menu. Click Virtual Drives and clear the respective checkbox.

Subtopics

Virtual folders

More information

Configuring iLO access settings
Virtual media considerations

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.

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.

Subtopics

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
- The Remote Console feature is 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: https://www.hpe.com/support/ilo-docs.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

More information

Configuring iLO access settings
Console capture (.NET IRC)

Saving server startup and server prefailure video files

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

More information

Configuring iLO access settings
Console capture (.NET IRC)

Capturing video files with the remote console

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

About this task

Use this procedure to capture video files of sequences other than server startup and server prefailure.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

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.

More information

Configuring iLO access settings
Console capture (.NET IRC)

Viewing saved video files with the remote console

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.

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.

More information

Configuring iLO access settings
Console capture (.NET IRC)

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.

Subtopics

Capturing the HTML5 remote console screen

Capturing the .NET IRC screen

Capturing the HTML5 remote console screen

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the remote console launch options.
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.

More information

Configuring iLO access settings

Capturing the .NET IRC screen

Prerequisites

- Remote Console privilege
- The Remote Console feature is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Remote Console & Media in the navigation tree.

   The Launch tab displays the Remote Console launch options.
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.

More information

Configuring iLO access settings

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.

Subtopics

Creating remote console hot keys

Keys for configuring remote console computer lock keys and hot keys

Resetting hot keys

Creating remote console hot keys

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Hot Keys tab.
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.

More information

Sending a remote console hot key
Keys for configuring remote console computer lock keys and hot keys

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

Prerequisites

Configure iLO Settings privilege

About this task

Resetting the hot keys clears all current hot key assignments.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Hot Keys tab.

2. Click Reset Hot Keys.

   iLO prompts you to confirm the request.

3. When prompted to confirm the request, click Yes, reset hot keys.

   iLO notifies you that the hot keys were reset.

Configuring remote console security settings

Subtopics

Configuring remote console computer lock settings

Configuring the remote console trust setting (.NET IRC)

Configuring remote console computer lock settings

Prerequisites

Configure iLO Settings privilege

About this task

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.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Security tab.
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.

Subtopics

Remote console computer lock options

More information

Remote console computer lock options
Keys for configuring remote console computer lock keys and hot keys

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.

More information

Remote console computer lock options
Keys for configuring remote console computer lock keys and hot keys

Configuring the remote console trust setting (.NET IRC)

Prerequisites

Configure iLO Settings privilege

About this task

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 the iLO processor, and this setting is enabled, ClickOnce notifies you that the application cannot start.

Hewlett Packard Enterprise recommends installing a trusted SSL certificate and enabling the IRC requires a trusted certificate in iLO setting. In this configuration, the .NET IRC is launched by using an HTTPS connection.

If the IRC requires a trusted certificate in iLO setting is disabled, the .NET IRC is launched by using a non-SSL connection, which is insecure. In this configuration, SSL is used after the .NET IRC starts to exchange encryption keys. If you cannot install a trusted SSL certificate, and you do not want to use a non-SSL connection, you can use the Standalone remote console (HPLOCONS) or the HTML 5 Integrated Remote Console.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Security tab.
2. To enable or disable the IRC requires a trusted certificate in iLO setting, click the toggle switch.
3. To save the changes, click Apply.

More information

Administering SSL certificates
.NET IRC requirements

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.

The text-based console option is described in the following section:

- iLO Virtual Serial Port

Subtopics

iLO Virtual Serial Port

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 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.

Subtopics

Using the iLO Virtual Serial Port

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

Configuring Linux to use the iLO Virtual Serial Port

Windows EMS Console with iLO Virtual Serial Port

Starting an iLO Virtual Serial Port session

Viewing the iLO Virtual Serial Port log

Downloading the Virtual Serial Port log through the iLO web interface

Using the iLO Virtual Serial Port

Procedure

1. Configure the iLO Virtual Serial Port in the UEFI System Utilities.
2. Configure the operating system to use the iLO Virtual Serial Port:
   - For supported Linux operating systems, see Configuring Linux to use the iLO Virtual Serial Port.
   - For supported Windows operating systems, see Windows EMS Console with iLO Virtual Serial Port.
3. Start an iLO Virtual Serial Port session.
4. (Optional) View the iLO Virtual Serial Port log.
5. (Optional) Download the iLO Virtual Serial Port log through the iLO web interface.

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

About this task

The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

Procedure

1. Access the UEFI System Utilities.
   a. (Optional) If you access the server remotely, start an iLO Remote Console session.
   b. Restart or power on the server.
   c. Press F9 in the server POST screen.

      The UEFI System Utilities start.
2. Set the Virtual Serial Port COM port.
   a. Click System Configuration, then click BIOS/Platform Configuration (RBSU).
   b. Click System Options, then click Serial Port Options.
   c. In the Virtual Serial Port menu, select the COM port you want to use.
3. Set the BIOS serial console and EMS properties.
   a. At the top of the Serial Port Options page, click BIOS Serial Console and EMS.
   b. In the BIOS Serial Console Port menu, select the COM port you want to use.
   c. In the BIOS Serial Console Baud Rate menu, select 115200.

      NOTE:

      The iLO Virtual Serial Port does not use a physical UART. The BIOS Serial Console Baud Rate value has no effect on the speed the iLO Virtual Serial Port uses to send and receive data.
   d. For Windows users only: In the EMS Console menu, select the COM port that matches the selected Virtual Serial Port COM port.
4. To save the changes and exit, press F12.
5. When prompted to confirm the request, click Yes - Save Changes.

   The UEFI System Utilities notify you that a system reboot is required.
6. Click Reboot.

Configuring Linux to use the iLO Virtual Serial Port

About this task

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).

Subtopics

Configuring Red Hat Enterprise Linux 9 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/oemhpe_vsp1` to view a login session to the Linux operating system.

Configuring Red Hat Enterprise Linux 8 to use the iLO Virtual Serial Port

Procedure

1. Use the `grub2-env` command to view the `kernelopts` parameters.

   For example:

   ```
   # grub2-editenv - list | grep kernelopts
   ```

```
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
```

2. Copy the results of the list command.

   For example:

```
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap
```

3. Set the kernel options.

   Include the existing kernel options copied in step 2, and add the serial console options at the end.

   For example:

```
# grub2-editenv - set
"kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0"
```

4. (Optional) To verify that the parameters were set correctly, run the list command again.

   For example:

```
# grub2-editenv - list | grep kernelopts
kernelopts=root=/dev/mapper/rhel-root ro crashkernel=auto resume=/dev/mapper/rhel-swap
rd.lvm.lv=rhel/root rd.lvm.lv=rhel/swap console=ttyS0,115200 console=tty0
```

5. Reboot the server.

Subtopics

Configuring GRUB to use a serial console (Red Hat Enterprise Linux 8)

Configuring GRUB to use a serial console (Red Hat Enterprise Linux 8)

About this task

You can configure GRUB to use the serial console instead of the VGA console. This feature allows you to perform tasks such as interrupting the boot process to choose a different kernel, or adding kernel parameters for tasks such as booting into single user mode.

Procedure

To configure GRUB to use the serial console, comment out the splash image and add the `serial` and `terminal` options to the `grub.conf` file.

For example:

```
[root@localhost ~]# cat /boot/grub/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/hda2
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=10
#splashimage=(hd0,0)/grub/splash.xpm.gz
serial --unit=0 --speed=115200
```

```
terminal --timeout=5 serial console
title Red Hat Enterprise Linux AS (2.4.21-27.0.2.ELsmp)
        root (hd0,0)
        kernel /vmlinuz-2.4.21-27.0.2.ELsmp ro root=LABEL=/ console=ttyS0,115200 console=tty0
        initrd /initrd-2.4.21-27.0.2.ELsmp.img
```

The changes take effect after the next system reboot.

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/oemhpe_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 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.

Subtopics

Configuring Windows for use with the iLO Virtual Serial Port

Configuring Windows for use with the iLO Virtual Serial Port

About this task

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 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

Prerequisites

- Secure Shell (SSH) and Virtual Serial Port Log Over CLI are enabled on the Security - 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: **https://www.hpe.com/support/ilo-docs**.

About this task

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.

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`.

> **NOTE:**
> The Virtual Serial Port log (VSP) is cleared after an AUX server cycle and cold boot. In case of warm-boot from the OS or iLO reset, the log file is not cleared, but appended to the previous log.

Downloading the Virtual Serial Port log through the iLO web interface

Prerequisites

- Configure iLO Settings privilege
- The Downloadable Virtual Serial Port Log option is 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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Security in the navigation tree.

   The Access Settings page is displayed.
2. Click  next to the iLO Access Settings category.

   The Edit iLO Settings page opens.
3. Click the Download link next to the Downloadable Virtual Serial Port Log option.

   iLO notifies you when the download is finished.

Using iLO on the host

The Virtual NIC feature enables a secure connection to iLO directly from the host operating system. Use this feature directly at the host server or through a Remote Console connection. You can interact with iLO by using the web interface, SSH, or the iLO RESTful API.

The Virtual NIC feature is useful when you want to:

- Access iLO when the network configuration prevents connection through the management network. For example, use a Virtual NIC connection when you have access to the production network but cannot access the iLO dedicated management network.
- Access iLO when there is no NIC cable attached to the host or iLO.

The factory default Virtual NIC setting is disabled in most versions of iLO. In iLO 6 v2.10, this setting is enabled by default. When you reset iLO to the factory default settings, the Virtual NIC setting returns to the default setting for the installed version of iLO. Firmware upgrades or downgrades do not change this setting.

Subtopics

Prerequisites for using the Virtual NIC

- The host server operating system that has an inbox driver module for USB CDC-EEM supports the Virtual NIC.

  Most of the supported Windows and Linux operating systems load the driver module automatically when the Virtual NIC is enabled in iLO.

  On Windows hosts, you can verify support by looking for `usbnet.sys` under `C:\Windows\System32`.

  On Linux hosts, you can use the following methods to verify support when the Virtual NIC feature is disabled in iLO:

  - Look for `cdc_eem.ko` under `/lib/modules`:

    ```
    find /lib/modules/$(uname -r)  *.ko* | grep cdc_eem
    ```

  - Enter the following command to check if `cdc_eem` is loaded:

    ```
    lsmod | grep cdc_eem
    ```

    If `cdc_eem` is not loaded, you can load it by entering the following command.

    ```
    sudo modprobe cdc_eem
    ```

    After you load `cdc_eem` manually, run `lsmod | grep cdc_eem` again to confirm that it loaded successfully.

- The host server OS supports the Virtual NIC.
- On Linux hosts, the USB CDC-EEM driver is installed and configured in the host server OS.

  This driver is part of the OS installation for the operating systems that support this feature.

- The Virtual NIC feature is enabled on the Access Settings page.
- The interface you want to use to connect to iLO is enabled on the Access Settings page.

  For example, if you want to connect to the iLO web interface, then the iLO Web Interface option is enabled.
- The host server is not configured to block the port for the interface you want to use to connect to iLO.

  For example, when you use the iLO web interface with the default iLO configuration, ensure that the host server does not block port 443.
- The Virtual NIC interface is not teamed or bridged with any of the host NICs. This configuration might cause the Virtual NIC to be unavailable or insecure.
- The iLO hostname and the Virtual NIC IP address are in the `hosts` file on the client system you will use to access the Virtual NIC. When you use the iLO hostname to connect to iLO with the Virtual NIC, this configuration is required to allow name resolution to work, and for SSL connections to validate correctly.

More information

Configuring iLO access settings
Operating system support for Virtual NIC

Operating system support for Virtual NIC

The Virtual NIC feature is qualified on servers with iLO 6 and the following operating systems:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- SUSE Linux Enterprise Server 12
- SUSE Linux Enterprise Server 15
- Red Hat Enterprise Linux 9
- Red Hat Enterprise Linux 8

This feature is expected to work with other nonqualified operating systems that include the required driver.

Configuring the Virtual NIC feature

Prerequisites

Configure iLO Settings privilege

Procedure

1. Verify that the Virtual NIC feature is enabled.
   a. Click Security in the navigation tree.

      The Access Settings page is displayed.
   b. Confirm that Virtual NIC is set to Enabled in the iLO section.
2. If Virtual NIC is not set to Enabled, enable it.
   a. Click  next to the iLO category.

      The Edit iLO Settings page opens.

b. Select the Virtual NIC check box, and then click OK.

   iLO notifies you that pending changes require a reset to take effect.

c. If you are done updating access settings, click Reset iLO.

   iLO prompts you to confirm the request.

d. Click Yes, reset iLO.

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

   After the reset is complete, the Virtual NIC feature is enabled, and it is detected by the host server OS.

3. (Optional) For Linux distributions that do not automatically configure new network interfaces for DHCP: Change the network configuration of the Virtual NIC interface from static to DHCP.

   For more information, see:

   - Changing the Virtual NIC interface from static to DHCP (Network Manager)
   - Changing the Virtual NIC interface from static to DHCP (CLI)

4. Verify that the Virtual NIC is available to the host operating system.

   a. Start a remote console session or access the physical host system.

   b. Log in to the host server operating system.

   c. Do one of the following:

      - On Windows systems: Run `ipconfig` and look for an adapter named Ethernet adapter Ethernet with the IP address 16.1.15.2 and the subnet mask 255.255.255.252.
      - On Linux systems: Identify the network interface name, and then run `ifconfig`. The adapter has the IP address 16.1.15.2 and the subnet mask 255.255.255.252.

      WARNING:

      Do not change the adapter IP address on the host. Changing the IP address from 16.1.15.2 to any other value makes the Virtual NIC inaccessible.

Subtopics

Changing the Virtual NIC interface from static to DHCP (Network Manager)

Changing the Virtual NIC interface from static to DHCP (CLI)

More information

Configuring iLO access settings

Changing the Virtual NIC interface from static to DHCP (Network Manager)

About this task

If your Linux distribution does not automatically configure new network interfaces for DHCP, change the Virtual NIC interface network configuration from static to DHCP.

Procedure

1. Open Network Manager.
2. Locate the Virtual NIC interface.
3. Configure the Virtual NIC interface to use DHCP.

Changing the Virtual NIC interface from static to DHCP (CLI)

About this task

If your Linux distribution does not automatically configure new network interfaces for DHCP, change the Virtual NIC interface network configuration from static to DHCP.

Procedure

1. Identify the device in `/sys/bus/usb/devices`.

   For example:

   - `cat /sys/bus/usb/devices/1-4/idVendor` shows the value `03f0`.
   - `cat /sys/bus/usb/devices/1-4/idProduct` shows the value `2927`.

2. Identify the Virtual NIC network interface name.

   For example:

   `/sys/bus/usb/devices/1-4/1-4:1.0/net/usb0`.

3. Write a network configuration script to configure the Virtual NIC interface to use DHCP.

   For example, create `/etc/sysconfig/network/ifcfg-usb0` with the following entry in the configuration script: `BOOTPROTO='dhcp'`.

4. Access the Virtual NIC interface or restart the network service.

Using the Virtual NIC to access the iLO web interface

Prerequisites

- Your environment meets the general prerequisites for using the Virtual NIC feature.
- The browser is not configured to use a proxy server.

Procedure

1. Start a remote console session or access the physical host system.
2. Log in to the host server operating system.
3. Open a supported browser.
4. Enter the following URL: **`https://16.1.15.1`**.

   If the iLO hostname and Virtual NIC IP address are in the hosts file on the client system, you can also connect by using the iLO hostname:

   `https://iLO hostname`

   A security warning related to the website certificate is displayed.

5. Depending on your browser, do one of the following:

   - **Microsoft Edge**—Click Details, and then click Go on to the webpage.
   - **Google Chrome**—Click Advanced, and then click Proceed to <iLO hostname or IP address> (unsafe).
   - Mozilla Firefox—Click Advanced, and then click Accept the risk and continue.

The iLO login screen for the local system is displayed.

6. Log in to iLO.

   Your session is displayed on the Session List page with the IP address 16.1.15.2.

7. Use the iLO web interface to view or update the server or iLO configuration.

More information

Logging in to the iLO web interface
Prerequisites for using the Virtual NIC
Supported browsers

Using iLOREST on the host

Prerequisites

- Your environment meets the general prerequisites for using the Virtual NIC feature.
- The RESTful Interface Tool is installed in the host server operating system.

Procedure

1. Start a remote console session or access the physical host system.
2. Log in to the host server OS.
3. Start iLOREST.
4. Log in to the iLO system:

   ```
   iLOrest > login 16.1.15.1 -u iLO user name -p iLO password
   ```

   If the iLO hostname and Virtual NIC IP address are in the hosts file on the client system, you can also connect by using the iLO hostname:

   ```
   iLOrest > login iLO hostname -u iLO user name -p iLO password
   ```

5. Use iLOREST commands to view or update the server or iLO configuration.

More information

Prerequisites for using the Virtual NIC

Using an SSH connection with the Virtual NIC

Prerequisites

- Your environment meets the general prerequisites for using the Virtual NIC feature.
- For Windows operating systems only: PuTTY or OpenSSH is installed.

Procedure

1. Start a Remote Console session or access the physical host system.
2. Log in to the host server operating system.
3. Depending on the installed operating system, open a command prompt or a PuTTY terminal prompt.
4. Log in to the iLO system:

```
ssh iLO user name@16.1.15.1
```

If the iLO hostname and Virtual NIC IP address are in the hosts file on the client system, you can also connect by using the iLO hostname:

```
ssh iLO user name@iLO hostname
```

5. Use the SSH client to view or update the server or iLO configuration.

More information

Prerequisites for using the Virtual NIC

Using iLO virtual media

Subtopics

Virtual media considerations

Virtual media operating system information

iLO web interface virtual media options

Setting up IIS for scripted 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.

  This limit classifies virtual floppy/USB keys and virtual folders as the same type of virtual media.

- 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.
- Virtual folders up to 2 gigabytes in size are supported.
- 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 CD/DVD-ROM is available at server boot time for supported operating systems. Booting from a virtual CD/DVD-ROM enables you to perform tasks such as deploying an OS from network drives, and performing disaster recovery of failed operating systems.
- 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: 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.
- If you have mounted virtual media using a local IMG, ISO file, or Virtual Folder it cannot be unmounted through Redfish.
- Hewlett Packard Enterprise recommends the following for the Scripted Virtual Media feature to work correctly:
  - Web server to set the media type for `.iso` and `.img` files as octet-stream. iLO expects the requested content coming from the webserver as binary data.
  - Web server to support HTTP Range in the client request header and respond accordingly.

NOTE: If you are using shared network port, the remote console and virtual media may disconnect. For more information see, Shared network port consideration.

Virtual media operating system information

This section describes the operating system requirements to consider when you are using the iLO virtual media features.

Subtopics

Operating system USB requirement

Operating system considerations: Virtual floppy/USB key

Operating system considerations: Virtual CD/DVD-ROM

Operating system considerations: Virtual folder

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.

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 disk during a Windows installation, disable the integrated disk drive in the host RBSU. This action 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 and SUSE Linux Enterprise Server

Linux supports the use of USB diskette and key drives.

Subtopics

Changing diskettes

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`).

Subtopics

Mounting a USB virtual media CD/DVD-ROM (Linux command line)

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.
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`

Operating system considerations: Virtual folder

- **Boot process and DOS sessions**—The virtual folder device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and the virtual folder simultaneously.
- **Windows**—A virtual folder appears automatically after Windows recognizes the mounting of the virtual USB device. You can use the folder the same way that you use a locally attached device. virtual folders are nonbootable. Attempting to boot from the virtual folder might prevent the server from starting.
- **Red Hat Enterprise Linux and SUSE Linux Enterprise Server**—Linux supports the use of the virtual folder feature, which uses a FAT 16

file system format.

iLO web interface virtual media options

When the Virtual Media feature is enabled on the Access Settings page, you can perform the following tasks on the Virtual Media page:

- View or eject local media, including physical drives, local image files, and virtual folders.
- View, connect, eject, or boot from URL-based media. URL-based media refers to connecting images hosted on a web server by using a URL. iLO accepts URLs in HTTP or HTTPS format. FTP is not supported.

Subtopics

Viewing virtual media status and port configuration

Viewing connected local media

Ejecting a local virtual media device

Connecting URL-based media

Viewing connected URL-based media

Ejecting a URL-based virtual media device

More information

Virtual media IRC features

Viewing virtual media status and port configuration

About this task

Use the Virtual Media page to view the virtual media feature configuration. You can configure these settings on the Access Settings page.

Procedure

1. Navigate to the Remote Console & Media page, and then click the Virtual Media tab.

   The Virtual Media Status, Virtual Media Port, and Enhanced Download Performance are displayed.

   NOTE: Enhanced Download Performance link is not displayed, if it is already enabled.

2. (Optional) To configure the virtual media feature status, click the Virtual Media Status link.

   The Access Settings page is displayed.

3. (Optional) To configure the virtual media port, click the Virtual Media Port link.

   The Access Settings page is displayed.

4. (Optional) To configure Enhanced Download Performance, click the Enhanced Download Performance link.

   The Access Settings page is displayed. You can configure the settings on the Access Settings page.

   For more information on the option, see the help on the Access Settings page.

More information

Configuring iLO access settings

Viewing connected local media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the Access Settings page.

Procedure

To view the connected local media devices, click Remote Console & Media in the navigation tree, and then click the Virtual Media tab.

Subtopics

Local media details

More information

Configuring iLO access settings

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
- The Virtual Media feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Virtual Media tab.
2. Click the Force Eject Media button in the Virtual Floppy/USB Key/Virtual Folder Status or Virtual CD/DVD-ROM Status section.

More information

Configuring iLO access settings

Connecting URL-based media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the Access Settings page.

About this task

You can connect URL-based media from the Virtual Media page. The Virtual Media page supports the connection of 1.44 MB floppy images (IMG) and CD/DVD-ROM images (ISO). The image must be on a web server on the same network as iLO.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click the Virtual Media tab.
2. Enter the URL for the URL-based media in the Virtual Media URL box in the Connect Virtual Floppy (IMG files) or Connect CD/DVD-ROM section (ISO files).
3. For CD/DVD-ROM only: Select the Boot on Next Reset check box if you want the server to boot to this image only on the next server reboot.

   The image will be ejected automatically on the second server reboot so that the server does not boot to this image twice.

   If this check box is not selected, the image remains connected until it is manually ejected. The server will boot to the image on all subsequent server resets, if the system boot options are configured accordingly.

   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. For virtual floppy only: Select the Read-Only check box if you want to connect the virtual media device with read-only permission.

   The Read-Only check box is enabled by default.
5. Click Insert Media.
6. (Optional) To boot to the connected image now, reboot the server.

More information

Configuring iLO access settings
Setting up IIS for scripted virtual media

Viewing connected URL-based media

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the Access Settings page.

Procedure

Click Remote Console & Media in the navigation tree, and then click the Virtual Media tab.

Subtopics

URL-based media details

More information

Configuring iLO access settings

URL-based media details

When URL-based 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.

  Scripted Media is displayed when URL-based media is connected.
- Connection Status—Indicates whether a virtual media device is connected.
- Image URL—The URL that points to the connected URL-based media.
- 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.

  Scripted Media is displayed when URL-based media is connected.
- Connection Status—Indicates whether a virtual media device is connected.
- Image URL—The URL that points to the connected URL-based media.

Ejecting a URL-based virtual media device

Prerequisites

- Virtual Media privilege
- The Virtual Media feature is enabled on the Access Settings page.

Procedure

1. Click Remote Console & Media in the navigation tree, and then click Virtual Media.
2. To eject URL-based media devices, click the Force Eject Media button in the Virtual Floppy/Virtual Folder Status or Virtual CD/DVD-ROM Status section.

More information

Configuring iLO access settings

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.

Subtopics

Configuring IIS

Configuring IIS for read/write access

Inserting virtual media with a helper application

Configuring IIS

About this task

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

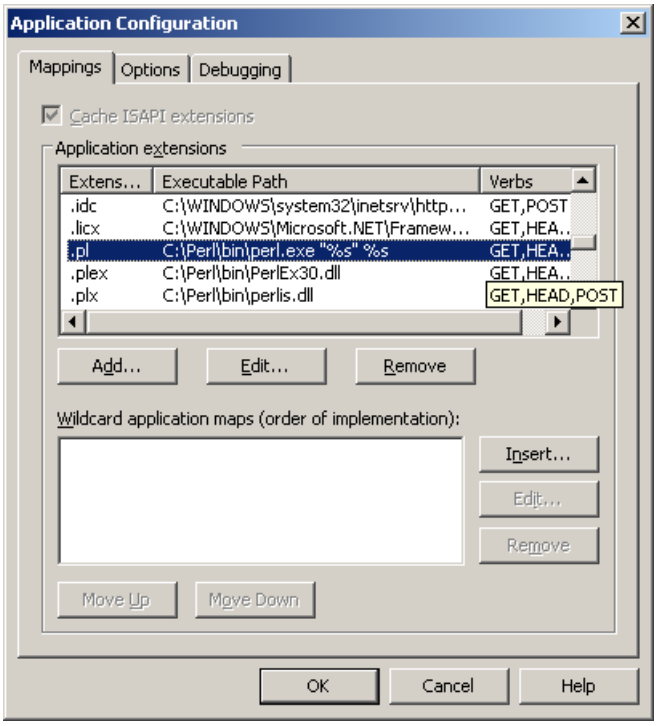
1. Install Perl (for example, ActivePerl).
2. Customize the virtual media helper application as needed.
3. Create a directory on your website for the virtual media helper script, and then copy the script to that directory.

   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 1. 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.

More information

Inserting virtual media with a helper application
Sample virtual media helper application

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 6 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";
```

Using the power and thermal features

Subtopics

Server power-on

Brownout recovery

Graceful shutdown

Power efficiency

Power-on protection

Power allocation (blade servers and compute modules)

Managing the server power

Configuring the System Power Restore Settings

Viewing server power usage

Power settings

Viewing power information

Configuring and viewing cooling features

Temperature information

Configuring user defined threshold using the RESTful Interface Tool

Server power-on

Secure recovery

When power is applied to the server, iLO validates and starts its own firmware. If the iLO firmware fails validation, the system automatically flashes the iLO firmware if a recovery image is available. This feature is supported with the iLO Standard license.

During server startup, the system ROM is validated. If the active system ROM fails validation, and the redundant system ROM is valid, the redundant system ROM becomes active. If both the active and the redundant system ROM are invalid, and an iLO Advanced license is installed, a firmware verification scan starts. Depending on the configured firmware verification settings, a repair is initiated with components in the System Recovery Set, or the failure is logged and you must complete the repair manually. If the system ROM is not verified, the server will not boot.

Check the IML for information about the firmware validation activities and recovery actions.

Nonblade servers

If an AC power loss occurs on a Gen11 server with iLO 6, approximately 30 seconds must elapse before the server 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.

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.

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.

More information

Auto Power-On

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 Agentless Management Service (AMS) must be loaded. iLO communicates with AMS and uses the appropriate operating system method of shutting down the system safely to ensure that data integrity is preserved.

If AMS is not loaded, the iLO processor attempts to use the operating system to perform a graceful shutdown through the power button. iLO emulates a physical power-button press (iLO momentary press) to prompt the operating system to shut down gracefully. The behavior of the operating system depends on its configuration and settings for a power-button press.

The Thermal Shutdown option in the 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.

More information

Agentless Management Service

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 UEFI System Utilities to configure HEM. You cannot configure these settings through iLO. For more information, see the UEFI System Utilities user guide.

The configured HEM settings are displayed on the Power Information page.

More information

Viewing power information

Power-on protection

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.

More information

Auto Power-On
Virtual power button options

Power allocation (blade servers and compute modules)

Blade servers operate in a shared power environment with an enclosure. Before a server can be powered on, it must obtain a power allocation from its enclosure.

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.

For troubleshooting information, see the error messages guide for your server.

Managing the server power

Prerequisites

Virtual Power and Reset privilege

About this task

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.

Procedure

1. Click Power & Thermal in the navigation tree.

   The page opens with the Server Power tab selected.

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.

Subtopics

Virtual power button options

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

Prerequisites

Configure iLO Settings privilege

About this task

The System Power Restore Settings enable you to control system behavior after power is lost.

Procedure

1. Click Power & Thermal in the navigation tree.

   The page opens with the Server Power tab selected.

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 Apply.

Subtopics

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 settings for all ProLiant servers.

- 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.

  NOTE: HPE ProLiant RL3xx Gen 11 platforms do not support Restore Last Power State option, if power was lost when the server was ON.

  This option is the default settings for all ProLiant servers.

  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.

  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.

Viewing server power usage

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: **https://www.hpe.com/support/ilo-docs**.
- The server power supplies and the system BIOS support power readings. If power readings are not supported, this page displays the following message: `Power Metering is unavailable for this configuration`.

About this task

Power meter graphs display recent server power usage. Power history information is not collected when the server is powered off. When you view a graph that includes periods in which the server was powered off, the graph displays a gap to indicate that data was not collected.

The graph data is cleared when iLO is reset or the server is power cycled. For example, the data is cleared when you use the Virtual Power Button Reset or Cold Boot actions. The data is not cleared when you use the Momentary Press or Press and Hold actions.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Meter tab.
2. Click 20 min, 24 hr, or 1 week to select a graph type.

   You can view a graph of the last 20 minutes, the last 24 hours, or the last week.
3. (Optional) To customize the graph display, select or clear the following check boxes:
   - Power Cap
   - Maximum
   - Average
   - Total CPU
   - Total GPU
   - Total DIMM

   If a server does not support a feature, then the associated check box is not displayed.
4. (Optional) Choose how to refresh data on this page.

   By default, the page data is not automatically refreshed after you open the page.
   - To refresh the page data for the selected graph type, click ↻.
   - To start refreshing the page data automatically, click ▷. Depending on the selected graph type, the page refreshes at ten-second or five-minute intervals until you click ☐ or navigate to another page.
5. (Optional) Configure the iLO power unit preference by clicking Watts or BTU/hr.

   When you set this value, it is stored in a cookie to provide a consistent web interface experience. The same setting is used on other pages that display power units.
6. (Optional) To view data for a specific point on the graph, move the slider ○ beneath the graph to the point you want to view.

   You can also use the following methods to move the slider:
   - Click the slider track.
   - Click the slider icon, and then press the arrow keys on the keyboard.

Power meter graph display options

Graph Type

Click the 20 min, 24 hr, or 1 week option to select a graph type.

- 20 min—Displays the power usage of the server over the last 20 minutes. The iLO firmware collects power usage information for this graph every 10 seconds.
- 24 hr—Displays the power usage of the server over the last 24 hours. The iLO firmware updates power usage information for this graph

every 5 minutes.

- 1 week—Displays the power usage of the server over the last 1 week. The iLO firmware updates power usage information for this graph once per hour.

Chart data

Use the following check boxes to customize the data included in power meter graphs.

If a server does not support a feature, then the associated check box is not displayed.

- Power Cap—The configured power cap during the sample.
  - 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 lower than the specified percentage threshold between maximum power and idle power might become unreachable because of changes in the server. Hewlett Packard Enterprise does not recommend configuring power caps lower than this threshold. Configuring a power cap that is too low for the system configuration might affect system performance.
- Maximum—The highest instantaneous power reading during the sample. iLO records this value on a subsecond basis.
- Average—The mean power reading during the sample.
- Total CPU—The total power reading for all CPUs in the server.
- Total GPU—The total power reading for all GPUs in the server.

  This value is displayed when:
  - The server has one or more GPUs installed.
  - The OS is running (POST is complete).
  - GPU drivers are installed in the OS.

    For Linux and VMware: NVIDIA option cards must have the vendor driver installed and persistent mode enabled. For more information, see the vendor option card documentation.
  - The GPU supports power reporting.
  - Power history data is available.
- Total DIMM— The total power reading for all DIMMs in the server.

> **NOTE:** For Total DIMM power reporting in Intel platforms, DRAM RAPL Reporting Support option must be enabled in ROM-Based system utility. The default value for RAM RAPL Reporting Support option in ROM-Based system utility is Enabled.

Refreshing power meter data

When you navigate to the Power Meter page, the default 20 minute graph is displayed.

- To refresh the page data for the selected graph type, click . When you use this method, custom graph settings are retained.
- To start refreshing the page data automatically, click . Depending on the selected graph type, the page refreshes at ten-second or five-minute intervals until you click or navigate to another page.

Power unit display

Click Watts or BTU/hr to change the power reading display to watts or BTU/hr.

Viewing a specific data point on the graph

- To view data for a specific point on the graph, move the slider beneath the graph to the point you want to view.

  You can also use the following methods to move the slider:
  - Click the slider track.

- Click the slider icon, and then press the arrow keys on the keyboard.

- When automatic refresh is running, move the slider  beneath the graph to focus on a data point that falls under a specific historical point along the x-axis. For example, on the 20 minute graph, you could position the slider at -10 minutes. Every time the chart refreshes, the slider remains positioned on the values that occurred 10 minutes ago.

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: `Power Metering is unavailable for this configuration`.

Procedure

Click Power & Thermal in the navigation tree, and then click the Power Meter tab.

The Power Status section displays the current power state details.

Current power state details

The values displayed in the Power Status section 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. It is not displayed on servers that do not support power capping.

- 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 supported servers.

- Peak Measured Power—The highest measured power reading.

  This value is displayed for supported 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: `Power Metering is unavailable for this configuration`.

Procedure

Click Power & Thermal in the navigation tree, and then click the Power Meter tab.

The Power History section displays the server power history details.

Power history details

The Power History table shows power readings from four time periods: 5 minutes, 20 minutes, 24 hours, and 1 week.

- 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.

HPE ProLiant RL3XX platforms do not support Power Capping and Power Regulator Mode

Subtopics

Configuring the Power Regulator settings

Configuring power caps

Configuring battery backup unit settings

Configuring SNMP alert on breach of power threshold settings

Configuring the persistent mouse and keyboard setting

Configuring the Power Regulator settings

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: **https://www.hpe.com/support/ilo-docs**.

About this task

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.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Settings tab.
2. Select a Power Regulator mode.

   Only supported modes are listed. Select from the following:

   - Dynamic Power Savings Mode—Intel systems only
   - Static Low Power Mode—Intel systems only
   - Static High Performance Mode—Intel and AMD systems
   - OS Control Mode—Intel and AMD systems
3. Click Apply.

   On Intel systems, if the server is off or in POST, the changes will not take effect until POST is complete.

   On AMD systems, mode changes cannot be applied when the system is in POST.

NOTE: Power Regulator mode can be modified irrespective of the workload profile set in the ROM-based system utility.

- When you click Apply on an Intel system:
  - If you changed to Dynamic Power Savings Mode, Static Low Power Mode, or Static High Performance Mode, iLO notifies you that the Power Regulator settings changed.
  - If you changed to OS Control Mode, or changed from OS Control Mode to any other mode, iLO notifies you that you must reboot the server to complete the change.
- When you click Apply on an AMD system, iLO notifies you that you must reboot the server to complete the change.

4. If a reboot is required, reboot the server.

Subtopics

Power Regulator modes

Power Regulator modes

Choose from the following modes when you configure the Power Regulator settings:

- Dynamic Power Savings Mode—Automatically varies processor speed and power usage based on processor utilization. This option allows the reduction of overall power consumption with little or no impact to performance. It does not require OS support.
- Static Low Power Mode—Reduces processor speed and power usage. This option guarantees a lower maximum power usage 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: **https://www.hpe.com/support/ilo-docs**.
- The server model supports power capping.

  See the server specifications for support information.

  Power capping is not supported on HPE ProLiant RL3xx Gen 11 platforms and Synergy compute modules.
- The power capping feature is enabled in the ROM-based system utility.

  When you reset the BIOS settings to the default values, power capping is disabled in the ROM-based system utility. You must enable the feature before you can use it.
- The server does not have a mismatched power supply configuration.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Settings tab.

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.

Subtopics

Power capping considerations

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 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 Advanced Power Manager

  See the server specifications at **https://www.hpe.com/info/quickspecs** 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

Prerequisites

Configure iLO Settings privilege

About this task

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.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Settings tab.
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.

Subtopics

Battery backup unit options

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: https://www.hpe.com/info/quickspecs.

Configuring SNMP alert on breach of power threshold settings

Prerequisites

Configure iLO Settings privilege

About this task

The SNMP Alert on Breach of Power Threshold feature enables the sending of an SNMP alert when power consumption exceeds a defined threshold.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Settings tab.
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.

Subtopics

SNMP Alert on breach of power threshold options

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 setting

Prerequisites

Configure iLO Settings privilege

About this task

The Other Settings section on the Power Settings page allows you to enable or disable the persistent keyboard and mouse feature.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Power Settings tab.
2. Configure the Enable persistent mouse and keyboard setting.

   iLO notifies you that the settings changed.

Subtopics

Other Settings option

Other Settings option

Enable persistent mouse and keyboard

- **Enabled**—The iLO virtual keyboard and mouse are always connected to the iLO UHCI USB controller.
- **Disabled** (default)—The iLO virtual keyboard and mouse are connected dynamically to the iLO UHCI controller only when a remote console application is open and connected to iLO.

  When this feature is disabled, some servers are able to increase power savings by 15 watts when:
  - The server OS is idle.
  - 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).

Viewing power information

Procedure

Click Power & Thermal in the navigation tree, and then click the Power tab.

The information displayed on the Power Information page varies depending on the server type. The following sections are possible:

- Power Supply Summary
- Power Supplies
- HPE Power Discovery Services
- Battery Backup Units
- Smart Storage Energy Pack
- Power Readings
- Power Microcontroller

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.
- For dual power domain system, power supply redundancy rules are independent for each domain.

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.

- Not Redundant—Indicates that at least one of the power supplies is not providing power to the server. The most common reason for this status is a loss of input power to the power supply.
- Failed Redundant—On servers that support four power supplies, this status indicates that the number of power supplies providing power to the server is less than the number required for server operation. The server might continue to operate, but there is a higher risk of power issues in this state. Verify that your power supply redundancy setting is correct in the ROM-based system utilities.
- 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.

High Efficiency Mode

The redundant power supply mode that will be used when redundant power supplies are configured.

For dual power domain system, high efficiency mode setting is independent for each domain.

The possible values follow:

- N/A—Not applicable.
- Balanced Mode—Delivers power equally across all installed power supplies.
- High Efficiency Mode (Auto)—Delivers full power to one of the power supplies, and places the other power supplies on standby at a lower power-usage level. A semirandom distribution is achieved because the Auto option chooses between the odd or even power supply based on the server serial number.
- High Efficiency Mode (Even Supply Standby)—Delivers full power to the odd-numbered power supplies, and places the even-numbered power supplies on standby at a lower power-usage level.
- High Efficiency Mode (Odd Supply Standby)—Delivers full power to the even-numbered power supplies, and places the odd-numbered power supplies on standby at a lower power-usage level.
- Not Supported—The installed power supplies do not support High Efficiency Mode.

More information

Viewing server power usage

System domain

Summarized information for system redundancy is displayed under System domain. For more information see Power Supplies list (This option is available only for supported servers).

GPU domain

Summarized information for GPU redundancy is displayed under GPU domain. For more information see Power Supplies list (This option is available only for supported servers).

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.
- Model—The power supply model number.
- Spare—The spare power supply part number.
- Serial Number—The power supply serial number.
- Power Consumption—Power consumption of each power supply (watts).
- 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.

More information

Viewing server power usage

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.

Battery Backup Unit details

The following details are displayed on nonblade servers that support a battery backup unit:

- Bay—The bay where the battery backup unit is installed.
- Present—Whether a battery backup unit is installed. The possible values are OK and Battery Failed, and Replace Battery.
- Status—The battery backup unit status. The possible values are OK, Degraded, Failed, or Other.
- Charge—The battery backup unit charge level (percent). The possible charging status values are Fully Charged, Discharging, Charging, Slow Charging, and Not Charging.
- Serial Number—The battery backup unit serial number.
- Capacity—The battery backup unit capacity (watts).
- Firmware—The installed battery backup unit firmware version.

Smart Storage Energy Pack list

The Power Information page displays the following information on servers that support the Smart Storage Energy Pack.

Index

The energy pack index number.

Present

The energy pack installation status. The possible values are OK and Not Installed.

Status

The energy pack health status. The possible values are OK, Degraded, Failed, or Other.

Model

The model number.

Spare

The part number of the spare energy pack.

Serial Number

The energy pack serial number.

Type

The energy pack type.

Firmware

The installed energy pack 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.

The iLO processor is an essential component of the Power Discovery Services infrastructure. The iLO processor communicates with the iPDU attached to each Platinum Plus power supply to determine rack and data center power redundancy. When the iLO processor is part of the Power Discovery Services infrastructure, it intelligently reports external server input power redundancy status and individual (internal) power supply status.

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

Configuring and viewing cooling features

Configuring the minimum fan speed

Prerequisites

Configure iLO Settings privilege

About this task

iLO supports a minimum fan speed (percentage) that prevents the installed fans from running at a speed lower than the configured setting. When the server is running, the fans run at the configured speed or higher.

The minimum fan speed setting overrides the thermal configuration setting if the minimum fan speed is greater than the thermal configuration value.

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Fans or Fans & Cooling Modules tab.

   The tab name depends on the features the server supports.
2. Click  .

   The Fan Settings page opens.
3. Enter the Minimum Fan Speed (%) for all installed fans, and then click OK.

Configuring the thermal configuration setting

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Fans or Fans & Cooling Modules tab.

   The tab name depends on the features the server supports.
2. Click  .

   The Fan Settings page opens.
3. Select a Thermal Configuration value.
4. Click OK.

   iLO notifies you that a reset is required to apply the change.
5. Click Yes, apply and reset.

   iLO saves the change and resets.

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

Thermal configuration settings

Optimal Cooling

Provides the most efficient solution by configuring fan speeds to the minimum required to provide adequate cooling.

Enhanced CPU Cooling

Provides additional cooling to the processors, which can improve performance.

Increased Cooling

Operates fans at a higher speed.

Maximum Cooling

Provides the maximum cooling available for the system.

The thermal configuration setting overrides the minimum fan speed setting if the thermal configuration value is greater than the minimum fan speed value.

Viewing fan information

About this task

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. Click Power & Thermal in the navigation tree, and then click the Fans or Fans & Cooling Modules tab.

   The tab name depends on the features the server supports.

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 summary details

Overall Status

The summarized health status for the installed fans.

Redundancy

The fan redundancy status.

Minimum Fan Speed

The minimum speed for all installed fans (0-100%). When the server is running, the fans run at the configured speed or higher.

Thermal Configuration

The thermal configuration value.

More information

Subsystem and device status values

Fan details

The following details are displayed for each fan:

- Fan—The fan name.
- Location— The location in the server chassis is listed.
- Redundant—Whether there is a backup component for the fan.
- Status—The fan health status.
- Speed—The fan speed (percent).

More information

Subsystem and device status values

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.

Viewing HPE Liquid Cooling Module information

About this task

The information displayed on this page varies depending on the server configuration.

NOTE: Liquid cooling information appears only for supported platforms.

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

Click Power & Thermal in the navigation tree, and then click the Fans & Cooling Modules tab.

HPE Liquid Cooling Module details

The following details are displayed for each HPE Liquid Cooling Module:

- Cooling Pump—The cooling pump name.
- Location—The cooling pump location.
- Redundant—Whether there is a backup component for the cooling pump.
- Status—The cooling pump health status.
- Speed—The cooling pump speed (percent).

HPE Liquid Cooling Module summary details

Overall Status

The summarized health status for the installed cooling pumps.

Redundancy

The cooling pump redundancy status.

Temperature information

The Temperature Information page displays the location, status, temperature, and threshold settings of temperature sensors in the server chassis. It also displays the temperature details of the available PCIe subcomponents.

The name of the PCIe subcomponent is derived from the auxiliary sensor name. If the auxiliary sensor name is not available, then the name is derived from the entity type. If the entity type is also not available, then the name of the PCIe subcomponent appears as NA.

Any PLDM reported adapter temperature sensors (subcomponents) appears in the Temperature Information page in aggregation with the main sensors. The main sensor that has subcomponents will display the details from one of the subcomponent with asterisk (*) character.

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.

Subtopics

Viewing the temperature graph

Procedure

1. Click Power & Thermal in the navigation tree, and then click the Temperatures tab.
2. (Optional) Customize the graph display.
   - To display a three-dimensional graph, enable the 3D option.
   - To display a two-dimensional graph, disable the 3D option.
   - 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.

Subtopics

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. Click Power & Thermal in the navigation tree, and then click the Temperatures tab.
2. (Optional) To expand or collapse details about a subcomponent, click > or ⌄.
3. (Optional) When temperatures are displayed in Celsius, click °F to change the display to Fahrenheit. When temperatures are displayed in Fahrenheit, click the °C switch to change the display to Celsius.
4. (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.

5. (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.

   The subcomponents are prefixed by numbers, which are then sorted based on internal calculation.

Subtopics

Temperature sensor details

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.
- X—The x-coordinate of the temperature sensor.
- Y—The y-coordinate of the temperature sensor.
- Status—The temperature status.
- Reading—The temperature recorded by the temperature sensor. If a temperature sensor is not installed, the Reading column shows the value N/A.
- Thresholds—The temperature thresholds for the warning for overheating conditions. The two threshold values are Caution and Critical. If a temperature sensor is not installed, the Thresholds column shows the value N/A. Devices with vendor-controlled threshold also show the value N/A.

NOTE: In addition to reporting the historical CPU temperature, iLO 6 also reports the CPU package temperature.

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.

  In this case, iLO 6 shuts down immediately. In another mechanism the shutdown is delayed by about 10 seconds.

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).

> **NOTE:**
> For Linux and VMware: NVIDIA option cards with a memory thermal sensor require installation of the vendor driver and persistent mode enabled. For more information, see the vendor option card documentation.

Configuring user defined threshold using the RESTful Interface Tool

Procedure

1. Open a text editor and create a file to define the User Defined Temperature threshold value.

   Use the following example as a template.

   ```
   {
   "path":"/redfish/v1/Chassis/1/Thermal/Actions/Oem/Hpe/HpeThermalExt.SetUserTempThreshold/",
   "body": {"SensorNumber": Supported Temperature Sensor,
   "ThresholdValue": Desired threshold temperature,
   "AlertType": "Warning" or "Critical"
   }
   }
   ```

2. Save the file as `filename.json`.
3. Start the RESTful Interface Tool.
4. Enter **`ilorest`**.
5. Log in to an iLO system:

   ```
   iLOrest > login iLO host name or IP address -u iLO user name -p iLO password
   ```

6. Enter the command to configure the alert:

   ```
   rawpatch filename.json
   ```

Using the performance management features

Subtopics

Performance monitoring

Workload advisor

Performance monitoring

Performance management features are applicable to Intel platforms only.

The Performance - Monitoring page provides performance data collected from the following sensors.

CPU Utilization

This sensor reports the utilization of all processors installed in the system. The measurement is based on a percentage of the maximum compute capacity of the processor. It considers how slow or fast the processor runs when doing work. This measurement might differ from the values that some OS report for utilization, which is often calculated by how often the processor is not idle.

Memory Bus Utilization

This sensor reports the utilization of the total bandwidth of the memory bus. The measurement is based on a percentage of the maximum memory bandwidth of the configuration. This measurement might differ from the values that some OS report for memory utilization, which is often calculated by how much of the available system memory is being used or allocated.

I/O Bus Utilization

This sensor reports the utilization of all processors connected to I/O buses (total PCI-e bus bandwidth). The measurement is based on a percentage of the maximum total bandwidth of these buses. This measurement is not an indication of how busy an I/O device might be, but rather how much PCI-e bandwidth the device is using.

CPU Interconnect Utilization

This sensor reports the calculated bandwidth usage of the link connecting multiple processor sockets in the system. It is an aggregate of all the links within the system.

Average CPU Frequency

This sensor reports the average overall processor frequency. A value of zero means that the processor is idle. This value is different from the "running frequency" often seen under some OS that measures frequency only when the processor is not idle.

CPU Power

This sensor reports the power consumed by the processor. It is based on an energy accumulator within the processor and is the value that the processor uses to regulate power limits internally.

The information on this page might differ from the Total CPU power data on the Power Meter page.

Subtopics

Viewing performance data

Configuring performance alerts

Viewing performance data

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: **https://www.hpe.com/support/ilo-docs**.

  If a license is not installed, a message is displayed, and only the 10 minute graph is available.
- MCTP Discovery is enabled.
- The iLO Date/Time is set correctly to ensure collection of valid performance telemetry samples.

About this task

When the server is powered off or in POST, a message is displayed, and measured performance values display the value 0. Performance data is updated when the server is powered on and POST is complete. After a reset, there might be 0 values in the graph where data was not collected when the server was off or in POST. To confirm that these values are due to a server reset, check the IML.

When iLO is reset:

- Performance data for the 10 min and 1 hr intervals is cleared.

- Data from the 24 hr and 1 week graphs is saved, and can be viewed after a reset is complete.
- Hourly data might be missing when you view the 24 hr and 1 week graphs after a reset is complete.

Procedure

1. Click Performance in the navigation tree, and then click the Monitoring tab.
2. Select a sensor in the Selected Sensor menu.
3. Click one of the following options to select a graph interval:
   - 10 min
   - 1 hr
   - 24 hr
   - 1 week

   The graph is populated with data for the requested interval.
4. (Optional) To view data for a specific point on the graph, move the slider beneath the graph to the point you want to view.

   When you move the slider, details for the selected point on the graph are displayed next to the graph.
5. (Optional) If you selected CPU Power or Average CPU Frequency, select or clear the check boxes in the CPU list next to the graph.

   Select a CPU check box to display it in the graph. Clear a CPU check box to remove it from the graph.
6. (Optional) Choose how to refresh data on this page.

   By default, the page data is not automatically refreshed after you open the page.
   - To refresh the page data for the selected graph type, click .
   - To start refreshing the page automatically, click . Depending on the selected graph type, the page refreshes at ten-second or five-minute intervals. The page refreshes until you click or navigate to another page.

Subtopics

Performance data details

Performance monitoring graph display options

More information

Viewing installed firmware information
Configuring MCTP discovery

Performance data details

The Performance Data section shows the following details:

Sensor

The name of the selected sensor.

Maximum

The maximum measured value.

Minimum

The minimum measured value.

Performance monitoring graph display options

Selected Sensor menu

To view performance data for a sensor, select the sensor in the Selected Sensor menu.

Graph Type

To specify the graph time period, click a graph type name:

- 10 min—Displays performance data for the last 10 minutes. The iLO firmware collects performance data for this graph every 20 seconds. The maximum number of samples displayed in the graph is 30.
- 1 hr—Displays the performance data for the last hour. The iLO firmware collects performance data for this graph every 20 seconds. The maximum number of samples displayed in the graph is 180.
- 24 hr—Displays the performance data for the last 24 hours. The iLO firmware collects performance data for this graph every 5 minutes. The maximum number of samples displayed in the graph is 288.
- 1 week—Displays the performance data for the last week. The iLO firmware collects performance data for this graph every 30 minutes. The maximum number of samples displayed in the graph is 336.

Refreshing performance graphs

- To refresh the page data for the selected graph type, click .
- To start refreshing the page automatically, click .

  The page refreshes automatically until you click or navigate to another page.

Viewing a specific data point on the graph

- To view data for a specific point on the graph, move the slider beneath the graph to the point you want to view.

  You can also use the following methods to move the slider:

  - Click the slider track.
  - Click the slider icon, and then press the arrow keys on the keyboard.

  When you move the slider, details for the selected point on the graph are displayed next to the graph.
- When automatic refresh is running, move the slider beneath the graph to focus on a data point that falls under a specific historical point along the x-axis.

Configuring performance alerts

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: **https://www.hpe.com/support/ilo-docs**.
- MCTP discovery is enabled.
- The iLO Date/Time is set correctly to ensure collection of valid performance telemetry samples.

About this task

You can configure performance alerts that will post an event in the IML when a configured threshold is reached.

Upper and lower thresholds are supported for the CPU Utilization, Memory Bus Utilization, and I/O Bus Utilization sensors.

Upper thresholds are supported for the CPU Interconnect Utilization, CPU Power, and Jitter Count sensors.

Procedure

1. Click Performance in the navigation tree, and then click the Monitoring tab.
2. Select a sensor that supports performance alerts.
3. Enter the threshold settings and dwell time, and then click Apply.

   To disable an alert, set the dwell time to 0.

Subtopics

Performance alert settings options

More information

Viewing installed firmware information

Performance alert settings options

Lower Threshold

The lowest value the sensor can report before an event is posted in the IML.

Enter a percentage of utilization.

Upper Threshold

The highest value the sensor can report before an event is posted in the IML.

- For utilization sensors, enter a percentage of utilization for the selected sensor.
- For CPU Power, enter a value in watts.
- For Jitter Count, enter the threshold count.

Dwell Time

The number of seconds the sensor reading is higher or lower than the configured value before the threshold is violated. When a threshold is violated, an event is posted in the IML.

For example, if you set an upper threshold to 70% with a dwell time of 40 seconds, an event is posted when the sensor reports readings over 70% for more than 40 seconds.

- To enable an alert, set the dwell time to a valid value in multiples of 20, between 20 and 64800 (20 seconds to 18 hours). If you enter a value that is not a multiple of 20, the value is rounded up to the next multiple of 20.
- To disable an alert, set the dwell time to 0.

Workload advisor

iLO monitors selected server workload characteristics and provides recommended performance tuning settings based on the monitored data.

HPE ProLiant RL3xx Gen 11 platforms do not support the following features or options:

- Workload advisor
- Workload profiles
- Performance telemetry

Subtopics

Viewing server workload details

Configuring the performance tuning options

Viewing server workload details

Prerequisites

- Host BIOS 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: **https://www.hpe.com/support/ilo-docs**.
- The server is powered on and POST is complete.

  Make sure that the server was powered on for the time interval you want to monitor. For example, data for the 24-hour interval is not available until the server has been powered on for 24 hours.
- MCTP discovery is enabled.
- The iLO Date/Time is set correctly to ensure collection of valid performance telemetry samples.

Procedure

1. Click Performance in the navigation tree, and then click the Workload Advisor tab.
2. Review the details in the Server Workload section.

   If iLO was reset, information for the 10 min and 1 hr intervals will be available after the server has been powered on for 10 minutes or 1 hour.
3. (Optional) To update the table with the latest information, click ↻.

Subtopics

Server workload details

More information

Configuring MCTP discovery
Viewing installed firmware information
Configuring iLO SNTP settings

Server workload details

Workload characteristics are qualitative assessments of how the workload is using system resources. They are based on the quantitative measurements from the performance monitoring events and are useful as a reference when making tuning decisions. These observed characteristics are typically needed for making intelligent tuning decisions. For instance, a specific BIOS option might provide benefits only if the workload has a high degree of NUMA awareness.

The following workload characteristics are displayed:

- CPU Utilization—How busy the processors are in the server.
- Memory Bus Utilization—The amount of memory traffic observed by the server.
- I/O Bus Utilization— The amount of I/O traffic observed by the server.
- NUMA Awareness—How the workload is distributing memory and I/O accesses across multiple processors. A high degree of NUMA awareness means that I/O and memory traffic are directed more to local resources versus remote resources.

The possible values are High, Medium, and Low.

Server workload data for the 10 min and 1 hr intervals is cleared when iLO is reset.

Configuring the performance tuning options

Prerequisites

- Host BIOS 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: **https://www.hpe.com/support/ilo-docs**.
- The server is powered on and POST is complete.

  Make sure that the server was powered on for the time interval you want to monitor. For example, data and recommendations for the 24 hr interval are not available until the server has been powered on for 24 hours.
- MCTP discovery is enabled.
- The iLO Date/Time is set correctly to ensure collection of valid performance telemetry samples.

Procedure

1. Click Performance in the navigation tree, and then click the Workload Advisor tab.
2. Select a value in the Selected Duration menu.

   You can review recommended settings based on data collected in 10 min, 1 hr, or 24 hr intervals.
3. Review the recommendations in the Recommended Setting column.

   If iLO was reset, information for the 10 min and 1 hr intervals will be available after the server has been powered on for 10 minutes or 1 hour.
4. To change one or more settings, click Settings.
5. Change the tuning options as needed, and then click Apply.

   iLO notifies you that changing the tuning options will change the Workload Profile setting to Custom.
6. Click Yes, apply.

   iLO saves the settings and notifies you that a server reboot is required for the changes to take effect.
7. Reboot the server.

   You can click the link in the status banner to navigate to the Server Power page.

Subtopics

Performance tuning settings

More information

Configuring MCTP discovery
Viewing installed firmware information
Configuring iLO SNTP settings

Performance tuning settings

Sub-NUMA Clustering

When this option is set to Enabled, this feature divides the processor cores, cache, and memory into multiple NUMA domains. Enabling

this feature can increase performance for workloads that are NUMA-aware and optimized.

When this feature is enabled, up to 1 GB of system memory might become unavailable.

NUMA Group Size Optimization

This option sets how the system BIOS reports the size of a NUMA node (number of logical processors), which assists the OS in grouping processors for application use (Kgroups). The default value Clustered provides better performance because it optimizes the resulting groups along NUMA boundaries. Some applications might not be optimized to take advantage of processors that span multiple groups. In such cases, it might be necessary to select the Flat option to allow affected applications to use more logical processors.

Uncore Frequency Scaling

This option controls the frequency scaling of the internal processor buses (the uncore). Setting this option to Auto enables the processor to dynamically change frequencies based on workload. Setting the Maximum or Minimum frequency enables tuning for latency or power consumption.

Memory Refresh Rate

This option controls the refresh rate of the memory controller. It might affect the performance and resiliency of the server memory. Hewlett Packard Enterprise recommends using the default value (1x Refresh) unless changing this value is recommended in other documentation for the server.

Power Regulator

Use this option to configure Power Regulator support. The following values are available:

- 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.

NOTE:

The Power Regulator setting displayed on the Workload Performance Advisor page reflects the static boot time configuration. It does not reflect run-time changes to this setting that have been applied since system power-on. Applying recommended settings changes on the Workload Performance Advisor page changes only the boot time configuration of this setting. A system reboot is required for the change to take effect.

Minimum Processor Idle Power Package C-state

Use this option to select the lowest idle power state (C-state) of the processor that the operating system uses. The higher the C-state, the lower the power usage of that idle state. C6 State is the lowest power idle state supported by the processor.

Energy/Performance Bias

Use this option to configure several processor subsystems to optimize the performance and power usage of the processor. The following values are available:

- Maximum Performance—This setting is for environments that require the highest performance and lowest latency, but are not sensitive to power consumption.
- Balanced Performance—This setting provides optimum power efficiency. Hewlett Packard Enterprise recommends this setting for most environments.
- Balanced Power—Provides optimum power efficiency based on server utilization.
- Power Savings Mode—This setting is suitable for environments that are power sensitive and can accept reduced performance.

Configuring iLO network settings

Subtopics

iLO network settings

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

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

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

Viewing the network configuration summary

Procedure

Depending on your network configuration, click iLO Dedicated Network Port or iLO Shared Network Port in the navigation tree.

The Network Summary tab is displayed.

Subtopics

Network information summary

The Information section displays the following details.

NOTE:

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

You can configure the 802.1X Support setting on the Access Settings page.

- 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 Setting—The link setting of the selected iLO network interface. The default value is Auto-Negotiate.

  This value is not displayed when:

  - The server is configured to use the Shared Network Port. This value must be managed in the host operating system when the Shared Network Port is enabled.
  - The server is configured to use the iLO Dedicated Network Port, and the server model does not support changing this value.
- Current Link Speed—The link speed of the network interface in megabits per second.

  The iLO Shared Network Port connection can operate up to a maximum speed of 100 Mbps. When the iLO Shared Network Port is enabled, the actual speed of the physical link or the external NIC port is displayed on iLO web interface.

  When the iLO Shared Network Port is used, 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.
- Duplex Setting—The link duplex setting for the selected iLO network interface. The default value is Auto-Negotiate.

  This value is not displayed when:

  - The server is configured to use the Shared Network Port. This value must be managed in the host operating system when the Shared Network Port is enabled.
  - The server is configured to use the iLO Dedicated Network Port, and the server model does not support changing this value.
- Current Duplex—Full-duplex or Half-duplex.
- 802.1X Support—Whether 802.1X Support is enabled or disabled.

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

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.

IPv6 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 follow:

- Active—The address is in use by iLO.
- Pending—Duplicate address detection is in progress.
- Failed—Duplicate address detection failed. The address is not in use by iLO).
- Invalid—The RA (Router Advertised) valid lifetime for the address prefix was not renewed, and it expired. This address is no longer in use.

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 iLO 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. Click iLO Dedicated Network Port or iLO Shared Network Port in the navigation tree.
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.

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

   To use a static domain name, disable the Use DHCPv4 Supplied Domain Name and Use DHCPv6 Supplied Domain Name settings on the IPv4 Settings and IPv6 Settings pages.

5. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.

6. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.

7. When you are finished configuring the iLO network settings, click Reset iLO.

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

More information

Configuring the iLO hostname and domain name for Kerberos authentication
Configuring IPv4 settings
Configuring IPv6 settings

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.

The NIC settings section is not available on Synergy compute modules.

Enabling the iLO Dedicated Network Port through the iLO web interface

Prerequisites

- Configure iLO Settings privilege
- If the default server configuration does not support remote management, an optional iLO network enablement module is installed.

Procedure

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Click iLO Dedicated Network Port in the navigation tree.
3. Click the General tab.
4. Select the Use iLO Dedicated Network Port check box.
5. Select a Link Setting.
6. To use a VLAN, set the Enable VLAN option to enabled.
7. If you enabled the VLAN option, enter a VLAN Tag.
8. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.
9. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.
10. When you are finished configuring the iLO network settings, click Reset iLO.

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

More information

iLO network connection considerations
iLO network port configuration options

Dedicated Network Port General settings

Link Setting

This value controls the speed and duplex settings of the iLO network transceiver.

Choose from the following values:

- 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).
- 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.

Some server models prevent changing the link speed and duplex setting when the Dedicated Network Port is enabled.

Enable VLAN

When VLAN is enabled, the iLO Dedicated 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.

Enabling the iLO Shared Network Port through the iLO web interface

Prerequisites

- Configure iLO Settings privilege

- If the default server configuration does not support remote management, an optional iLO network enablement module is installed.
- Supported network cards are available in the system.

Procedure

1. Connect the Shared Network Port OCP1, OCP2, or Embedded NIC to a LAN.
2. Click iLO Shared Network Port in the navigation tree, and then click the General tab.
3. Select the Use Shared Network Port check box.
4. Select a network card from the list of available options.
5. Select a value from the Port menu.
6. To use a VLAN, set the Enable VLAN option to enabled.
7. If you enabled the VLAN feature, enter a VLAN Tag.
8. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.
9. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.
10. When you are finished configuring the iLO network settings, click Reset 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 OCP1, OCP2, or Embedded NIC port.

More information

iLO network connection considerations
iLO network port configuration options

Shared Network Port General settings

NIC

The server NIC type.

Port

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 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 on the back of the server.

  The RJ-45 jack is labeled iLO.

  On some servers, this option is provided by installing an optional iLO network enablement module.

A dedicated management network is the preferred iLO network configuration.

- Shared Network Port—Depending on your configuration, the following Shared Network Port options are available:
  - Shared Network Port OCP1—Uses an optional Open Compute Project NIC installed in OCP slot 1. This NIC normally handles server network traffic. It can be configured to handle iLO network traffic at the same time through a common SFP or RJ-45 connector.
  - Shared Network Port OCP2—Uses an optional Open Compute Project NIC installed in OCP slot 2. This NIC normally handles server network traffic. It can be configured to handle iLO network traffic at the same time through a common SFP or RJ45 connector.
  - Shared Network Port Embedded NIC—Uses a permanently installed NIC that is built into the server. This NIC normally handles server network traffic. It can be configured to handle iLO network traffic at the same time through a common RJ45 connector.

For information about the NICs your server supports, see the server specifications at the following website: **https://www.hpe.com/info/quickspecs**.

Shared network port consideration

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 OS 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 can operate up to a maximum speed of 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.

HPE ProLiant RL3xx platforms do not support Shared network port option.

For more information about the Shared network port consideration, see iLO 6 Troubleshooting guide.

iLO network connection considerations

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

  If both the server and the NIC support port selection, the iLO firmware allows you to select a different port number. If a port other than port 1 is selected for Shared Network Port use, and your server does not support that configuration, iLO switches back to port 1 when it starts.
- On servers that do not include 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, or using the Dedicated Network Port. For more information about network connectivity, see the iLO specifications document at the following website: **https://www.hpe.com/info/quickspecs**.

  If the switch port that iLO is connected to is configured for 1Gb/s, some copper iLO Shared Network Port adapters might lose connectivity when the server is powered off. Connectivity will return when the server is powered back on.
- Disabling the iLO Shared Network Port does not completely disable the system NIC—server network traffic can still pass through the NIC port. When the iLO Shared Network Port is disabled, any traffic going to or originating from iLO will not pass through the Shared Network Port.

- If the Shared Network Port is enabled, you cannot modify the link setting or duplex setting. When using Shared Network Port configurations, these settings must be managed in the operating system.
- Some servers require an optional iLO network enablement module to add support for remote management through a dedicated management network (default) or a shared network connection. If an iLO network enablement module is not installed, iLO access is supported only through host-based (in-band) access methods. Some examples of the supported host-based access methods include the iLO RESTful API, UEFI System Utilities, iLO Service Port (if available), and the Virtual NIC.

Configuring IPv4 settings

Prerequisites

Configure iLO Settings privilege

About this task

When you configure the IPv4 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.

Procedure

1. Click iLO Dedicated Network Port or iLO Shared Network Port in the navigation tree, and then click the IPv4 tab.
2. Configure the DHCPv4 Configuration settings.
3. Configure the Static IPv4 Address Configuration settings.
4. Configure the DNS Configuration settings.
5. Configure the Static Route Configuration settings.
6. Configure the Ping Gateway on Startup setting.
7. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.
8. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.
9. When you are finished configuring the iLO network settings, click Reset iLO.

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

DHCPv4 Configuration settings

The DHCPv4 settings are enabled by default.

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 Setting, Static Route #2 Setting, and Static Route #3 Setting boxes.

Use DHCPv4 Supplied Domain Name

Specifies whether iLO uses the DHCP server-supplied domain name. If DHCP is not used, enter a domain name in the Domain Name

box on the Network General Settings page.

Use DHCPv4 Supplied DNS Servers

Specifies whether iLO uses the DHCP server-supplied DNS server list. If not, enter the DNS server addresses in the Primary DNS Server, Secondary DNS Server, and Tertiary DNS Server boxes.

Use DHCPv4 Supplied Time Settings

Specifies whether iLO uses the DHCPv4-supplied NTP service locations.

Use DHCPv4 Supplied WINS Servers

Specifies whether iLO uses the DHCP server-supplied WINS server list. If not, enter the WINS server addresses in the Primary WINS Server and Secondary WINS Server boxes.

NOTE:

To create a reservation in a DHCP server, a DHCP client identifier (unique identifier) is required. For iLO 6 systems, the DHCP client identifier is the hardware MAC address followed by three bytes (six characters) of zero. For example, if the iLO 6 MAC address is 00-53-00-AA-BB-CC, then the associated DHCP client identifier is `005300AABBCC000000`.

Static IPv4 Address Configuration 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.

IPv4 DNS Configuration 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

Enable or disable this option to specify whether iLO registers its IPv4 address and name with a DNS server.

This option is enabled by default.

IPv4 Static Route Configuration settings

Static Route #1 Setting, Static Route #2 Setting, and Static Route #3 Setting

The iLO static route destination, mask, and gateway addresses. If Use DHCPv4 Supplied Static Routes is enabled, these values are supplied automatically. If not, enter the static route values.

Other IPv4 settings

Ping Gateway on Startup

Enable this option to configure 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.

This option is enabled by default.

Configuring IPv6 settings

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click iLO Dedicated Network Port or iLO Shared Network Port in the navigation tree.
2. Click the IPv6 tab.
3. Configure the Global IPv6 Configuration settings.
4. Configure the DHCPv6 Configuration settings.
5. Configure the DNS Configuration settings.
6. Configure the Static IPv6 Address Configuration settings.
7. Configure the Static Route Configuration settings.
8. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.
9. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.
10. When you are finished configuring the iLO network settings, click Reset iLO.

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

Global IPv6 Configuration 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 it accesses a client application. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.

- Enable this option if you want iLO to use IPv6 first.
- Disable this option if you want iLO to use IPv4 first.

If communication fails using the first protocol, iLO automatically tries the second protocol.

This option is enabled by default.

Enable Stateless Address Auto Configuration (SLAAC)

Enable this option to configure iLO to create IPv6 addresses for itself from router advertisement messages.

iLO creates its own link-local address even when this option is not enabled.

This option is enabled by default.

DHCPv6 Configuration settings

Enable DHCPv6 in Stateful Mode (Address)

Enable this option to allow iLO to request and configure IPv6 addresses provided by a DHCPv6 server.

This option is enabled by default.

- 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.

This option is disabled by default.

Enable DHCPv6 in Stateless Mode (Other)

Enable this option to configure iLO to request settings for NTP and DNS service location from the DHCPv6 server.

This option is enabled by default.

- Use DHCPv6 Supplied Domain Name—Select this check box to use the DHCPv6 server-supplied domain name.

  This option is enabled by default.

- 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.

  This option is enabled by default.

- 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.

  This option is enabled by default.

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 Configuration 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

Enable or disable this option to specify whether iLO registers its IPv6 address and name with a DNS server.

This option is enabled by default.

Static IPv6 Address Configuration 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.

Status information is displayed for each address.

Static Default Gateway

Enter a default IPv6 gateway address for cases in which no router advertisement messages are present in the network.

IPv6 Static Route Configuration settings

Static Route #1 (Destination), Static Route #2 (Destination), and Static Route #3 (Destination)

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.
Status information is displayed for each Static Route value.

iLO features that support IPv6

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:

HPE ProLiant RL3xx Gen 11 platforms do not support RIBCL and iLO Federation.

- IPv6 over Shared Network Port connections
- 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
- 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
- URL-based virtual media
- CLI/RIBCL key import over an IPv6 connection
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation
- IPMI
- Embedded remote support

Configuring iLO SNTP settings

Prerequisites

- Configure iLO Settings privilege
- At least one NTP server is available on your management network.
- If you will use a DHCPv4-provided NTP service configuration, DHCPv4 is enabled on the IPv4 tab.
- If you will use a DHCPv6-provided NTP service configuration, DHCPv6 Stateless Mode is enabled on the IPv6 tab.

Procedure

1. Click iLO Dedicated Network Port or iLO Shared Network Port in the navigation tree.
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.

   On nonblade servers, this setting is called Propagate NTP Time to Host.
6. Click Apply to save the changes.

   iLO notifies you that an iLO reset is required for one or more pending changes to take effect. If your account is assigned the Configure iLO Settings privilege, the Reset iLO button is included in the message.

   This message is displayed on all iLO Dedicated Network Port or iLO Shared Network Port tabs until an iLO reset is complete.
7. (Optional) Configure other network settings on the General, IPv4, IPv6, and SNTP tabs.
8. When you are finished configuring the iLO network settings, click Reset iLO.

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

Subtopics

SNTP options

iLO clock synchronization

DHCP NTP address selection

More information

Configuring IPv4 settings
Configuring IPv6 settings
DHCP NTP address selection
iLO clock synchronization

SNTP options

Use DHCPv4 Supplied Time Settings

Configures iLO to use a DHCPv4-provided NTP server address.

This option is enabled by default.

Use DHCPv6 Supplied Time Settings

Configures iLO to use a DHCPv6-provided NTP server address.

This option is enabled by default.

NTP time propagation setting

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

- Propagate NTP Time to Host—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 default settings.

  For all servers the setting will be effective only when #PRODABR# is able to obtain time from an NTP time source.

  NTP time source can be HPE OneView for Synergy servers.

- Propagate NTP —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.

This option is disabled by default.

NOTE:

- When BIOS Time Format is set to UTC, then along with the server time, the server time zone setting is also synchronized with the iLO time zone setting.
- During the first POST after AC power is applied, if iLO is not able to obtain time from the configured NTP server, then iLO synchronizes its time and time zone with the time and time zone configured in the BIOS.

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 logs to display the correct local time, you must specify the server location time zone, and select Show Local Time in the log display filters.

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 Greenwich (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 System ROM during POST.

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 Gen10 and later 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.

Subtopics

NIC auto-selection support

iLO startup behavior with NIC auto-selection enabled

Enabling iLO NIC auto-selection

Configuring NIC failover

More information

Enabling iLO NIC auto-selection

NIC auto-selection support

- ProLiant Gen10 and later nonblade servers support NIC auto-selection.
- iLO 6 can be configured to search both Shared Network Ports on servers that support this configuration.
- iLO 6 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 `oemhpe_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 6 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.

More information

iLO NIC auto-selection
NIC auto-selection support
iLO startup behavior with NIC auto-selection enabled

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 6 Scripting and Command Line Guide.

Procedure

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

More information

Enabling iLO NIC auto-selection

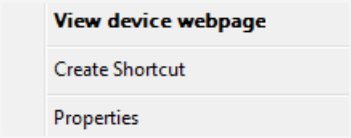
Viewing iLO systems in the Windows Network folder

About this task

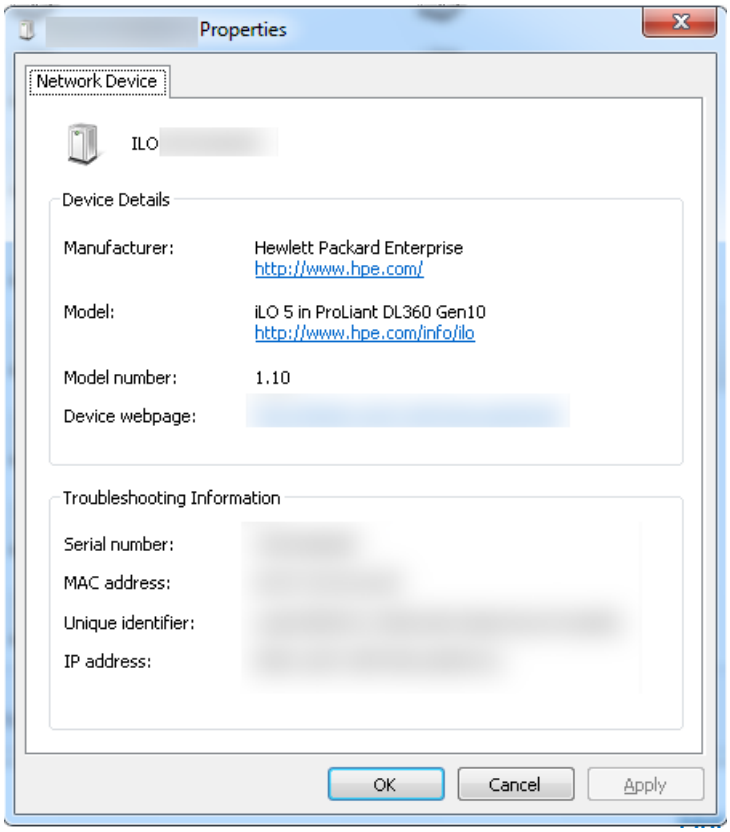
If UPnP is configured, iLO systems on the same network as a Windows system are displayed in the Windows Network folder.

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.

Managing remote support

Subtopics

HPE embedded remote support

HPE iLO 6 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.

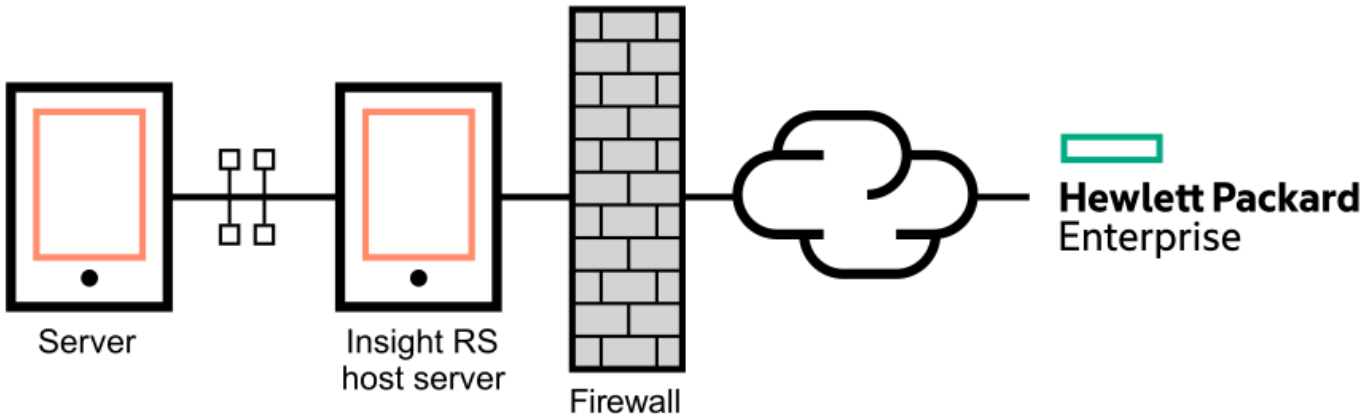
Connecting a device to Hewlett Packard Enterprise allows it to be remotely supported and to send diagnostic, configuration, telemetry, and contact information to Hewlett Packard Enterprise. No other business information is collected, and the data is managed according to the Hewlett Packard Enterprise privacy statement. You can view the privacy statement at the following website: https://www.hpe.com/info/privacy.

IMPORTANT:

HPE now supports only Insight Remote Support central connect. If you are using HPE Insight Online direct connect, Hewlett Packard Enterprise recommends to unregister Insight Online direct connect and register with Insight Remote Support central connect.

Insight Remote Support central connect

Register a supported device 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.



Device support

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

IMPORTANT:

If you use HPE OneView to manage your environment, use it to register for remote support. For more information, see the HPE OneView user guide.

Insight Remote Support central connect

- HPE ProLiant Gen10 servers

- HPE ProLiant Gen10 Plus servers
- HPE ProLiant Gen11 servers

HPE ProLiant RL3xx Gen 11 platforms do not support Insight Remote Support.

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.

More information

Active Health System
Remote Support data collection
Remote support service events

Prerequisites for remote support registration

Procedure

1. Install a supported browser to use when you log in to the remote support solution components .
2. 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: **https://www.hpe.com/support/hpesc**.
3. Collect the following information. This information is used during 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.
4. 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.
5. 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.
6. Set up the Insight Remote Support central connect environment .

Subtopics

Supported browsers for HPE embedded remote support

Setting up a ProLiant server for remote support registration

Setting up the Insight Remote Support central connect environment

Supported browsers for HPE embedded remote support

iLO

iLO 6 supports the browsers listed in Supported browsers.

Insight RS

- Mozilla Firefox: 49.x
- Google Chrome: 53.x

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 **Service Pack for ProLiant**. The SPP includes the iLO firmware, iLO 6 Channel Interface Driver, and AMS. Download the SPP from the SPP download page at **https://www.hpe.com/servers/spp/download**.

You can download the iLO 6 Channel Interface Driver, iLO firmware, and AMS separately at the following website: **https://www.hpe.com/support/ilo6**.

Procedure

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

   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.

   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 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 RS:
   - For Windows systems only, start the operating system. 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 RS.
6. On Windows servers: Install the iLO 6 Channel Interface Driver.

   For Red Hat Enterprise Linux and SUSE Linux Enterprise Server, the driver is included in the Linux distribution.
7. Verify that the time zone is set in iLO.

More information

Installing the iLO drivers
Installing AMS
Configuring iLO network settings
Configuring iLO SNTP settings
Viewing the network configuration summary
iLO encryption settings
Viewing installed firmware information

Setting up the Insight Remote Support central connect environment

About this task

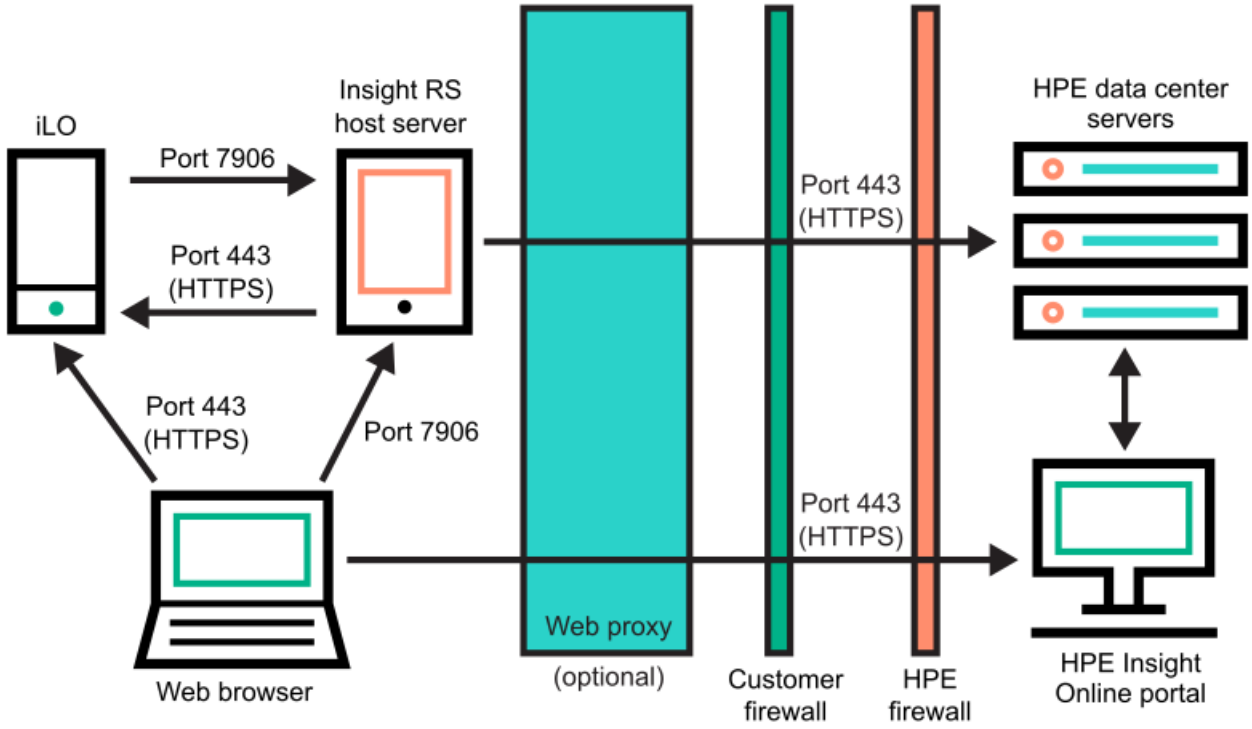
Insight Remote Support relies on communication between your environment and Hewlett Packard Enterprise to deliver support services.

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 Network requirements for Insight Remote Support central connect.

Figure 1. 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`).

Registering for Insight Remote Support central connect

Prerequisites

- Your environment meets the prerequisites for embedded remote support registration.
- Configure iLO Settings privilege

Procedure

1. Click Remote Support in the navigation tree.

   The Registration page is displayed.

2. 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.

3. Click **Register**.

   iLO notifies you that the registration process is finished.

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

More information

Prerequisites for remote support registration
Sending a test service event
Enabling AlertMail
Changing a supported device from direct connect to central connect remote support

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. Click Remote Support in the navigation tree.

   The Registration page is displayed.

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 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.

HPE ProLiant RL3xx Gen 11 platforms do not support Insight Remote Support.

Subtopics

Service event transmission

Setting maintenance mode

Editing the maintenance mode expiration time

Clearing maintenance mode

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.

Setting maintenance mode

Prerequisites

- Configure iLO Settings privilege
- The server is registered for remote support.

About this task

Use maintenance mode when you perform maintenance on a server. When maintenance mode is set, communications sent to Insight RS are flagged to indicate that action is not required. This feature helps Hewlett Packard Enterprise to determine whether to open a support case.

Procedure

1. Click Remote Support in the navigation tree, and then click the Service Events tab.
2. Click  in the Maintenance Mode section.

   The Edit Maintenance Mode Settings page opens.
3. Select the Maintenance Mode check box.
4. Select a time from the Expires in menu.
5. Click Apply.

   iLO notifies you that maintenance mode is set.

   Maintenance mode ends automatically when the specified time period has passed. If needed, you can clear maintenance mode manually.

   An event is recorded in the iLO event log when maintenance mode is set, expired, or cleared.

Editing the maintenance mode expiration time

Prerequisites

- Configure iLO Settings privilege
- The server is registered for remote support.
- Maintenance mode is enabled.

Procedure

1. Click Remote Support in the navigation tree, and then click the Service Events tab.

   The Service Events page shows the time remaining for maintenance mode.

2. Click  in the Maintenance Mode section.

   The Edit Maintenance Mode Settings page opens.

3. Select a new value in the Expires in menu, and then click Apply.

   iLO notifies you that maintenance mode is set.

   Maintenance mode ends automatically when the specified time period has passed. If needed, you can clear maintenance mode manually.

   An event is recorded in the iLO event log when maintenance mode is set, expired, or cleared.

Clearing maintenance mode

Prerequisites

- Configure iLO Settings privilege
- The server is registered for remote support.

Procedure

1. Click Remote Support in the navigation tree, and then click the Service Events tab.
2. Click  in the Maintenance Mode section.

   The Edit Maintenance Mode Settings page opens.

3. Clear the Maintenance Mode check box, and then click Apply.

   iLO notifies you that maintenance mode is cleared and an event is recorded in the iLO event log.

Viewing maintenance mode status

Prerequisites

The server is registered for remote support.

Procedure

Click Remote Support in the navigation tree, and then click the Service Events tab.

The Maintenance Mode section shows the current maintenance mode status.

If maintenance mode is enabled, the remaining time is displayed. The remaining time is updated when you refresh the browser window or send a test service event.

Sending a test service event

Prerequisites

- Configure iLO Settings privilege
- The server is registered for remote support.

About this task

You can send a test event to verify that your remote support configuration is working correctly.

Procedure

1. Click Remote Support in the navigation tree, and then click the Service Events tab.
2. Click Send Test Event.
3. When prompted to confirm the request, click Yes, send.

   When the transmission is complete, the test event is listed in the service event log and the Insight RS Console.

   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) You can view the test event in the Insight RS Console.

Subtopics

Viewing a test service event by using the Insight RS Console

More information

Viewing a test service event by using the Insight RS Console

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, 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

Click Remote Support in the navigation tree, and then click the Service Events tab.

Subtopics

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.
- 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
202	Power Fuse 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
307	NVMe Drive Status Change
308	NVMe Drive Wear Status Change
309	SSD Drive Wear Status Change
400	Memory Module Failed or Predicted to Fail Event
401	NVDIMM Failure
500	Storage System Fan Status Changed Event
501	Storage System Power Supply Status Changed Event
600	Uncorrectable Machine Check Exception Event
1000	Generic IML Service Event

Clearing the service event log

Prerequisites

- Configure iLO Settings privilege
- The server is registered for remote support.

Procedure

1. Click Remote Support in the navigation tree, and then click the Service Events tab.
2. Click Clear Event Log.

   iLO prompts you to confirm the request.

3. Click Yes, clear.

   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.

Subtopics

Sending data collection information

Sending Active Health System reporting information

Viewing data collection status in iLO

Viewing Active Health System reporting status in iLO

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

Sending data collection information

Prerequisites

Configure iLO Settings privilege

About this task

The Insight RS host server sends server health, configuration, and run-time telemetry information to Hewlett Packard Enterprise for analysis and proactive services in accordance with your warranty and service agreements.

- **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.

Procedure

1. Click Remote Support in the navigation tree, and then click the Data Collections tab.
2. Click Send Data Collection.
3. When prompted to confirm the request, click Yes, send.

   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) View the data collection status in the Insight RS Console.

More information

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

Sending Active Health System reporting information

Prerequisites

Configure iLO Settings privilege

About this task

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 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.

Procedure

1. Click Remote Support in the navigation tree, and then click the Data Collections tab.
2. Click Send Active Health System Report.
3. When prompted to confirm the request, click Yes, send.

   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) View the Active Health Service Collection status in the Insight RS Console.

More information

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

Viewing data collection status in iLO

Procedure

Click Remote Support in the navigation tree, and then click the Data Collections tab.

Subtopics

Data Collection details

Data Collection details

- Last Data Collection Transmission—The date and time of the last data collection.
- Last Data Collection Transmission Status—The status of the last data transmission.

Viewing Active Health System reporting status in iLO

Procedure

Click Remote Support in the navigation tree, and then click the Data Collections tab.

Subtopics

Active Health System reporting details

Active Health System reporting details

- Last Active Health System Reporting Transmission —The date and time of the last Active Health System report.
- Last Active Health System Reporting Transmission Status —The status of the last data transmission.

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.

Changing the remote support configuration of a supported device

Subtopics

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

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.

More information

Registering for Insight Remote Support central connect

Using the iLO administration features

Subtopics

iLO user accounts

iLO directory groups

Boot Order

Installing a license key

Using remote key managers with iLO

Language packs

Firmware verification

Using Smart Update Manager to create a custom ISO on Windows

iLO user accounts

HPE ProLiant RL3xx Gen 11 platforms do not support RIBCL.

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.

If a supported application that works with iLO requires a service account, you can add a user account and designate it as a service account. You can also add service accounts by using a supported application or the iLO RESTful API.

To support more than 12 users, configure iLO to use a directory service to authenticate and authorize its users.

Subtopics

Adding local user accounts

Editing local user accounts

Enabling a user account

Disabling a user account

Deleting a user account

iLO user account options

iLO user account privileges

iLO user account roles

Password guidelines

IPMI/DCMI users

Viewing user accounts

More information

Directory authentication and authorization settings in iLO

Adding local user accounts

Prerequisites

Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.

   The User Administration tab is displayed.

2. Click New.

3. Enter the following details:

   - Login Name
   - User Name
   - New Password and Confirm Password

4. (Optional) To select a predefined set of user privileges, select a role in the Role menu.

   If you want to manually select privileges, use the default role (Custom).

5. If you selected Custom in step 4, select from the following privileges:

   - Login
   - Remote Console
   - Virtual Power and Reset
   - Virtual Media
   - Host BIOS
   - Configure iLO Settings
   - Administer User Accounts
   - Host NIC
   - Host Storage
   - Recovery Set

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

6. (Optional) If the account will be used as a service account for a supported application, select the Service Account check box.

   Examples of supported application are iLO Amplifier Pack.

   You can configure the service account property only during the initial user account creation. You cannot edit this setting for existing user accounts.

7. To save the new user, click Add User.

   iLO notifies you that the account was added.

More information

iLO user account options

iLO user account privileges
Password guidelines

Editing local user accounts

Prerequisites

Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.

   The User Administration tab is displayed.
2. Select a user account, and then click Edit.
3. Update the following values, as needed:
   - Login Name
   - User Name
4. To change the password, click the Change password check box, and then update the New Password and Confirm Password values.
5. (Optional) If you want to change the user account privileges, do one of the following:
   - To manually select privileges, select Custom from the Role menu, and then select privileges from the list.

     To select all available user privileges, click the select all check box.
   - To select a predefined set of user privileges, select Administrator, Operator, or ReadOnly from the Role menu.
6. To save the user account changes, click Update User.

   iLO notifies you that the selected account was updated.

More information

iLO user account options
iLO user account privileges
Password guidelines

Enabling a user account

Prerequisites

Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.

   The User Administration tab is displayed.
2. Select the check box next to a user account that you want to enable.
3. Click Enable.

   iLO notifies you that the selected account is enabled.

Disabling a user account

Prerequisites

Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.

   The User Administration tab is displayed.
2. Select the check box next to a user account that you want to disable.
3. Click Disable.
4. When prompted to confirm the request, click Yes, disable.

   iLO notifies you that the selected account is disabled.

Deleting a user account

Prerequisites

Administer User Accounts privilege

Procedure

1. Click Administration in the navigation tree.

   The User Administration tab is displayed.
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 Yes, delete.

   iLO notifies you that the selected accounts were deleted.

iLO user account options

- 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 Session List page, in the menu that is displayed when you click the user icon, 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.
- 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.
- New Password and Confirm Password set and confirm the password that is used for logging in to iLO.
- Role allows you to select a predefined set of user privileges when you add or edit a user account. You can use the custom option to define a customized privilege set.
- Service Account designates the account as a service account. Service accounts are used by supported products that work with iLO.

  Examples of supported applications include iLO Amplifier Pack and Onboard Administrator.

  You can configure the service account property only during the initial user account creation. You cannot edit this setting for existing

user accounts.

iLO user account privileges

The following privileges apply to user accounts:

- Login— Enables a user to log in to iLO.
- Remote Console—Enables a user to access the host system remote console, including video, keyboard, and mouse control.

  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network tasks.
- 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.
- Virtual Media—Enables a user to use the virtual media feature on the host system.
- Host BIOS—Allows configuration of the host BIOS settings by using the UEFI System Utilities. This privilege is required for replacing the active system ROM with the redundant system ROM.

  This privilege does not affect configuration through host-based utilities.
- 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 from the following interfaces:

  - iLO web interface
  - iLO RESTful API
  - CLI
  - HPQLOCFG

  Users who have access to the following interfaces can still reconfigure iLO:

  - UEFI System Utilities
  - HPONCFG

  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 are not assigned this privilege, you can view your own settings and change your own password.
- Host NIC—Enables a user to configure the host NIC settings.

  This privilege does not affect configuration through host-based utilities.
- Host Storage—Enables a user to configure the host storage settings.

  This privilege does not affect configuration through host-based utilities.
- Recovery Set—Enables a user to manage the Recovery Set.

  By default, the Recovery Set privilege is assigned to the default Administrator account. This privilege can be added to a user account only by creating or editing the account with an account that already has this privilege.

  If there is no user account with the Recovery Set privilege, and an account with this privilege is required, reset the management processor to the factory default settings. The factory default reset creates a default Administrator account with the Recovery Set privilege.

  This privilege is not available when iLO security is disabled with the system maintenance switch.

The following privileges are not available through the CLI or RIBCL scripts:

- Host NIC
- Host Storage
- Recovery Set
- Host BIOS
- Login

The following privileges are not available through the iLO 6 Configuration Utility in the UEFI System Utilities:

- Recovery Set
- Login

iLO user account roles

Administrator

Enables all privileges except Recovery Set.

Operator

Enables all privileges except Configure iLO Settings, Administer User Accounts, and Recovery Set.

ReadOnly

Enables only the Login privilege.

Custom (default)

Allows the user to define a custom privilege set.

Password guidelines

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

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

If you enable the Password complexity setting on the Access Settings page, iLO enforces these password characteristics when you create or edit a user account.

- The minimum length for a user account password is set on the Access Settings page. Depending on the configured Minimum Password Length value, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. Hewlett Packard Enterprise recommends using a Minimum Password Length of eight or more characters. The default value is eight characters.

  IMPORTANT:

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

More information

Configuring iLO access settings
Security guidelines

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.

Viewing user accounts

Procedure

1. Click Administration in the navigation tree.

   The User Administration page is displayed.

   The Local Users table shows the login names, user names, status, and assigned privileges of each local user.

   Assigned privileges are displayed with a check mark icon and unassigned privileges are displayed with an X icon.

   If service accounts are configured, the Service table shows the login names, user names, status, and assigned privileges of each service account. If no service accounts exist, this table is not displayed.

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

More information

iLO user account options
iLO user account privileges

iLO directory groups

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

More information

Kerberos authentication with iLO
Schema-free directory authentication

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: https://www.hpe.com/support/ilo-docs.

Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.
2. Click New.
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:
   - Login
   - Remote Console
   - Virtual Power and Reset
   - Virtual Media
   - Host BIOS
   - Configure iLO Settings
   - Administer User Accounts
   - Host NIC
   - Host Storage
   - Recovery Set
5. To save the new directory group, click Add Group.

More information

Directory group options
Directory group privileges
Active Directory nested groups (schema-free configuration only)

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.
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:
   - Login
   - Remote Console
   - Virtual Power and Reset
   - Virtual Media
   - Host BIOS
   - Configure iLO Settings
   - Administer User Accounts
   - Host NIC
   - Host Storage
   - Recovery Set
5. To save the directory group changes, click Update Group.

More information

Directory group options
Directory group privileges
Active Directory nested groups (schema-free configuration only)

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.
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 Yes, delete.

   iLO notifies you that the group was deleted.

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.

Nested groups are not supported when you use CAC Smartcard authentication.

Directory group privileges

- Login—Enables directory users to log in to iLO.
- Remote Console—Enables directory users to access the host system remote console, including video, keyboard, and mouse control.

  Users with this privilege can access the BIOS, and therefore might be able to perform host-based BIOS, iLO, storage, and network configuration tasks.

- Virtual Power and Reset—Enables directory users 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.
- Virtual Media—Enables directory users to use the virtual media feature on the host system.
- Host BIOS—Enables directory users to configure the host BIOS settings by using the UEFI System Utilities.

  This privilege does not affect configuration through host-based utilities.

- Configure iLO Settings—Enables directory users 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 iLO web interface, iLO RESTful API, HPQLOCFG, or the CLI. Users who have access to 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 directory users to add, edit, and delete local iLO user accounts.
- Host NIC—Enables directory users to configure the host NIC settings.

  This privilege does not affect configuration through host-based utilities.

- Host Storage—Enables directory users to configure the host storage settings.

  This privilege does not affect configuration through host-based utilities.

- Recovery Set—Enables directory users to manage the System Recovery Set.

  By default, this privilege is assigned to the default Administrator account. To assign this privilege to another account, log in with an account that already has this privilege.

This privilege is not available if you start a session when the system maintenance switch is set to disable iLO security.

Viewing directory groups

Procedure

1. Click Administration in the navigation tree, and then click the Directory Groups tab.

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

   Assigned privileges are displayed with a check mark icon and unassigned privileges are displayed with an X icon.

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

More information

Directory group options
Directory group privileges

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.

From Gen11 onwards, only UEFI boot mode is supported.

Subtopics

Configuring the server boot mode

Configuring the server boot order

Changing the one-time boot status

Booting to the ROM-based utility on the next reset

Configuring the server boot mode

Prerequisites

- Configure iLO Settings privilege

About this task

Use the Boot Mode setting to define how the server looks for OS boot firmware. Select UEFI mode.

Procedure

1. Click Administration in the navigation tree, and then click the Boot Order tab.
2. Select Unified Extensible Firmware Interface (UEFI) 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. Reset the server.

Configuring the server boot order

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Administration in the navigation tree, and then click the Boot Order tab.

   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 UEFI mode, select an option from the list of available boot devices.

   > **NOTE:**
   > Floppy drives are supported iLO virtual media devices, but they are not supported as bootable devices.

3. Click Apply.

   iLO confirms that the boot order was updated successfully.

Changing the one-time boot status

About this task

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.

Subtopics

Changing the one-time boot status in UEFI mode

Changing the one-time boot status in UEFI mode

Prerequisites

- Configure iLO Settings privilege
- The server was rebooted after an iLO firmware or system ROM update.
- The server was rebooted after being configured to use the UEFI boot mode.

Procedure

1. Click Administration in the navigation tree, and then click the Boot Order tab.
2. Select an option from the Select One-Time Boot Option list.
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, if you have a hard drive with two bootable partitions, you can select the 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.

Subtopics

UEFI mode one-time boot options

UEFI mode one-time boot options

The following UEFI mode one-time boot options are supported.

NOTE:
Floppy drives are supported iLO virtual media devices, but they are not supported as bootable devices.

- No One-Time Boot
- CD/DVD Drive
- USB Storage Device
- Hard Disk Drive
- Network Device—The BIOS scans for enabled network devices. The server attempts to boot to the detected devices, one at a time, until successful.
- Intelligent Provisioning
- HTTP Boot—The server boots to an HTTP URI if a URI to a bootable image is defined in the ROM-based system utility.

  This option is supported in configurations that use a DHCP server to configure the network settings.
- 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—The server boots to an embedded shell environment that is separate from the UEFI System Utilities.
- Embedded iPXE—The server boots to the embedded iPXE application.

  The embedded iPXE is an open-source network boot application embedded in the system BIOS. You can use this option to perform a network boot.

Booting to the ROM-based utility on the next reset

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Administration in the navigation tree, and then click the Boot Order tab.
2. To load the ROM-based setup utility on the next server reset, click Boot to System Setup Utilities.

Installing a license key

Prerequisites

- Configure iLO Settings privilege

- Your iLO license is supported on the server on which you want to install it.

  For more information, see the HPE iLO Licensing Guide.

Procedure

1. Click Administration in the navigation tree, and then click the Licensing tab.
2. Enter a 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.

   If you install a license key on a server that already has a key installed, the new key replaces the installed key.

   After you install a license key, only the last five digits are displayed in iLO. Hewlett Packard Enterprise recommends recording and saving your license key information in case it is needed later.
3. Click Install.

   iLO prompts you to confirm that you have read and accept the EULA.

   The EULA details are available in the License Pack option kit.
4. Click I agree.

   The license key is now enabled.

Subtopics

Viewing license information

iLO licensing

Viewing license information

Procedure

Click Administration in the navigation tree, and then click the Licensing tab.

Subtopics

License details

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 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 features such as the graphical remote console with multiuser collaboration, video record and playback, and many more features.

- An iLO license is required for each server on which the product is installed and used.
- Licenses are not transferable.
- The iLO Advanced license is automatically included with Synergy compute modules.
- The iLO Advanced license is automatically included with ProLiant e910 server blades shipped after June 1, 2020.
- If you lose a license key, follow the lost license key instructions in the HPE iLO Licensing Guide.
- See the HPE iLO Licensing Guide at **https://www.hpe.com/support/ilo-docs** for information about:
  - Obtaining a free iLO trial license.
  - Purchasing, registering, and redeeming a license key.

Benefits of registering iLO license keys

Registering your license is an important step. Benefits include:

- Accessing the Hewlett Packard Enterprise Support Center (**https://www.hpe.com/support/hpesc**).
- Accessing software updates through the My HPE Software Center website (**https://www.hpe.com/downloads/software**).
- Tracking of all your Hewlett Packard Enterprise product licenses in one convenient place through the My HPE Software Center website (**https://www.hpe.com/software/hpesoftwarecenter**).
- Receiving important product alerts.
- Activating your unique Hewlett Packard Enterprise Support Agreement ID (SAID).

  Your SAID identifies you and tracks your products so that Hewlett Packard Enterprise can provide fast, personalized support.

> **NOTE:**
>
> At this time, the My HPE Software Center portal does not track SAID agreements.

Using remote key managers with iLO

iLO 6 supports remote key managers, which can be used in conjunction with HPE Storage Controllers.

A remote 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 remote key manager and the other products. iLO uses a unique user account based on its own MAC address for communicating with the remote key manager. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the remote key manager with administrator privileges. For more information about the deployment user account, see the remote key manager documentation.

Subtopics

Viewing key manager events

Clearing the key manager log

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 the FIPS security state is enabled.

  HPE ProLiant RL3xx platforms do not support ESKM.

  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

NOTE:

Using a key manager is not supported when iLO is configured to use the CNSA security state.

Configuring remote key management

Procedure

1. Install and configure the key management software on the key server.
   a. Create a local user.
   b. Create local groups.
   c. Create a master key.

   For more information, see the supported key manager software documentation.
2. Configure iLO to support remote key management.
   a. Configure key manager servers.
   b. Add key manager configuration details.
   c. (Optional) Test the key manager configuration.
3. Configure supported devices to operate in remote key management mode.
   - For NVMe drives, see the UEFI System Utilities user guide.
   - For MRXXX Storage Controllers, see HPE MegaRAID MR Controller User Guide.

   These documents are available at the following website: **https://www.hpe.com/support/hpesc**.
4. (Optional) For SRXXX Storage Controllers only: Verify that the Encryption Status is listed as Encrypted on the iLO Storage Information

page.

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: **https://www.hpe.com/support/ilo-docs**.
- iLO is not configured to use the CNSA security state.

Procedure

1. Click Administration in the navigation tree, and then click the Key Manager tab.
2. Click  in the Key Manager Servers section.

   The Edit Key Manager Server Settings page opens.
3. Enter the following information:
   - Primary Key Server Address
   - Primary Key Server Port
   - Secondary Key Server Address
   - Secondary Key Server Port
4. (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.
5. Click OK.

   For more information about Thales CipherTrust Manager 2.2.0, see **Remote Key Manager Support for Cipher Trust Manager** Configuration guide.

Subtopics

Key manager server options

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: **https://www.hpe.com/support/ilo-docs**.
- iLO is not configured to use the CNSA security state.
- At least one key manager server is configured.

Procedure

1. Click Administration in the navigation tree, and then click the Key Manager tab.
2. Click  in the Key Manager Configuration section.

   The Edit Key Manager Configuration Settings page opens.
3. Enter the following information in the iLO Account on Key Manager section:
   - Account Group
   - (Optional) Key Manager Local CA Certificate Name

   The Account Name value is read-only.
4. Enter the following information in the Key Manager Administrator Account section:
   - Login Name
   - Password
5. Click OK.

   iLO sends an information request to the key manager server.
   - If the ilo-<iLO MAC address> account name does not exist:
     - The user account you entered in the Key Manager Administrator Account section creates the account name and associates it with the key manager local user and its generated password.
     - The account name is added to the account group you entered in step 3.
   - If the ilo-<iLO MAC address> account name exists:
     - The user account you entered in the Key Manager Administrator Account section associates the account name with the key manager local user, and a new password is generated.
     - If the user account you entered in the Key Manager Administrator Account section is not a member of the account group associated with the ilo-<iLO MAC address> account, it is added to the account group.
     - If the ilo-<iLO MAC address> is already a member of a key manager local group, the group you entered in step 3 is ignored. The existing group assignment on the key manager is used, and it is displayed in the iLO web interface. If a new group assignment is needed, you must 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.

Subtopics

Key manager configuration details

Account 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.

Account 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

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: **https://www.hpe.com/support/ilo-docs**.
- A key manager is set up and the key manager configuration is complete in iLO.

About this task

To verify the configured settings, test the key manager configuration. The following tests are attempted:

- Confirm that the key manager software version is compatible with iLO.
- Connect to the primary key manager server (and secondary key manager server, if configured) by using TLS.
- Authenticate to the key manager by using the configured credentials and account.

Procedure

1. Click Administration in the navigation tree, and then click the Key Manager tab.
2. Click  .

The test results are displayed in the Key Manager Events table. A success or failure message is displayed at the top of the iLO web

interface window.

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Administration in the navigation tree, and then click the Key Manager tab.
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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Administration in the navigation tree, and then click the Key Manager tab.
2. Click Clear Key Manager Log.

   iLO prompts you to confirm the request.
3. Click Yes, clear.

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.
- You can install multiple language packs.

  If a language pack is installed, installing a newer language pack of the same language replaces the installed language pack.
- The integrated remote console uses the language of the current iLO session.
- 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.

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. If there is no cookie, and the browser or OS language is not supported, iLO uses the configured default language.

Installing language packs with the flash firmware feature

Prerequisites

Configure iLO Settings privilege

Procedure

1. Download a language pack from the following website: **https://www.hpe.com/support/ilo6**.
2. Extract the language pack `LPK` 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:
     - `#rpm2cpio <language_pack_file_name>.rpm | cpio -id`

   The language pack file name is similar to the following: `lang_<language>_<version>.lpk`.
3. Click Firmware & OS Software in the navigation tree, and then click Update Firmware.

   The Flash Firmware controls appear.
4. Depending on the browser you use, click Browse or Choose File.
5. Select the `lang_<language>_<version>.lpk` file, and then click Open.
6. (Optional) To save a copy of the language pack file to the iLO Repository, select the Also store in iLO Repository check box.
7. Click Flash.

   iLO prompts you to confirm the installation request.
8. Click OK.

   iLO installs the language pack, initiates a reset, and closes your browser connection.

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

More information

Viewing and managing firmware and software

Selecting a language pack

About this task

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 icon at the top of any iLO web interface page, and then select a language.
- Click Administration in the navigation tree, and then click the Language tab. Click a language in the Installed Languages list.

Configuring the default language settings

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.

About this task

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

Procedure

1. Click Administration in the navigation tree, and then click the Language tab.
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.

More information

Installing language packs with the flash firmware feature

Configuring the current iLO web interface session language

Prerequisites

The language pack for the language you want to use is installed.

Procedure

1. Click Administration in the navigation tree, and then click the Language tab.
2. Click the name of a language in the Installed Languages list.

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

More information

Installing language packs with the flash firmware feature

Uninstalling a language pack

Prerequisites

- Configure iLO Settings privilege
- The language you want to remove is not configured as the default language.
- The language you want to remove was installed as a language pack. You cannot remove the English language.

Procedure

1. Click Administration in the navigation tree, and then click the Language tab.
2. Click  next to the language you want to remove.
3. When prompted to confirm the request, click Yes, remove.

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

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

Firmware verification

The Firmware Verification feature allows you to run an on-demand scan or implement scheduled scans.

To respond to detected issues, you can configure iLO to:

- Log the results.
- Log the results and initiate a repair action that uses a recovery install set.

Depending on the scan results, information is logged in the Active Health System Log and the Integrated Management Log.

The following firmware types are supported:

- iLO Firmware
- System ROM (BIOS)
- System Programmable Logic Device (CPLD)
- Server Platform Services (SPS) Firmware (supported servers only)
- Server Platform Services Full Recovery Image (supported servers only)

When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository.

If an invalid iLO or System ROM (BIOS) firmware file is detected, the invalid file is saved to a quarantine area in the iLO Repository. You can download the invalid file to investigate its type and origin. Quarantined images are not displayed on the iLO Repository page, and you cannot select them when you use the Flash Firmware feature.

If a corrupted Server Platform Services (SPS) Descriptor is detected, the corrupted firmware image is moved to the quarantine area in the iLO Repository. If the Server Platform Services Full Recovery Image is available in the System Recovery Set, and Log and Repair Automatically is selected on the Firmware Verification page, recovery occurs automatically. When recovery occurs, an event is logged in the IML and the Security Log. Automatic recovery of corrupted SPS Descriptor requires an iLO Advanced License.

If a supported management tool is configured to listen for system recovery events, you can send a recovery event from this page.

Configuring the firmware verification settings

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. Click the Scan Settings icon .
3. Set Enable Background Scan to enabled or disabled status.
4. Select an Integrity Failure Action.
5. Set the Scan Interval in days.

   Valid values are from 1 to 365 days.
6. Click Submit.

   HPE ProLiant RL3xx Gen 11 platforms do not support On demand scan.

Firmware Verification scan options

On Demand scan option is available only in supported platforms.

- Enable Background Scan—Enables or disables Firmware Verification scanning. When enabled, iLO scans the supported installed firmware for file corruption.
- Integrity Failure Action—Determines the action iLO takes when a problem is found during a Firmware Verification scan.
  - To log the results, select Log Only.
  - To log the results and initiate a repair action, select Log and Repair Automatically.

    If a problem is detected for a supported firmware type, iLO checks for the affected firmware type in a protected install set. By default, this set is the Recovery Set. If a firmware image is available, iLO flashes that firmware image to complete the repair.
- Scan Interval (in days)—Sets the background scan frequency in days. Valid values are from 1 to 365.

More information

System Recovery Set

Running a firmware verification scan

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. Click Run Scan.

   When a firmware verification scan is in progress, you cannot install firmware updates or upload firmware to the iLO Repository.

   The scan results are displayed at the top of the page.

   If a failure occurred, the firmware state on the Firmware Verification page changes to Failed/Offline, the System Health status changes to Critical, and an event is recorded in the IML. If the firmware verification scan feature is configured to Log and Repair Automatically, the failed firmware is flashed. If successful, the firmware state and System Health status are updated, and the IML event changes to Repaired status.

   If automatic repair is not configured, you must complete the repair manually.

Viewing firmware health status

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

Navigate to the Administration page, and then click the Firmware Verification tab.

Firmware health status details

The following information is displayed for each supported firmware type.

Firmware Name

The name of the installed firmware.

Firmware Version

The firmware version.

Health

The firmware health status.

State

The firmware status. The possible values follow:

- Enabled—The firmware is verified and enabled.
- Scanning—A firmware verification scan is in progress or is about to start.
- Flashing—A firmware update is in progress.
- Failed/Offline—The firmware could not be verified and was not repaired.

Recovery Set Version

The version of the firmware in the System Recovery Set.

If this firmware type is not in the System Recovery Set, or there is no System Recovery set, Not present is displayed.

Viewing quarantined firmware

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

Navigate to the Administration page, and then click the Firmware Verification tab.

Quarantined firmware files are listed in the Quarantine section.

If there are no quarantined files, the message `There are no items under quarantine` is displayed.

Quarantined firmware details

The Quarantine section displays the following information about invalid firmware files.

Name

The name of the invalid firmware file.

Created

The invalid file creation date.

Size

The invalid file size.

Individual quarantined file details

When you click a file in the list, the following details are displayed:

- Name—The name of quarantined file.
- Created—The invalid file creation date.
- File Name—The name used by the iLO Repository.
- Image URI—The quarantined file location.
- Size—The invalid file size.
- Device Class—An ID that can be used to correlate between iLO Repository resources and firmware inventory data.

Downloading quarantined firmware

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: **https://www.hpe.com/support/ilo-docs**.

About this task

If a file is saved to the quarantine area in the iLO Repository, you can download the file for offline analysis.

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. In the Quarantine section, click next to the file you want to download.

   A status message displays the download progress.
3. Follow the browser instructions to save or open the file.

Deleting quarantined firmware

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: **https://www.hpe.com/support/ilo-docs**.
- Recovery Set privilege

Procedure

1. Navigate to the Administration page, and then click the Firmware Verification tab.
2. In the Quarantine section, click next to the file you want to delete.

   iLO prompts you to confirm the request.
3. Click Yes, remove.

Initiating a full system recovery

Prerequisites

- Configure iLO Settings privilege
- 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: **https://www.hpe.com/support/ilo-docs**.
- A System Recovery Set exists in the iLO Repository.
- A supported management tool (such as iLO Amplifier Pack 1.15 or later) is configured to manage the server.

About this task

You can use iLO to generate a recovery event that triggers a separate management tool to initiate a full system recovery. Recovery involves installation of the System Recovery Set followed by reimaging the server operating system.

> **CAUTION:**
> Reimaging a server might cause the loss of existing data.

Procedure

1. Shut down the server if the recovery process includes components that require the server to be shut down.
2. Navigate to the Administration page, and then click the Firmware Verification tab.
3. Click Send Recovery Event.
4. In the Send Recovery Event pane, select the Yes, generate a recovery event check box, and then click Send Recovery Event.

The recovery event is sent to the management tool that is configured to listen for recovery events.

If the event was sent successfully, the following informational event is logged in the IML:

```
Firmware recovery is requested by Administrator.
```

More information

System Recovery Set

Using Smart Update Manager to create a custom ISO on Windows

About this task

NOTE: 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**.

Smart Update Manager (SUM) does not support HPE ProLiant RL3xx Gen 11 platforms.

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 the iLO security features

Subtopics

Security guidelines

Key security features

Ports used by iLO features

Secure Protocol and Data Model

Server identity

One-button secure erase for DevIDs and System IAK

System board replacement

802.1X and iLO

iLO access settings

iLO Service Port

Managing SSH keys

CAC Smartcard Authentication

Administering SSL certificates

Directory authentication and authorization settings in iLO

iLO security states

iLO encryption settings

HPE SSO

Configuring the Login Security Banner

System maintenance switch

Security guidelines

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

- Set up iLO on a dedicated management network.

  Hewlett Packard Enterprise recommends establishing a private management network that is separate from your data network. Configure the management network so that it can be accessed only by administrators.

  If you connect iLO devices to a shared network, consider the iLO devices as separate servers and include them in security and network audits.

- Do not connect iLO directly to the Internet.

  The iLO processor is a management and administration tool, not an Internet gateway. Connect to the Internet by using a corporate VPN that provides firewall protection.

  IMPORTANT:

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

- Replace the default self-signed certificate by installing an SSL certificate that is signed by a Certificate Authority (CA).

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

- Install trusted CA certificates to enable certificate validation for external services such as LDAP.

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

  Change the iLO management passwords according to the same guidelines as the server administrative passwords.

  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 user 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.

  This feature allows authentication and authorization using the same login process throughout the network. It provides a way to control multiple iLO devices simultaneously. Directories provide role-based access to iLO with specific roles and privileges based on time and location.

- Implement two-factor authentication.

  This feature provides additional security, especially when you make connections remotely or outside the local network.

- Protect SNMP traffic.

  Reset the community strings according to the same guidelines as the administrative passwords. Also set firewalls or routers to accept only specific source and destination addresses. Disable SNMP at the server if you do not need it.

- Disable ports and protocols that you do not use (for example, SNMP or IPMI/DCMI over LAN).

  You can perform this task on the Access Settings page.

- Use HTTPS for the .NET remote console.

  To configure this option, 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 & Media page Security tab respectively.

- Disable features that you do not use (for example, remote console).

  You can perform this task on the Access Settings page.

- Configure the remote console to automatically lock the server OS console.

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

- Configure a higher security state on the Encryption Settings page.

- Disable the iLO 6 Configuration Utility in the UEFI System Utilities or configure iLO to require login credentials when users access it.

  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.

- Enable firmware verification scans.

  You can perform this task on the Firmware Verification page.

- Use the Security Dashboard page to monitor security risks and recommendations.

- Use the Security Log to monitor security-related events.

- Enable the Require Host Authentication feature.

  You can perform this task on the Access Settings page.

- Set the Downgrade Policy to Downgrade requires Recovery Set privilege.

  You can perform this task on the Access Settings page.

- Keep the Recovery Set up to date.

- 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 & Media 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.

For more information, see:

- Top 10 security settings for HPE iLO 6.
- Recommended Security Settings in HPE iLO 6.
- The HPE Gen11 and Later Security Reference Guide at the following website: https://www.hpe.com/support/ilo-docs.

Key security features

Configure iLO security features on the following web interface pages.

Access Settings

- Enable or disable iLO interfaces and features.
- Customize the TCP/IP ports iLO uses.
- Configure authentication failure logging and delays.
- Secure the iLO 6 Configuration Utility.

iLO Service Port

Configure iLO Service Port availability, authentication, and supported devices.

Secure Shell Key

To provide stronger security, add SSH keys to iLO user accounts.

Certificate Mappings and CAC Smartcard

Configure CAC Smartcard authentication and configure smartcard certificates for local users.

SSL Certificate

Install X.509 CA signed certificates to enable encrypted communications.

Directory

Configure Kerberos authentication and Directory integration.

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

Encryption

Implement a higher security environment by changing the iLO security state from the default value (Production) to a stronger setting.

HPE SSO

Configure supported tools for single-sign-on with iLO.

Login Security Banner

Add a security notice that is displayed when you:

- Navigate to the iLO web interface login page.
- Start the HTML5 standalone remote console.
- Connect to iLO through an SSH connection.

Ports used by iLO features

Network settings and ports

The values listed in Table: Network settings and ports configurable through iLO can be configured to comply with site requirements or security initiatives. These settings can be configured on the iLO Access Settings page.

Table 1. Network settings and ports configurable through iLO

Description	Default Setting or Port	Protocol type
IPMI/DCMI over LAN port	623	UDP
IPMI/DCMI over LAN Specifies whether to allow IPMI/DCMI communications over the LAN with iLO.	Disabled	
IPMI over KCS	Enabled	
Remote Console Port	17990	TCP
Remote Console Allows you to enable or disable access through the iLO remote consoles.	Enabled	
Secure Shell (SSH) Port	22	TCP
Secure Shell (SSH) Allows you to enable or disable the SSH feature. SSH provides encrypted access to the iLO command-line protocol (CLP).	Enabled	
SNMP Port	161	UDP
SNMP Trap Port	162 for SNMP alerts (outgoing only).	UDP
SNMP Specifies whether iLO responds to external SNMP requests.	Enabled	
Virtual Media Port	17988	TCP
Virtual Media Enables you to specify whether virtual media is enabled or disabled.	Enabled	
Web Server Non-SSL Port (HTTP)	80	TCP
Web Server SSL Port (HTTPS)	443	TCP
Web Server [1] Allows you to enable or disable access through the iLO web server.	Enabled	

[1] Supports the iLO web interface, remote console, iLO RESTful API, iLO Federation, firmware updates, and RIBCL.

Other outgoing ports

Security administrators might need to know the ports listed in Table: Other ports used by iLO. These ports are for outgoing third-party services.

Table 2. Other ports used by iLO

Description	Default port	Protocol type	Location in iLO web interface
DNS Resolution	53	UDP	N/A
SSDP Multicast	1900	UDP	N/A
DHCPv4	67, 68	UDP	N/A
DHCPv6	547	UDP	N/A
NTP	123	UDP	N/A
NetBIOS Name Service/WINS	137	UDP	iLO Dedicated Network Port > IPv4 iLO Shared Network Port > IPv4
Kerberos KDC Server Port	88	TCP, UDP	Security > Directory
Directory Server LDAP SSL Port	636	TCP	Security > Directory
AlertMail SMTP Port	25	TCP	Management > Mail
Remote Syslog Port	514	UDP	Management > Remote Syslog
Key Manager Port	9000	TCP	Administration > Key Manager
Remote Support Port	7906	TCP	Remote Support > Registration

Ports not supported by iLO

iLO does not support the commonly used ports listed in Table: Unsupported ports.

Table 3. Unsupported ports

Description	Port	Protocol type	Notes
LDAP-unsecured • Connection (TCP) • Connectionless (UDP)	389	TCP/UDP	iLO uses secure port 636 for outgoing LDAP connections.
Global Catalog LDAP-unsecured • Connection (TCP) • Connectionless (UDP)	3268	TCP/UDP	iLO uses secure LDAP connections.

Secure Protocol and Data Model

iLO uses the Secure Protocol and Data Model (SPDM) to verify the integrity of components and authenticate the Option Cards. All the components do not support SPDM. If SPDM is enabled, an unsupported or non-authentic component will change the iLO security status to Risk.

iLO supports SPDM v1.0 and v1.0.1. For devices not supporting any of the SPDM versions, iLO logs Security log events for SPDM failures.

You can check the status of each component authentication in the Security Log.

HPE ProLiant RL3xx Gen 11 platforms do not support SPDM.

Subtopics

Global component integrity

Component integrity policy

More information

Device status values
SPDM supported algorithms

Global component integrity

Global component integrity option allows iLO to authenticate the components in the server using SPDM. When the option is enabled, iLO will verify and authenticate all the applicable components in the server using SPDM.

The option is Disabled by default. When disabled, iLO does not validate the components for SPDM authentication and even the SPDM supported cards are reported as Not Supported.

You can enable this option on the Access Settings page.

Subtopics

Enabling Global Component Integrity

Enabling Global Component Integrity

Prerequisites

- Option Cards supporting SPDM
- CA of the Option Cards is available in the iLO Firmware

Procedure

1. Navigate to Access settings page.
2. Click  on the iLO settings.
3. Select Global Component Integrity check box to enable the option.

Component integrity policy

Component integrity policy controls the system boot policy based on the SPDM authentication results of the devices in the server.

Subtopics

Supported policies

Supported policies

The two supported policies are:

- Halt Boot On SPDM Failure —Select the option to halt the system boot during SPDM Authentication failure.

- No Policy—Select the option to boot the system in normal mode.

To set the desired Component Integrity Policy settings, navigate to Access settings page, click  on the iLO settings.

Server identity

Server Identity (DevID) is a standard (based on IEEE 802.1AR) way to uniquely identify a server across networks. DevID is uniquely bound to a server that enables a server to prove its identity in various industry standards and protocols that authenticate, provision, and authorize communicating devices.

iLO supports factory provisioned server identity (iLO IDevID) and user defined server identity (iLO LDevID). iLO also stores the system certificates (System IDevID and System IAK).

Following are the different server management identities:

- iLO IDevID
- iLO LDevID
- System IDevID certificate

Subtopics

iLO IDevID

iLO LDevID

System IDevID certificate

System IAK certificate

Platform certificate

iLO IDevID

iLO can be provisioned with server identity in the factory. This factory provisioned server identity is called iLO IDevID. HPE servers can be securely on boarded into a customer network using the IDevID for 802.1X authentication. iLO IDevID has life time validity and is immutable.

Subtopics

iLO IDevID features

iLO IDevID features

iLO does not allow you to update or delete IDevID since it is immutable.

You can view the iLO IDevID certificate using the RESTFul API GET command:

```
"/redfish/v1/Managers/1/SecurityService/iLOIDevID/Certificates/1"
```

iLO LDevID

IDevID can be supplemented by a user-defined server identity, called iLO LDevID. iLO LDevID is unique in the administrative domain, in

which the server is used. HPE servers can be securely on boarded into a customer network using the LDevID for 802.1X authentication. Hewlett Packard Enterprise recommends using LDevID always to assure the privacy of iLO IDevID.

LDevID helps in facilitating the enrollment (authentication and authorization of credentials) by local network administrators. iLO allows to import, view, and delete LDevID outside the factory.

Subtopics

Importing LDevID certificate

About this task

Procedure

1. Generate a Certificate Signing Request (CSR) for LDevID. iLO allows creation of a CSR in PEM format for LDevID using the RESTful API POST command:

   `"/redfish/v1/CertificateService/Actions/CertificateService.GenerateCSR"`

   ```
   {
       "Action": "CertificateService.GenerateCSR",
       "CertificateCollection": {
           "@odata.id": "/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/"
       }
   }
   ```

2. Send this CSR to Certificate Authority to obtain a trusted certificate.

3. Import the trusted LDevID certificate into iLO. iLO allows import of LDevID certificate in PEM format using the RESTful API POST command:

   `"/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/"`

   ```
   {
       "CertificateType": "PEM",
       "CertificateString": <Contents of the trusted certificate>
   }
   ```

   Before importing, iLO validates the input certificate with the following parameters:
   - The public key in the certificate matches the one generated with its corresponding CSR.
   - The signing and hashing algorithms used in the certificate are FIPS compliant.

   NOTE: iLO supports import of LDevID certificates upto 16 KB size.

Viewing the imported LDevID certificate

To view the imported LDevID certificate, use the following RESTful API GET command:

`"/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/1"`

Deleting the imported LDevID certificate

To delete the imported LDevID certificate, use the following RESTful API DELETE command:

```
"/redfish/v1/Managers/1/SecurityService/iLOLDevID/Certificates/1"
```

Replacing LDevID certificate

You cannot update a LDevID certificate. To replace a certificate, you must delete the existing LDevID certificate and generate a new certificate. See Importing LDevID certificate.

NOTE: In case LDevID certificate is lost due to one-button secure erase, you can restore it using the Backup and Restore feature or replace it.

System IDevID certificate

iLO can be provisioned with the server host identity, available for use by the operating system. This factory provisioned system identity is called System IDevID, whose corresponding private key is stored in TPM. System IDevID follows the TCG proposal for TPM2.0 implementation of an IDevID.

iLO does not allow you to update or delete the certificate. You can only view the certificate using the RESTful API GET command:

```
"/redfish/v1/Managers/1/SecurityService/SystemIDevID/Certificates/1"
```

System IAK certificate

iLO can be provisioned with the System Initial Attestation Key (IAK) certificate in the factory. This is similar to System IDevID but used for TPM-based attestation. The corresponding private key is stored in TPM. System IAK follows the TCG proposal for TPM2.0 implementation of an IDevID.

iLO does not allow you to update or delete the certificate. You can only view the certificate using the RESTful API GET command:

```
"/redfish/v1/Managers/1/SecurityService/SystemIAK/Certificates/1"
```

NOTE: iLO IDevID, iLO LDevID, System IDevID, and System IAK are preserved across iLO security state transitions, reset to factory defaults.

Platform certificate

iLO can be provisioned with the platform certificate which is an attribute certificate that functions as a signed manifest for the hardware chassis or configuration used to detect supply chain tampering. This certificate is TCG compliant.

iLO does not allow you to update or delete the certificate. You can only view the certificate using the RESTful API GET command:

```
"/redfish/v1/Managers/1/SecurityService/PlatformCert/Certificates/1"
```

One-button secure erase for DevIDs and System IAK

iLO IDevID, iLO LDevID, System IDevID, and System IAK are removed after one-button secure erase.

Hewlett Packard Enterprise recommends to perform a manual backup of iLO to minimize the impact of loss of iLO IDevID, iLO LDevID, System IDevID, and System IAK after one button secure erase. In manual backup, iLO includes all the certificates in its backup service. You can restore these certificates from the backup file.

System board replacement

Once the board is replaced, iLO IDevID, iLO LDevID, System IDevID, and System IAK become invalid. You have to replace all of these on the new board. The factory provisioned certificates (iLO IDevID, System IDevID, and System IAK) cannot be replaced on the new board outside the factory.

In the event of the board replacement, you can create a new LDevID. For more information see, Importing LDevID certificate. On the new board, iLO LDevID will be the only server identity for authentication and authorization.

802.1X and iLO

IEEE 802.1X is a mechanism for port-based network access control, which regulates access to the network and protect against unidentified and unauthorized parties accessing the network.

802.1X uses Extensible Authentication Protocol (EAP) for message exchange during the authentication process. EAP-Transport Layer Security (EAP-TLS) is an EAP type which uses certificates or smart cards for authentication.

HPE iLO 6 supports EAP-TLS based authentication for onboarding into an 802.1X access-controlled network. Using a factory provisioned server identity (iLO IDevID), HPE servers can securely onboard and establish its identity with zero touch (unattended autonomous operation) for 802.1X authentication. iLO also supports user provisioned server identity (iLO LDevID) for 802.1X authentication. When both iLO IDevID and iLO LDevID is present in the system, iLO LDevID is used for EAP-TLS authentication.

The default setting for 802.1X authentication is "Enabled". But iLO 6 does not initiate the EAP-TLS authentication or respond to any authentication requests, if the system does not have iLO IDevID or iLO LDevID.

For more information see iLO IDevID and iLO LDevID.

Subtopics

Prerequisites for 802.1X authentication

Prerequisites for 802.1X authentication

- Secure device identity (iLO IDevID or iLO LDevID) pre-installed.
- Configure your Authentication, Authorization, and Accounting (AAA) server to accept iLO DevID certificate (for example, configuring to support EAP-TLS and installing DevID issuer certificate in RADIUS server).

iLO access settings

HPE ProLiant RL3xx Gen 11 platforms do not support the following features or options:

- HPE SIM

- Platform Level Data Model (PLDM)
- RIBCL

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.

Subtopics

Configuring iLO access settings

Prerequisites

- Prerequisite for modifying any access setting:
  - Configuring iLO Settings privilege
- Additional prerequisites for modifying the Update Service setting:
  - Recovery Set 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: **https://www.hpe.com/support/ilo-docs**.
- Additional prerequisite for modifying the Downloadable Virtual Serial Port Log or Virtual Serial Port Log Over CLI setting:
  - 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: **https://www.hpe.com/support/ilo-docs**.

About this task

This procedure is for all Access Settings except iLO Functionality. To disable iLO Functionality, see Disabling the iLO functionality.

Procedure

1. Click Security in the navigation tree.

   The Access Settings page is displayed.

2. Click  next to the Access Settings category that you want to update.

   Choose from the following:

   - Server
   - Account Service
   - iLO
   - Update Service

- Network

The Edit *Setting Type* page opens.

3. Update the settings as needed, and then click OK.

   Depending on the type of setting you changed, the following might happen:

   - iLO notifies you that the update is complete.
   - iLO notifies you that pending changes require a reset to take effect.

     For some settings, you might observe an immediate impact when the setting is changed, before a reset is complete. For example, if you disable access through the remote console, you cannot start a remote console session after you click OK. A reset is required to complete the configuration change.

     Other settings that require a reset allow you to manually revert the configuration back to its original state without a reset taking place. For those settings, you can manually revert the change, and then click ✕ to dismiss the reset message. For example, if you enable the Virtual NIC feature, iLO notifies you that the pending change requires a reset. If you manually revert this change by resetting the Virtual NIC option to disabled, the pending reset message remains, and you can click ✕ to dismiss the message.

     Clicking ✕ dismisses the reset message, but it does not revert the iLO configuration to the previous settings. If you want to undo a change, you must revert the change manually.

4. (Optional) Repeat steps 2–3 to update additional access settings.
5. If a reset is required and you are done updating access settings, click Reset iLO.

   iLO prompts you to confirm the request.

6. Click Yes, reset iLO.

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

More information

Disabling the iLO functionality

Disabling the iLO functionality

Prerequisites

Configure iLO Settings privilege

About this task

The iLO Functionality setting controls whether iLO functionality is available.

- When this setting is enabled (default), the iLO network is available and communications with operating system drivers are active.
- When this setting is disabled, the iLO network and communications with operating system drivers are terminated.

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

Use this procedure to change the iLO Functionality setting. To update other iLO access settings, see Configuring iLO access settings.

Procedure

1. Click Security in the navigation tree.

   The Access Settings page is displayed.

2. Click ✎ next to the iLO section.

   The Edit iLO Settings page opens.

3. Click Show Advanced Settings.
4. Click Disable in the iLO Functionality section.

   iLO prompts you to confirm the request.
5. Select the Confirm disabling of iLO Functionality check box.
6. Click Yes, disable iLO functionality.

   CAUTION:

   If you click this button, iLO will be inaccessible through any interface. You can use the UEFI System Utilities to restore iLO functionality.

   iLO ends your session and you cannot connect through any iLO interface until you enable the iLO Functionality setting again.
7. (Optional) To re-enable the iLO Functionality, use the UEFI System Utilities or the system maintenance switch.

   Hewlett Packard Enterprise recommends using the UEFI System Utilities to perform this task.

Subtopics

Methods for enabling iLO Functionality

More information

Configuring iLO access settings
Reasons to disable iLO security

Methods for enabling iLO Functionality

When the iLO Functionality is disabled, you cannot re-enable it through the iLO web interface. You can use the UEFI System Utilities or the system maintenance switch to re-enable the iLO Functionality.

UEFI System Utilities

Hewlett Packard Enterprise recommends using the UEFI System Utilities to re-enable iLO Functionality.

For more information, see the UEFI System Utilities documentation.

System maintenance switch

An alternative method for restoring the iLO Functionality is to disable iLO security with the system maintenance switch.

When iLO security is disabled, the iLO network configuration is reset to the factory default settings. If the factory default network interface is connected to the network, iLO is available on the network. This change persists after you restore iLO security.

CAUTION:

Any user can access iLO and modify the configuration when you disable security and iLO is using the Production security state. If you disable security with the system maintenance switch, Hewlett Packard Enterprise strongly recommends using iLO in this configuration for as short a time as possible.

Server access settings options

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

Server Name

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.

Server FQDN/IP Address

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.

Account Service access settings options

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

Authentication Failures Before Delay

Enables you to configure the number of failed login attempts that are allowed before iLO imposes a login delay.
The following values are valid:

- Every failure causes delay—A login delay occurs after the first failed login attempt.
- 1 failure causes no delay (default)—A login delay is not imposed until the second failed login attempt.
- 3 failures cause no delay—A login delay is not imposed until the fourth failed login attempt.
- 5 failures cause no delay—A login delay is not imposed until the sixth failed login attempt.

Authentication Failure Delay Time

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.

Authentication Failure Logging

Enables you to configure logging criteria for failed authentications. All login types are supported; each login type works independently.
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.

Minimum Password Length

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.

When the Password complexity setting is enabled, iLO might not allow passwords that satisfy the minimum password length. For example, if the minimum password length is set to 1, a one-character password is invalid because it does not meet the password complexity requirements.

Password complexity

Controls the password complexity check behavior when you create or edit user accounts and iLO Federation groups.
After you enable this setting, new or updated user account passwords must include 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)

When this setting is disabled (default), these password characteristics are not enforced.

iLO access settings options

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

Global Component Integrity

Enables or disables authentication to all applicable components in the server using SPDM.

This setting is disabled by default.

Enabling the option allows iLO to validate the components on the servers using SPDM.

Component Integrity Policy

Specifies the system boot policy based on the device component integrity policy settings. The two policies are:

- Halt Boot On SPDM Failure —Select the option to halt the system boot during SPDM Authentication failure.
- No Policy—Select the option to boot the system in normal mode.

Downloadable Virtual Serial Port Log

Enables or disables logging of the virtual serial port to a file that you can download through the iLO web interface.

When this setting is enabled, Virtual Serial port activity is logged to a file that you can download from the Access Settings page.

This setting is disabled by default.

A license is required to use this feature. If a license that supports this feature is not installed, this option is not displayed. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/ilo-docs**.

For information about logging the virtual serial port to a file you can view through the CLI, see Network access settings options.

Idle Connection Timeout (minutes)

Specifies how long iLO sessions can be inactive before they end automatically.

The iLO web interface and the .NET IRC track idle time separately because each connection is a separate session. When the Idle Connection Timeout is reached, only the idle session ends.

The iLO web interface and the HTML5 remote console share one iLO session. When the Idle Connection Timeout is reached, the shared session ends.

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 browsing to a different site, or closing the browser window, 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 expire.

This setting applies to local and directory users. Directory server timeout settings might pre-empt 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

For information about this setting, see Disabling the iLO functionality.

iLO RIBCL Interface

Specifies whether RIBCL commands can be used to communicate with iLO.

This setting is enabled by default.

RIBCL over HTTP/HTTPS and RIBCL through in-band communication do not work when this feature is disabled.

The following message is displayed if you try to use RIBCL when it is disabled:

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

```
<RIBCL VERSION="2.23">
<RESPONSE
STATUS="0x00FC"
MESSAGE='RIBCL is disabled.'
/>
</RIBCL>
```

When you change this value, you must reset iLO.

NOTE: You cannot change the default settings for Synergy compute modules. If you try to change the default settings, an error message is displayed.

RIBCL must be enabled for proper communication between HPE OneView and iLO.

iLO ROM-Based Setup Utility

Enables or disables the iLO configuration options in the UEFI System Utilities.

- When this setting is enabled (default), the iLO configuration options are available when you access the UEFI System Utilities.
- When this setting is disabled, the iLO configuration options are not available when you access the UEFI System Utilities.

This setting cannot be enabled if option ROM prompting is disabled in the System BIOS.

iLO Web Interface

Specifies whether the iLO web interface can be used to communicate with iLO.

This setting is enabled by default.

When you change this value, you must reset iLO. After you complete the reset, you will not be able to access the iLO interface through a web browser until you re-enable this setting by using the UEFI System Utilities or the iLO RESTful API.

Remote Console Thumbnail

Enables or disables the display of the remote console thumbnail image in iLO.

Disabling the thumbnail does not disable the remote console feature.

When you disable this setting, it takes approximately 30 seconds for the web interface to stop displaying the thumbnail.

When you enable this setting, refresh the browser window to view the thumbnail. You can also log out and then log back in to iLO to view the thumbnail.

Require Host Authentication

Determines whether iLO user credentials are required to use host-based configuration utilities that access the management processor. These utilities run from the host OS command line in the host context of Administrator or root.

- When this setting is enabled, valid credentials are required for all commands.
- When this setting is disabled, valid credentials are not required and commands operate with Administrator privileges.

  Disabling this setting is not supported when iLO is configured to use a security state higher than High Security.

Require Login for iLO RBSU

Determines whether user credentials are required when a user accesses the iLO configuration options in the UEFI System Utilities.

- When this setting is disabled (default), login is not required when a user accesses the iLO configuration options in the UEFI System Utilities. However, you need to login when Require Host Authentication is enabled.

  When the iLO security state is higher than Production, user credentials are required for accessing the iLO configuration options in the UEFI System Utilities, even if this setting is disabled.
- When this setting is enabled, a login dialog box opens when a user accesses the iLO configuration options in the UEFI System Utilities.

Serial Command Line Interface Speed

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)

  For Synergy compute modules only: The Synergy Console and Composer CLI require setting this value to 9600.
- 19200
- 38400—The iLO configuration options in the UEFI System Utilities 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 UEFI System Utilities.

Serial Command Line Interface Status

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 SMASH CLP from a terminal connected to the host serial port. Valid iLO user credentials are required.
- Enabled-No Authentication—Enables access to SMASH CLP 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.

Show iLO IP during POST

Enables the display of the iLO network IP address during host server POST.

- When this setting is enabled (default), the iLO IP address is displayed during POST.
- When this setting is disabled, the iLO IP address is not displayed during POST.

Show Server Health on External Monitor

Enables the display of the Server Health Summary screen on an external monitor.

- When this setting is enabled, you can press and release the server UID button to display the Server Health Summary screen on an external monitor.
- When this setting is disabled, the Server Health Summary screen does not open when you press and release the server UID button.

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.

This feature is not supported on Synergy compute modules.

For more information about the Server Health Summary screen, see the HPE iLO 6 Troubleshooting Guide.

For more information about the Server Health Summary screen, see the iLO troubleshooting documentation.

VGA Port Detect Override

Controls how devices connected to the system video port are detected. Dynamic detection protects the system from abnormal port voltages.

- When this setting is enabled (default), the iLO firmware detects connected devices before activating video output.
- When this setting is disabled, the iLO hardware detects connected devices before activating video output.

This setting can be used for troubleshooting cases when there is no video output to displays, KVM concentrators, or active dongles.

This setting is not supported on Synergy compute modules.

Virtual NIC

Determines whether you can use a virtual NIC over the USB subsystem to access iLO from the host operating system.

- When this setting is enabled, you can:
  - Initiate iLO RESTful API commands from the RESTful Interface Tool or another client running in the host OS.
  - Connect to iLO with an SSH client running in the host OS.
  - Access the iLO web interface through a supported browser running in the host OS.
  - View the virtual NIC IP address on the Overview page.
- When this setting is disabled, you cannot access iLO through the virtual NIC.

  The factory default Virtual NIC setting is disabled in most versions of iLO. In iLO 6, this setting is enabled by default. When you reset iLO to the factory default settings, the Virtual NIC setting returns to the default setting for the installed version of iLO. Firmware upgrades or downgrades do not change this setting.

Update Service access settings options

Downgrade Policy

Specifies how iLO handles requests to downgrade any of the firmware types that you can update through iLO.

A license is required to use this feature. If a license that supports this feature is not installed, this option is not displayed. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/ilo-docs**.

Choose from the following values:

- Allow downgrades (default)—Any user with the Configure iLO Settings privilege can downgrade firmware.
- Downgrade requires Recovery Set privilege—Only a user with the Configure iLO Settings and Recovery Set privileges can downgrade firmware.
- Permanently disallow downgrades—No user can downgrade firmware.

> **CAUTION:**
>
> Configuring this setting makes a permanent change to iLO. After you configure iLO to permanently disallow downgrades, you cannot reconfigure this setting through any iLO interface or utility. Setting iLO to the factory default settings will not reset this value.

Accept 3rd Party Firmware Update Packages

Specifies whether iLO will accept third-party firmware update packages that are not digitally signed. Platform Level Data Model (PLDM) firmware packages are supported.

This setting is disabled by default.

Network access settings options

The Network section on the Access Settings page allows you to enable and disable iLO features, and to configure the ports they use.

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.

Anonymous Data

This setting controls the following:

- The XML object iLO provides in response to an anonymous request for basic system information.
- The information provided in response to an anonymous Redfish call to `/redfish/v1`.

When this setting is enabled (default):

- Other software is allowed to discover and identify the iLO system on the network. To view the XML response that iLO provides, click View XML.
- An anonymous Redfish call to `/redfish/v1` includes information similar to the following:

```
"ManagerFirmwareVersion": "1.10",
"ManagerType": "iLO 6",
"Status": {"Health": "OK"}
```

- When the iLO health status is Degraded, the iLO health status and a description of the issue are displayed 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.

When this option is disabled:

- iLO responds to requests with an empty XML object.
- iLO version information is not displayed on the login page.
- An anonymous Redfish call to `/redfish/v1` excludes the following information: `ManagerFirmwareVersion`, `ManagerType`, and `Status`.

When you enable a security state higher than Production or High Security, this setting is disabled automatically.

Enhanced Download Performance

Allows you to improve the download performance for iLO Scriptable Virtual Media and URL based firmware upload.

When this option is Enabled, iLO will optimize its communication with the web server hosting the images. After changing the option, the setting will take effect only on new virtual media connections and firmware update operations initiated.

This setting is enabled by default.

To edit the Enhanced Download Performance settings, navigate to Access settings page, click  on the Network settings.

IPMI/DCMI over LAN

Allows you to send industry-standard IPMI and DCMI commands over the LAN.

This setting is disabled by default.

When this setting is disabled, iLO disables IPMI/DCMI over the LAN. Server-side IPMI/DCMI applications are still functional when this feature is disabled.

When this setting is enabled, iLO allows you to use a client-side application to send IPMI/DCMI commands over the LAN.

When IPMI/DCMI over LAN is disabled, the configured IPMI/DCMI over LAN Port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

When you enable a security state higher than Production or High Security, this setting is disabled automatically.

IPMI/DCMI over LAN Port

Sets the IPMI/DCMI port number.

The default value is UDP 623.

IPMI over KCS

IPMI over Keyboard Controller Style (KCS) enables you for management of a computer system and monitoring the operations from within the host OS.

IPMI over KCS option allows you to enable or disable KCS interface.

This setting is Enabled by default. But while upgrading from iLO 6 1.50 to a later version, the default value for IPMI over KCS is stored based on the previous configuration settings.

To edit the setting from the Access settings page, click on the Network settings and uncheck IPMI over KCS check box.

Commands to enable and disable KCS interface

Volatile configuration

Command syntax-- `0x06 command: 0x41(get)/0x40(set) interface : 0x0F(KCS) conf:0x82(enable)/0x80(disable) 0x00`
To enable the KCS interface, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x40 0x0F 0x82 0x00` **command.**
To check the KCS interface status, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x41 0x0F 0x80` **command.**
Response Data : 02 04

`02` **--Indicates KCS is enabled**

`04` **-- Indicates ADMIN privileges**

To disable KCS interface, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x40 0x0F 0x80 0x00` **command.**

Non-Volatile configuration

Command syntax-- `0x06 command: 0x41(get)/0x40(set) interface : 0x0F(KCS) conf:0x42(enable)/0x40(disable) 0x00`
To enable KCS interface, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x40 0x0F 0x42 0x00` **command.**
To check the KCS interface status, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x41 0x0F 0x40` **command.**
Response Data: 02 04

`02` **--Indicates KCS is enabled**

`04` **-- Indicates ADMIN privileges**

To disable KCS interface, run `#> ipmitool -I lanplus -H <IP Address> -U <user name> -P <password> raw 0x06 0x40 0x0F 0x40 0x00` **command.**

NOTE:

- In Volatile configuration, enable or disable of KCS interface is possible only through ipmitool.
- A change in Volatile configuration does not affect Non-Volatile configuration.
- In Nonvolatile configuration, enable or disable of KCS interface is possible through Redfish, iLO web interface, or ipmitool.
- A change in Nonvolatile configuration also affects Volatile configuration.
- HPE ProLiant RL3xx Gen 11 platforms do not support IPMI over KCS. IPMI in-band operation is supported through SSIF protocol.

Remote Console

Allows you to enable or disable access through the iLO remote consoles.

When this option is disabled, the graphical remote console and the text-based remote console are disabled. The configured remote console port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Disabling the remote console does not disable the remote console thumbnail. To disable the remote console thumbnail, edit the Remote Console Thumbnail option in the iLO Access Settings section.

This setting is enabled by default.

Remote Console Port

Sets the remote console port.

The default value is TCP 17990.

Secure Shell (SSH)

Allows you to enable or disable the SSH feature.

SSH provides encrypted access to the iLO command-line protocol (CLP).

This setting is enabled by default.

Secure Shell (SSH) Port

Sets the SSH port.

The default value is TCP 22.

SNMP

Specifies whether iLO responds to external SNMP requests.

If you disable SNMP access, 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 disabled, most of the boxes on the SNMP Settings page are unavailable.

When you enable a security state higher than Production or High Security, this setting is disabled automatically.

SNMP Port

Sets the SNMP port.

The default value is UDP 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.

If the SNMP option is disabled, you cannot update this value.

SNMP Trap Port

Sets the SNMP trap port.

The default value is UDP 162 for SNMP alerts (or traps).

If you customize the SNMP Trap Port, some SNMP monitoring applications 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.

If the SNMP option is disabled, you cannot update this value.

Virtual Media

Allows you to enable or disable the iLO virtual media feature.

When this option is disabled, virtual media features are disabled. The configured virtual media port is not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Virtual Media Port

The port that iLO uses to listen for incoming local virtual media connections.

The default value is TCP 17988.

Virtual Serial Port Log Over CLI

Enables or disables logging of the virtual serial port that you can view by using the CLI.

When this setting is enabled, virtual serial port activity is logged to a 150-page circular buffer in the iLO memory. Use the CLI command `vsp log` to view the logged information. The virtual serial port buffer size is 128 KB.

This setting is disabled by default.

A license is required to use this feature. If a license that supports this feature is not installed, this option is not displayed. For information about the available license types and the features they support, see the licensing documentation at the following website: **https://www.hpe.com/support/ilo-docs**.

For information about logging the virtual serial port to a file you can download through the iLO web interface, see iLO access settings options.

Web Server

Allows you to enable or disable access through the iLO web server.

CAUTION:

If you set this value to disabled, iLO will not listen for communication on the configured Web Server Non-SSL Port (HTTP) or the Web Server SSL Port (HTTPS).

The following features do not work when the web server is disabled:

- iLO web interface
- Remote console
- iLO RESTful API
- RIBCL

When this option is disabled, the configured Web Server Non-SSL Port (HTTP) and Web Server SSL Port (HTTPS) are not detected in a security audit that uses a port scanner to scan for security vulnerabilities.

Web Server Non-SSL Port Enabled

Disables the HTTP port.

Web Server Non-SSL Port (HTTP)

Sets the HTTP port.

The default value is TCP 80.

Web Server SSL Port (HTTPS)

Sets the HTTPS port.

The default value is TCP 443.

NOTE: You cannot change the default settings for Synergy compute modules. If you try to change the default settings, an error message is displayed.

When this option is disabled, iLO fails to detect the communication from configured Web Server and results in disabling RIBCL.

RIBCL must be enabled for proper communication between HPE OneView and iLO

Web Proxy

Specifies whether the Web proxy server is enabled or not.

To enable the Web proxy from the Access Settings page:

- Click on the Network settings and select the Web Proxy check box.
- Enter the Web Proxy Server name, Web Proxy Port number, Web Proxy User Name, and Web Proxy Password.
  - Web Proxy Server—Indicates the hostname or IP address of proxy server.
  - Web Proxy Port —Specifies the web proxy port number. The range of valid port values in iLO is from 1–65535.
  - Web Proxy User Name—Indicates web proxy user name.
  - Web Proxy Password—Indicates web proxy password.
- Click OK to enable the proxy server.

To reset the web proxy settings to default values, clear the Web proxy check box and click OK.

802.1X Support

Specifies whether iLO supports 802.1X-based authentication. This feature supports using a factory-provisioned server identity (iLO IDevID) or a user-defined server identity (iLO LDevID) for authentication.

Subtopics

iLO login with an SSH client

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.

iLO Service Port

The Service Port is a USB port with the label **iLO** on supported servers and compute modules.

To find out if your server or compute module supports this feature, see the server specifications document at the following website: **https://www.hpe.com/info/quickspecs**.

When you have physical access to a server, you can use the Service Port to do the following:

- Download the Active Health System Log to a supported USB flash drive.

  When you use this feature, the connected USB flash drive is not accessible by the host operating system.

- Connect a client (such as a laptop) with a supported USB to Ethernet adapter to access the following:
  - iLO web interface
  - Remote console
  - iLO RESTful API
  - CLI
  - RIBCL scripts

When you use the iLO Service Port:

- Actions are logged in the iLO event log.
- The server UID flashes to indicate the Service Port status.

  You can also retrieve the Service Port status by using a REST client and the iLO RESTful API.

- You cannot use the Service Port to boot any device within the server, or the server itself.
- You cannot access the server by connecting to the Service Port.

- You cannot access the connected device from the server.

Downloading the Active Health System Log through the iLO Service Port

Prerequisites

The iLO Service Port and USB flash drives options are enabled on the iLO Service Port page.

Procedure

1. Create a text file named `command.txt` with the required content for downloading the Active Health System Log.
2. Save the file to the root directory of a supported USB flash drive.
3. Connect the USB flash drive to the iLO Service Port (the USB port labeled **iLO**, on the front of the server).

   The file system is mounted and the `command.txt` file is read and executed.

   The iLO Service Port status changes to Busy, and the UID flashes at a rate of four medium flashes then off for one second.

   If the command is successful, the iLO Service Port status changes to Complete, and the UID flashes at a rate of one fast flash then off for three seconds.

   If the command is not successful, the iLO Service Port status changes to Error, and the UID flashes at a rate of eight fast flashes then off for one second.

   The file system is unmounted.
4. Remove the USB flash drive.

   The iLO Service Port status changes to Ready. The UID stops flashing or flashes to indicate another state such as remote console access or a firmware update in progress.
5. (Optional) Upload the file to HPE InfoSight.

   You can access the Analyze Logs page in HPE InfoSight by selecting Infrastructure > Analyze Logs under the Compute heading.

   For more information, see the HPE InfoSight for Servers User Guide at the following website: **https://www.hpe.com/support/infosight-servers-docs**.

   HPE ProLiant RL3xx Gen 11 platforms do not support HPE InfoSight.

More information

Configuring the iLO Service Port settings
iLO Service Port supported devices
Sample text file for Active Health System Log download through iLO Service Port

Connecting a client to iLO through the iLO Service Port

Prerequisites

- The iLO Service Port and USB Ethernet adapters options are enabled on the iLO Service Port page.
- The client NIC is configured to support the Service Port feature.
- You have physical access to the server.

Procedure

1. Use a supported USB to Ethernet adapter to connect a client to the Service Port (the USB port labeled **iLO**, on the front of the server).

   The client NIC is assigned a link-local address. This process might take several seconds.
2. Connect to iLO by using the following IPv4 address: `169.254.1.2`.

   The same IP address is used when you connect a client to any server through the Service Port. You cannot change this address.

The Service Port status changes to Busy, and the UID flashes at a rate of four medium flashes then off for one second.

3. When you are finished, disconnect the client from the Service Port.

   The Service Port status changes to Ready. The UID stops flashing or flashes to indicate a state such as remote console access or a firmware update in progress.

More information

Configuring the iLO Service Port settings
Configuring a client to connect through the iLO Service Port

Configuring the iLO Service Port settings

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Security in the navigation tree, and then click the iLO Service Port tab.
2. Configure the following settings:
   - iLO Service Port
   - USB flash drives
   - Require authentication
   - USB Ethernet adapters
3. Click Apply.

   The updated settings take effect immediately, and information about the configuration change is logged in the iLO event log.

iLO Service Port options

- iLO Service Port—Allows you to enable or disable the iLO Service Port. The default setting is enabled. When this feature is disabled, you cannot configure the features in the Mass Storage Options or Networking Options sections on this page.

  Do not disable the iLO Service Port when it is in use. If you disable the port when data is being copied, the data might be corrupted.

- USB flash drives—Allows you to connect a USB flash drive to the iLO Service Port to download the Active Health System Log. The default setting is enabled.

  Do not disable this setting when the iLO Service Port is in use. If you disable USB flash drives when data is being copied, the data might be corrupted.

  If you insert a USB flash drive in the iLO Service Port when this setting is disabled, the device is ignored.

- Require authentication—Requires you to enter iLO user credentials in the `command.txt` file when you use the iLO Service Port to download the Active Health System Log. The default setting is disabled.

  User credentials are not required when the system maintenance switch is set to disable iLO security.

- USB Ethernet adapters—Allows you to use a USB to Ethernet adapter to connect a laptop to the iLO Service Port to access the Integrated remote console. The default setting is enabled.

  If you connect a laptop when this setting is disabled, the device is ignored.

Configuring a client to connect through the iLO Service Port

Procedure

1. Configure the client NIC to obtain an IPv4 autoconfiguration address automatically.

For more information, see your operating system documentation.

2. Do one of the following:

   - Add a proxy exception. Use one of the following formats:
     - Edge, Chrome: `169.254.*`
     - Firefox: `169.254.0.0/16`
   - Disable web proxy settings on the client.

   For more information about proxy settings, see your operating system documentation.

iLO Service Port supported devices

Mass storage devices

The iLO Service Port supports USB keys with the following characteristics:

- High-speed USB 2.0 compatibility.
- FAT32 format, preferably with 512 byte blocks.
- One LUN.
- One partition with a maximum size of 127 GB and sufficient free space for the Active Health System Log download.
- Valid FAT32 partition table.

  If the USB key fails to mount, it probably has an invalid partition table. Use a utility such as Microsoft DiskPart to delete and recreate the partition.
- Not read-protected.
- Not bootable.

Mass storage devices are not supported on servers that do not include a NAND.

USB Ethernet adapters

The iLO Service Port supports USB Ethernet adapters that contain one of the following chips by ASIX Electronics Corporation:

- AX88772
- AX88772A
- AX88772B
- AX88772C

Hewlett Packard Enterprise recommends the HPE USB to Ethernet Adapter (part number Q7Y55A).

Sample text file for Active Health System Log download through iLO Service Port

When you use the iLO Service Port to download the Active Health System Log, you create a text file called `command.txt` and save the file to a supported USB device. When you connect the USB device to a server, the `command.txt` file runs and downloads the log file.

File template for command.txt file

Use the following example as a template for your `command.txt` file:

```
{
  "/ahsdata/" : {
    "POST" : {
      "downloadAll"  : "0",
      "from"         : "2016-08-25",
      "to"           : "2016-08-26",
      "case_no"      : "ABC0123XYZ",
```

```
      "contact_name" : "My Name",
      "company"      : "My Company, Inc.",
      "phone"        : "281-555-1234",
      "email"        : "my.name@mycompany.com",
      "UserName"     : "my_username",
      "Password"     : "my_password"
    }
  }
}
```

Parameters for command.txt file

You can customize the following values:

- `downloadAll` —Controls the download scope. To download the log for a range of dates, enter `0`. To download the entire log, enter `1`.
- `from` —The start date when you download the log for a range of dates.
- `to` —The end date when you download the log for a range of dates.
- `case_no` (optional)—The case number for an open HPE support case. This value can be up to 14 characters long. If you enter this value, it is included in the downloaded file.
- `contact_name` (optional)—The contact person for this server. If you enter this value, it is included in the downloaded file. This value can be up to 255 characters long.
- `company` (optional)—The company that owns this server. If you enter this value, it is included in the downloaded file. This value can be up to 255 characters long.
- `phone` (optional)—The phone number of a contact person for this server. If you enter this value, it is included in the downloaded file. This value can be up to 39 characters long.
- `email` (optional)—The email address of a contact person for this server. If you enter this value, it is included in the downloaded file. This value can be up to 255 characters long.
- `UserName` —If iLO is configured to require authentication for iLO Service Port actions on mass storage devices, enter your iLO account user name. A user name is not required when the system maintenance switch is set to disable iLO security.
- `Password` —If iLO is configured to require authentication for iLO Service Port actions on mass storage devices, enter the password for the user name you entered. A password is not required when the system maintenance switch is set to disable iLO security.

File requirements for command.txt file

- The file must be in valid JSON format.

  Hewlett Packard Enterprise recommends using an online JSON formatter to verify the file syntax. A free utility is available at the following website: **http://www.freeformatter.com/json-formatter.html**.
- Do not include comments in the file.
- The text in the file is case-sensitive.
- The file supports plain text only. Do not create the file with an application that embeds additional formatting properties.

Managing SSH keys

About this task

Subtopics

Authorizing a new SSH key by using the web interface

Prerequisites

Administer User Accounts privilege

Procedure

1. Generate either a 2,048-bit or 4,096 bit DSA or RSA key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.

   DSA is allowed only when iLO is configured to use the Production security state and Disable Weak Ciphers option is not selected in Security > Encryption tab.

   ECDSA 384-bit keys that use the NIST P-384 curve are required when iLO is configured to use the CNSA security state.
2. Save the public key as `key.pub`.
3. Copy the contents of the `key.pub` file.
4. Click Security in the navigation tree, and then click the Secure Shell Key tab.
5. 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.
6. Click Authorize New Key.
7. Paste the public key into the Public key box.
8. 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.

   ECDSA 384-bit keys that use the NIST P-384 curve are required when iLO is configured to use the CNSA security state.
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 "oemhpe_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:

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

Deleting SSH keys

Prerequisites

Administer User Accounts privilege

About this task

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.

Procedure

1. Click Security in the navigation tree, and then click the Secure Shell Key tab.
2. In the Authorized SSH Keys list, select the check box to the left of one or more user accounts.
3. Click Delete Selected Key(s).

   iLO prompts you to confirm the request.
4. Click Yes, delete.

   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.

HPE ProLiant RL3xx Gen 11 platforms do not support HPE SIM.

Viewing the SSH host key

About this task

Use the following procedure to view the SSH host key reported by iLO.

Procedure

1. Click Security in the navigation tree, and then click the Secure Shell Key tab.

   The SSH host key is displayed.

2. (Optional) Add the hostname/IP address and the SSH host key to the SSH client configuration file.

   For example:

   - For OpenSSH users on Linux: Update the `.ssh/known_hosts` file.
   - For PuTTY users on Windows: Update the Windows registry (`HKEY_CURRENT_USER\SoftWare\SimonTatham\PuTTY\SshHostKeys`).

3. (Optional) To verify that your connection is secure, compare the SSH Host Key value to the value reported by your SSH client.

   For example:

```
Linux-client:~ # grep ilo.example.com .ssh/known_hosts
ilo.example.com,[redacted] ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC9E/XDH9xPU+NdMyTu5Oylw9AN6mJlH7woMqcf791da6DeS1D+vX1I
Wg3GwDKFUobabQ+gZtkBrxWFzwAf51CPitsybQCK2hvLztsypb/W3p+MPZ9zU6/voCHzL2v0bAxeXuX8ack/8RA
w011agB5xY6B3pjP/qaeFJb29sGqPwoaXps6g5t/YFhxIQ8is8N+LnfuTzMtQDj74rfq6pcXGnXq+ErmbkcfHn
AdSMveT6rXPM1U+Je1B9VOVS23fUL7mfoshLnSHrJJtP7XkZ1rKf1QPKCChWLfpdmTprsaJrxDrwCNxX4+pPh
UXqHYLTlvPA8xsqaPxPZfHxZWTZrCp
```

4. If the keys do not match, make sure that you understand why before you continue.

   Some possible reasons include:

   - The iLO system you viewed in step 1 is not the same system that you connected to with the SSH client.
   - The SSH connection is being redirected. Ask an administrator if your network is configured to redirect the connection. If the network is not configured to redirect the connection, the network security might be compromised.
   - The iLO SSH host key on the system you want to access changed because iLO was reset to the factory default settings. You did not change your SSH client configuration.

Viewing authorized SSH keys

Procedure

1. Click Security in the navigation tree, and then click the Secure Shell Key tab.

   The Authorized SSH Keys table displays the hash of the SSH public key associated with each user account.

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.

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.
- Only the iLO legacy format is supported with RIBCL scripts.
- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.
- The iLO firmware 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 you use HPQLOCFG and a RIBCL script to enter the public key, you append the iLO user name to the public key data. The public key is stored with that user name.
- 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
ZtzF0VInP5x2VFVYmIvdVjSupD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCTCRLF
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
a9QI9lH1r3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/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
```

CAC Smartcard Authentication

A common access card (CAC) is a United States Department of Defense (DoD) smartcard for multifactor authentication. Common access cards are issued as standard identification for active-duty military personnel, reserve personnel, civilian employees, non-DoD government employees, state employees of the National Guard, and eligible contractor personnel. In addition to its use as an ID card, a common access card is required for access to government buildings and computer networks.

Each CAC carries a smartcard certificate that must be associated with your local user account in the iLO web interface. Upload and associate your smartcard certificate with your account by using the controls on the Certificate Mappings page.

CAC authentication with LDAP directory support uses a service account to authenticate to the directory service, and the user account must be present in the same domain as the configured directory server. Additionally, the user account must be a direct member of the configured groups or extended schema Roles. Cross-domain authentication and nested groups are not supported.

Two-factor authentication

Part of the requirement necessary to satisfy Federal Government Certification is two-factor authentication. Two-factor authentication is the dual authentication of the CAC. For example, the CAC satisfies two-factor authentication by mandating that you have the physical card and you know the PIN number associated with the card. To support CAC authentication, your smartcard must be configured to require a PIN.

Configuring CAC smart card authentication settings

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: **https://www.hpe.com/support/ilo-docs**.
- (Optional) The LDAP server CA certificates for directory integration are installed.
- (Optional) LDAP directory integration in directory default schema mode is configured.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Import a trusted CA certificate.

   This certificate is used to validate certificates that are presented to iLO. The certificate must be compliant with the configured iLO security state.
3. Configure the Authentication Options:
   a. Enable CAC Smartcard Authentication.
   b. (Optional) Enable CAC Strict Mode.
4. (Optional) For additional security when CAC Strict Mode is enabled, Hewlett Packard Enterprise recommends enabling the following:
   - Require Host Authentication—You can configure this setting on the Access Settings page.

- FIPS security state—You can configure this setting on the Encryption page.

5. (Optional) If you are using directory integration, select an option in the Directory User Certificate Name Mapping section.

   This setting identifies which portion of your user certificate will be used to identify your directory user account.

6. To save the Authentication Options and Directory User Certificate Name Mapping settings, click Apply.

   If you enabled CAC Strict Mode, iLO prompts you to confirm the request, which requires an iLO reset.

   If you did not enable CAC Strict Mode, iLO notifies you that the changes were saved.

7. If iLO prompted you to confirm the changes and initiate a reset, click Yes, apply and reset.
8. (Optional) Import a Certificate Revocation List (CRL).
9. (Optional) To check user certificates using the Online Certificate Status Protocol (OCSP), enter an HTTP or HTTPS URL in the OCSP Settings section, and then click Apply.
10. Upload and map smart card certificates to local iLO user accounts (when using iLO with local user authentication only).

More information

Managing trusted certificates for CAC Smartcard Authentication
Authorizing a new local user certificate
Schema-free directory authentication

CAC smart card authentication settings

CAC Smartcard Authentication

Enables and disables authentication through a common access smart card.

CAC Strict Mode

Enables or disables CAC Strict Mode, which requires a client certificate for every connection to iLO. When this mode is enabled, iLO will not accept user names or passwords, and only key-based authentication methods are allowed.

> **NOTE:**
> If you do not have a trusted certificate, you cannot access iLO. Attempts to browse to the iLO web interface will generate an error.

Directory User Certificate Name Mapping

The For Directory Username setting allows you to select the portion of the user certificate to use as your directory user name:

- Use Certificate SAN UPN—Uses the first subject alternative name (SAN) field of type userPrincipalName (UPN), which contains the user and domain names in an email address format, as the user name. For example, `upn:testuser@domain.com` produces `testuser@domain.com`.
- Use Certificate Subject CN—Uses only the CN or CommonName portion of the subject as the user name. For example, in the following DN: `cn=test user, ou=users,dc=domain,dc=com` the common name is `test user`.
- Use Full Certificate Subject DN—Uses the complete distinguished name as the user name when searching for the user in the directory service. For example, a distinguished name appears as follows: `cn=test user, ou=users,dc=domain,dc=com`.
- Use Certificate SAN RFC822 Name—Uses the first SAN field of type rfc822Name, which contains an email address as the username. For example, `rfc822Name:testuser@domain.com` produces `testuser@domain.com` as the username.

OCSP Settings

Use this feature to check user certificates by using the Online Certificate Status Protocol (OCSP).

HTTP and HTTPS URLs are accepted.

A response of `Unknown` or `Revoked` causes authentication to fail.

Managing trusted certificates for CAC Smartcard Authentication

Importing a trusted CA certificate

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: **https://www.hpe.com/support/ilo-docs**.
- You obtained a trusted CA certificate.

  The certificate must be in PEM encoded Base64 format.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Paste a trusted CA certificate in the Direct Import section.
3. Click Apply.

   If the operation does not appear to have worked, scroll to the top of the page to see if any error messages displayed.

Deleting a trusted CA certificate

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Scroll to the Manage Trusted CA Certificates section.
3. Select the check box next to the certificate to be deleted.
4. Click Delete.

   iLO prompts you to confirm the request.
5. Click Yes, delete.

   The certificate is deleted.

   If the operation does not appear to have worked, look for error messages at the top of the page.

Importing a certificate revocation list (CRL) from a URL

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: **https://www.hpe.com/support/ilo-docs**.

About this task

To invalidate previously issued certificates that have been revoked, import a CRL.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Type or paste a URL in the Import Revocation List section.

The CRL size limit is 100 KB and the CRL must be in DER format.

3. Click Apply.

   The CRL changes will be applied to future CAC login sessions.

   To enforce the CRL changes on existing CAC login sessions, do one of the following:

   - Reset iLO.
   - Identify the CAC sessions in the active session list, and then disconnect them.

   The CRL description and serial number are displayed in the Certificate Revocation List (CRL) section.

Deleting a certificate revocation list

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: **https://www.hpe.com/support/ilo-docs**.

Procedure

1. Click Security in the navigation tree, and then click the CAC/Smartcard tab.
2. Scroll to the Certificate Revocation List (CRL) section.
3. Click Delete.

   iLO prompts you to confirm the request.

4. Click Yes, delete.

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.

Certificates are included when you use the iLO backup and restore feature.

Subtopics

Viewing SSL certificate information

Procedure

Click Security in the navigation tree, and then click the SSL Certificate tab.

Subtopics

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.

Automatic certificate enrollment

iLO now supports obtaining and renewing SSL certificate automatically using the Simple Certificate Enrollment Protocol (SCEP). Currently, iLO supports these features on the Microsoft Network Device Enrollment Service (NDES).

To enable the certificate enrollment for iLO , you must first configure the following services on the certificate enrollment server:

- Configure the Certificate Authority (CA). CA is the server that runs the Certificate Services and issues certificates.
- Configure NDES. NDES is the Certificate Enrollment Server.

NOTE:
This feature is not supported when iLO is in CNSA security state.

By default the feature is disabled. For more information on enabling the feature, see Enabling Automatic certificate enrollment section.

Trusted SSL certificate

Procedure

1. To customize the SSL certificate, select one of the following options:
   - Generate CSR and Import an SSL Certificate —Use this option to create a Certificate Signing Request (CSR) that you can send to a Certificate Authority (CA) to obtain a trusted SSL certificate to import into iLO.
   - Import an SSL Certificate and Private Key —Use this option to manually import a Trusted SSL Certificate and corresponding Private Key.
   - Automatically manage SSL Certificate —Use this option to manage automatic generation or renewal of SSL Certificates.
2. Click Customize Certificate.

   A new page opens for certificate customization process.

Customize certificate

Obtaining and importing SSL certificate manually

Enabling Automatic certificate enrollment

Generate CSR and Import an SSL Certificate

Prerequisites

Configure iLO Settings privilege

About this task

HPE ProLiant RL3xx Gen 11 platforms do not support CNSA security state.

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

iLO supports import of SSL certificate chains (in PEM format) that are up to 20 KB in size.

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 to obtain a new certificate from a CA.

Procedure

1. Obtain a trusted certificate from a CA.
2. Import the trusted certificate to iLO.

Obtaining a trusted certificate from a CA

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Security in the navigation tree, and then click the SSL Certificate tab.
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 or a CNSA-compliant key signed using SHA-256. 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. Click Security in the navigation tree, and then click the SSL Certificate tab.
2. Select Generate CSR and Import an SSL Certificate .
3. Click Customize Certificate.
4. Click Import Certificate.
5. In the Import Certificate window, paste the certificate into the text box, and then click Import.

   iLO prompts you to confirm the request and reset iLO.
6. Click Yes, apply and reset.

   iLO imports the certificate, and then resets.

Enabling Automatic certificate enrollment

Prerequisites

- URL of the certificate enrollment server
- Challenge password
- CA certificate of the certificate enrollment server.
- Configure CSR.
- 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: **https://www.hpe.com/support/ilo-docs**.
- Configure iLO Settings privilege.

About this task

Procedure

1. Click Security in the navigation tree, and then click the SSL Certificate tab.

   iLO self signed certificate is the default certificate.

2. Select Automatically manage SSL Certificate.
3. Click Customize Certificate . Automatic Certificate Enrollment page opens.
4. Enter the following values for certificate enrollment settings:
   - Server URL—The URL of the Certificate Enrollment server.
   - Challenge Password—Challenge password obtained from the Certificate Enrollment Server and used to authenticate iLO during certificate enrollment and renewal.
   - CA Certificate—The CA certificate of the Certificate Enrollment server. CA certificate is used to establish trust between iLO and Certificate Enrollment Server.

     NOTE:
     - Server URL, Challenge Password, and CA Certificate are mandatory fields for certificate enrollment.
     - iLO supports import of CA certificate (in PEM format) that are up to 6 KB in size.
     - iLO supports challenge password that are up to 63 characters.

   - Country (C)—The two-character country/region code that identifies the country/region 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.

   NOTE: CSR fields are common for both manual import and automatic import of SSL certificate.

5. (Optional) To include the iLO IP addresses in the CSR, select the include iLO IP Address(es) check box.

   NOTE:

   Some certificate authorities (CAs) might not support this CSR field. 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.
6. Click Enable to initiate the enrollment process.

   As soon as the certificate enrollment service is enabled, the certificate enrollment status will be In-progress.

   After a few minutes (up to 10), refresh the page to get the latest certificate enrollment status. Certificate enrollment status will be Success when the enrollment is successful. Also, a message notifies that the Certificate Enrollment Service is enabled successfully. You must reset iLO manually after successful enrollment. The newly trusted certificate will be in use only after iLO reset.

   Certificate enrollment status will be Failed when the enrollment failed. For more information on cause of failure and recommended actions, see the Security Logs page.

   NOTE: If Enrollment Service is enabled, removal and manual import of certificate is not allowed.

Updating certificate enrollment settings

Prerequisites

Configure iLO Settings privilege.

About this task

Procedure

1. Click Security in the navigation tree, and then click the SSL Certificate tab.

   A message notifies that Trusted SSL certificate is in use.
2. Under Trusted SSL Certificate, Automatically manage SSL Certificate option is selected by default.
3. Click Customize Certificate. Automatic Certificate Enrollment page opens.
4. Edit the fields and click Update.

> **NOTE:** Updating the settings does not initiate certificate enrollment. To start the enrollment, first disable the service and enable it again.

Renewing automatically managed SSL certificate

About this task

When the certificate enrollment service is enabled and the certificate is about to expire (that is 30 days from the expiry date), iLO initiates certificate renewal automatically. As soon as iLO initiates certificate renewal, the certificate enrollment status will be In-progress.

Certificate enrollment status will be Success when the renewal is successful. For information on renewal status, see the Security Logs page. You must reset iLO manually after successful renewal. The newly trusted certificate will be in use only after iLO reset.

Certificate enrollment status will be Failed when the renewal failed. For more information on cause of failure and recommended actions, see the Security Logs page.

Disabling enrollment service

Prerequisites

Configure iLO Settings privilege.

About this task

Disabling enrollment service does not remove the certificate generated using the service. To remove the certificate, see Removing an SSL certificate.

When the service is disabled, iLO does not initiate renewal of the certificate automatically.

Procedure

1. Under Trusted SSL Certificate, Automatically manage SSL Certificate option is selected by default.
2. Click Customize Certificate. Automatic Certificate Enrollment page opens.
3. Click Disable service.
4. Click Yes, disable to confirm disable. The certificate enrollment status is also disabled.

   For information on enabling the certificate enrollment, see Enabling Automatic certificate enrollment section.

Removing an SSL certificate

Prerequisites

Configure iLO Settings privilege

About this task

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

NOTE: If Certificate Enrollment Service is enabled, removal and manual import of certificate is not allowed.

You might want to remove a 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 the certificate.

Procedure

1. Click Security in the navigation tree, and then click the SSL Certificate tab.
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 Yes, remove.

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

   It might take several minutes for iLO to generate the new certificate.
4. Recommended: Obtain and import a trusted certificate.

   Hewlett Packard Enterprise recommends importing a trusted certificate.

More information

Generate CSR and Import an SSL Certificate
Enabling Automatic certificate enrollment

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. You can also setup Two Factor Authentication for Microsoft Active Directory login users.

When two factor authentication is enabled, basic authorization through REST API is not be supported for Active Directory users. HTTP 401 error stating `Unauthorized login attempt` is displayed.

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.

Subtopics

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.

More information

Configuring Kerberos authentication
Configuring directory integration (schema free configuration)
Configuring directory integration (HPE Extended Schema configuration)

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. Click Security in the navigation tree, and then click the Directory tab.
2. Enable Kerberos Authentication.
3. Set Local User Accounts to enabled 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 your browser), and then follow the onscreen instructions.

8. Click Apply Settings.
9. To configure directory groups, click the Directory Groups link.

Subtopics

Kerberos settings

More information

Prerequisites for configuring authentication and directory server settings
iLO directory groups
Configuring Kerberos authentication

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. To configure OpenLDAP based directory server, see the OpenLDAP Software Administrator's Guide.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.
2. Select Use Directory Default Schema from the LDAP Directory Authentication menu.
3. Set Local User Accounts to enabled if you want to use local user accounts at the same time as directory integration.
4. OpenLDAP users only: Enable Generic LDAP.

   This setting is available only if Use Directory Default Schema is selected and Two Factor Authentication is disabled.
5. For configurations with CAC/Smartcard authentication enabled, enter the CAC LDAP service account and password in the iLO Object Distinguished Name CAC LDAP Service Account and iLO Object Password boxes.
6. Enter the FQDN or IP address of a directory server in the Directory Server Address box.
7. Enter the directory server port number in the Directory Server LDAP Port box.
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 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. Enter valid search contexts in one or more of the Directory User Context boxes.
11. Click Apply Settings.
12. To test the communication between the directory server and iLO, click Test Settings.
13. To configure directory groups, click the Directory Groups link.

Subtopics

Schema-free directory settings

More information

Prerequisites for configuring authentication and directory server settings
iLO directory groups
Running directory tests
Directory user contexts
Directory Server CA Certificate
Local user accounts with Kerberos authentication and directory integration
Configuring directory integration (schema free configuration)

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.
- iLO Object Distinguished Name/CAC LDAP Service Account —Specifies the CAC LDAP service account when CAC/Smartcard authentication is configured and used with the schema-free directory option.

  User search contexts are not applied to the iLO object DN when iLO accesses the directory server.
- iLO Object Password—Specifies the CAC LDAP service account password when CAC/Smartcard authentication is configured and used with the schema-free directory option.
- 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 7 KB in size.

Configuring HPE Extended Schema directory settings in iLO

Prerequisites

Your environment meets the prerequisites for using this feature.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.
2. Select Use HPE Extended Schema from the LDAP Directory Authentication menu.
3. Set Local User Accounts to enabled if you want to use local user accounts at the same time as directory integration.
4. Enter the location of this iLO instance in the directory tree in the iLO Object Distinguished Name/CAC LDAP Service Account box.
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. (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.
8. (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.
9. Enter valid search contexts in one or more of the Directory User Context boxes.
10. Click Apply Settings.
11. To test the communication between the directory server and iLO, click Test Settings.

Subtopics

HPE Extended Schema directory settings

More information

Prerequisites for configuring authentication and directory server settings
Running directory tests
Directory user contexts
Local user accounts with Kerberos authentication and directory integration
Configuring directory integration (HPE Extended Schema configuration)

HPE Extended Schema directory settings

- Use HPE Extended Schema—Selects directory authentication and authorization by using directory objects created with the HPE Extended Schema. Select this option when the directory has been extended with the HPE Extended Schema. The HPE Extended Schema works only with Microsoft Windows. This configuration supports Active Directory.

- iLO Object Distinguished Name/CAC LDAP Service Account —For the HPE Extended Schema configuration, this setting 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 iLO 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.

- 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 7 KB in size.

- 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.

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. Click Security in the navigation tree, and then click the Directory tab.
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.

Enabling Two Factor Authentication in iLO

Prerequisites

- Enable SMTP for Two Factor Authentication option is enabled in Management > Mail page.
- Generic LDAP is disabled.
- Your environment meets the prerequisites for using this feature.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.

2. Enable Two Factor Authentication.
3. Click Apply Settings.

Disabling Two Factor Authentication in iLO

Prerequisites

- Generic LDAP is disabled.

Procedure

1. Click Security in the navigation tree, and then click the Directory tab.
2. Disable Two Factor Authentication.
3. Click Apply Settings.

Running directory tests

About this task

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. Click Security in the navigation tree, and then click the Directory tab.
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.

Subtopics

Directory test input values

Directory test status values and controls

Directory test results

iLO directory tests

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.

NOTE:

- The maximum length for Directory Administrator Distinguished Name and Test User Name is 128 characters.
- The maximum length for Directory Administrator Password and Test User Password is 64 characters.

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 iLO 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.

iLO security states

Production (default)

When iLO is set to this security state:

- iLO uses the factory default encryption settings.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) disables the password requirement for logging in to iLO.
- Remote console data uses AES-128 bidirectional encryption.

High Security

When iLO is set to this security state:

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.

- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

FIPS

The FIPS security state might be required for Common Criteria compliance, Payment Card Industry compliance, or other standards.

When iLO is set to this security state:

- iLO operates in a mode intended to comply with the requirements of FIPS 140-2 level 1.

  FIPS is a set of computer security standards that are mandated for use by United States government agencies and contractors.

  The FIPS security state is not the same as FIPS validated. FIPS validated refers to software that received validation by completing the Cryptographic Module Validation Program.
- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3 .
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

CNSA

The CNSA security state (also called SuiteB mode) is available only when the FIPS security state is enabled.

When iLO is set to this security state:

- iLO operates in a mode intended to comply with the CNSA requirements defined by the NSA.
- iLO operates in a mode intended to secure systems that hold United States government top secret classified data.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.
- Any software or utility that you use to connect to iLO must be CNSA-compliant.

  For example:
  - Firmware update utilities
  - SSH clients
  - HPE and third-party scripting and command-line tools

- HPE and third-party management tools
- AlertMail, syslog, LDAP, or key manager servers
- Remote support software

- Make sure that you use the HTML5 remote console. This console enforces the use of AES-256 bit CNSA-compliant ciphers. The .NET IRC is not CNSA-compliant.

To verify compliance, check with your software vendor or use a utility such as Wireshark.

Synergy Security Mode

A special security state used by Composer 2. You cannot change the security state on a device that uses this mode.

iLO encryption settings

HPE iLO Standard, that comes with every Gen11 server gives customers the ability to configure servers in one of three security states. With an iLO Advanced license, customers that need the highest-level encryption capabilities of CNSA have a fourth security state available to them.

As you move up the scale in security, the server enforces stronger encryption rules for web pages, SSH, and network communications. Note that both ends of each network connection must support the encryption rules, or they cannot communicate, and some interfaces are shut down to limit potential security threats.

The following security states are available:

- Production
- High Security
- FIPS
- CNSA

Subtopics

Enabling the Production security state

Prerequisites

Configure iLO Settings privilege

Procedure

1. (Optional) Install any needed firmware and software updates.
2. Click Security in the navigation tree, and then click the Encryption tab.

   The following Current Settings appears:
   - Negotiated cipher—The negotiated cipher appears.
   - Security State—The selected security state appears.
   - Enabled TLS Versions—The enabled TLS versions appears.
3. In Update Security Settings, select Production in the Security State menu.

   By default, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are enabled in Production mode. TLS 1.3 and TLS 1.2 cannot be disabled in any mode.

   By default, Disable Weak Ciphers is not selected in Production mode.
4. (Optional) You can Disable Weak Ciphers in Production mode. TLS 1.0 and TLS 1.1 are disabled when Disable Weak Ciphers is selected. By default, Disable Weak Ciphers is selected in higher security modes.

   NOTE:
   - Tools that use weak ciphers and key length less than 2048-bit will not be able to connect to iLO when Disable Weak Ciphers is selected.
   - If Disable Weak Ciphers is selected, iLO supports the following SSL ciphers:
     - 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
     - 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
     - 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
     - 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
     - TLS 1.3 256 bits AES GCM with AEAD MAC (TLS AES 256 GCM SHA384)
     - TLS 1.3 128 bits AES GCM with AEAD MAC (TLS AES 128 GCM SHA256)
   - If Disable Weak Ciphers is selected, iLO supports the following SSH ciphers:
     - AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
     - diffie-hellman-group-exchange-sha256 and ecdh-sha2-nistp384 key exchange
     - hmac-sha2-256 or AEAD_AES_256_GCM MACs
5. (Optional) You can disable TLS 1.0, TLS 1.1, or both in Production mode.

   NOTE:
   - TLS versions 1.0 and 1.1 can be enabled or disabled only in Production mode.
   - TLS versions 1.0 and 1.1 are disabled in higher security modes.
   - Tools that do not support TLS 1.3 and TLS 1.2 will not be able to connect to iLO when TLS 1.0 and 1.1 are disabled.
   - TLS versions 1.0, 1.1, and 1.2 supports Extended Master Secret (EMS).
6. Click Apply.

   iLO prompts you to confirm that you want to restart iLO to apply the new settings.

7. To end your browser connection and restart iLO, click Yes, apply and reset.

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

8. Close all open browser windows.

   Any browser sessions that remain open might use the wrong cipher for the configured security state.

More information

Configuring iLO access settings
iLO security states

Enabling the High Security security state

Prerequisites

Configure iLO Settings privilege

Procedure

1. (Optional) Install any needed firmware and software updates.
2. Click Security in the navigation tree, and then click the Encryption tab.

   The following Current Settings appears:
   - Negotiated cipher—The negotiated cipher appears.
   - Security State—The selected security state appears.
   - Enabled TLS Versions—The enabled TLS versions appears.
3. In Update Security Settings, select High Security in the Security State menu.
4. Click Apply.

   iLO prompts you to confirm that you want to restart iLO to apply the new settings.
5. To end your browser connection and restart iLO, click Yes, apply and reset.

   It might take several minutes before you can re-establish a connection.
6. Close all open browser windows.

   Any browser sessions that remain open might use the wrong cipher for the configured security state.
7. Confirm that Anonymous Data is disabled on the Access Settings page.

Enabling the FIPS and CNSA security states

Prerequisites

- Configure iLO Settings privilege
- If you plan to enable the optional CNSA security state, a license that supports this feature is installed.
- The default iLO user credentials are available.

About this task

This procedure is for configuring the FIPS or CNSA security states. To configure iLO in a FIPS-validated environment, see Configuring a FIPS-validated environment with iLO.

HPE ProLiant RL3xx Gen 11 platforms do not support FIPS and CNSA states.

Procedure

1. (Optional) Back up the current iLO configuration.

   You can complete this step by using HPONCFG.

2. (Optional) Install any needed firmware and software updates.

3. Click Security in the navigation tree, and then click the Encryption tab.

   The following Current Settings appears:
   - Negotiated cipher—The negotiated cipher appears.
   - Security State—The selected security state appears.
   - Enabled TLS Versions—The enabled TLS versions appears.

4. In Update Security Settings, select FIPS in the Security State menu, and then click Apply.

   iLO prompts you to confirm the request.

   > **CAUTION:**
   >
   > Enabling the FIPS security state resets iLO to the factory default settings. All iLO settings are erased, including user data and most configuration settings. The iLO Event Log, IML, and Security Log are also erased. Installed license keys are retained.
   >
   > The only way to disable the FIPS security state is to reset iLO to the factory default settings.

5. To confirm the request to enable the FIPS security state, click Yes, apply and reset.

   iLO reboots with the FIPS security state enabled. Wait at least 90 seconds before attempting to re-establish a connection.

6. (Optional) Enable the CNSA security state.

   a. Log in to iLO by using the default user credentials.

   b. Click Security in the navigation tree, and then click the Encryption tab.

      The following Current Settings appears:
      - Negotiated cipher—The negotiated cipher appears.
      - Security State—The selected security state appears.
      - Enabled TLS Versions—The enabled TLS versions appears.

   c. In Update Security Settings, select CNSA in the Security State menu, and then click Apply.

      iLO prompts you to confirm the request.

   d. To confirm the request to enable the CNSA security state, click Yes, apply and reset.

      iLO reboots with the CNSA security state enabled. Wait at least 90 seconds before attempting to re-establish a connection.

   e. Log in to iLO again by using the default iLO credentials.

   If your license expires or is downgraded after you enable the CNSA security state, iLO continues to operate with the configured security state. All other features activated by the expired or downgraded license will be unavailable.

7. Install a trusted certificate.

   The default self-signed SSL certificate is not allowed when the FIPS security state is enabled. Previously installed trusted certificates (either installed through Manual Import or Automatic Certificate Enrollment) are deleted when you set iLO to use the FIPS security state.

8. Disable the IPMI/DCMI over LAN Access, Anonymous Data, 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 Security Policy documents for validated versions of iLO are available on the **NIST website**. To access iLO 6 FIPS information, enter certificate number 3122 on the validated modules search page.

9. (Optional) If you backed up the iLO configuration, restore it.

   You can complete this step by using HPONCFG.

10. (Optional) If you restored the configuration, set new passwords for local iLO user accounts.
11. (Optional) If you restored the configuration, confirm that IPMI/DCMI over LAN Access, Anonymous Data, and SNMP Access are disabled on the Access Settings page.

    These settings might be reset when you restore the configuration.

12. (Optional) Configure the Login Security Banner to inform iLO users that the system is using FIPS security state.

More information

iLO default DNS name and user account
iLO backup and restore
Configuring iLO access settings
Generate CSR and Import an SSL Certificate
Configuring the Login Security Banner

Connecting to iLO when using higher security states

When you enable a security state that is higher than the default value (Production), iLO requires that you connect through secure channels by using an AES cipher.

When iLO is configured to use the CNSA security state, an AES 256 GCM cipher is required.

Web browser

Configure the browser to support TLS 1.2, TLS 1.3, or both and an AES cipher. If the browser is not using an AES cipher, you cannot connect to iLO.

Different browsers use different methods for selecting a negotiated cipher. For more information, see your browser documentation.

Log out of iLO through the current browser before changing the browser cipher setting. Any changes made to the cipher settings while you are logged in to iLO might enable the browser to continue using a non-AES cipher.

SSH connection

For information about setting the available ciphers, see the SSH utility documentation.

RIBCL

- HPQLOCFG displays the cipher details in the output, for example:

  ```
  Detecting iLO...
  Negotiated cipher: 256-bit Aes256 with 0-bit Sha384 and 384-bit 44550
  ```

- HPONCFG requires user credentials when the High Security, FIPS, or CNSA security states are enabled. If you are not assigned the required user privileges, an error message is displayed.

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

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

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

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

iLO RESTful API

Use a utility that supports TLS 1.2, TLS 1.3, or both and an AES cipher.

Configuring a FIPS-validated environment with iLO

About this task

Use the following instructions to operate iLO in a FIPS-validated environment. To use the FIPS security state in iLO, see Enabling the FIPS and CNSA security states.

It is important to decide if a FIPS-validated version of iLO is required for your environment, or if running iLO with the FIPS security state 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.

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 6 FIPS information, enter certificate number 3122 on the validated modules search page.

Disabling the FIPS security state

Procedure

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

   You can perform this task by using RIBCL scripts, the iLO RESTful API or the BMC Configuration Utility.

   CAUTION:

   When you reset iLO to the factory default settings, all iLO settings are erased. The erased settings include user data, license data, configuration settings, and logs. If the server has a factory installed license key, the license key is retained.

   Events related to the reset are not logged because this step clears all the data in the iLO logs.

2. Reboot the server operating system.

   During the reset to the factory default settings, SMBIOS records are cleared. Memory and network information will not be displayed in the iLO web interface until the server OS reboot is complete.

More information

Resetting iLO to the factory default settings (iLO 6 Configuration Utility)

Disabling the CNSA security state

Procedure

1. To disable the CNSA security state, do one of the following:

   - To disable the CNSA security state and continue using the FIPS security state, change the security state from CNSA to FIPS.

- To disable the CNSA and FIPS security states, set iLO to the factory default settings.

  You can perform this task by using the RIBCL scripts, iLO RESTful API, or the iLO 6 Configuration Utility.

  CAUTION:

  When you reset iLO to the factory default settings, all iLO settings are erased. The erased settings include user data, license data, configuration settings, and logs. If the server has a factory installed license key, the license key is retained.

  Events related to the reset are not logged because this step clears all the data in the iLO logs.

2. If you reset iLO to the factory default settings, reboot the server operating system.

   During the reset to the factory default settings, SMBIOS records are cleared. Memory and network information will not be displayed in the iLO web interface until the server OS reboot is complete.

More information

Resetting iLO to the factory default settings (iLO 6 Configuration Utility)

iLO security states

Production (default)

When iLO is set to this security state:

- iLO uses the factory default encryption settings.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) disables the password requirement for logging in to iLO.
- Remote console data uses AES-128 bidirectional encryption.

High Security

When iLO is set to this security state:

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.
- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

FIPS

The FIPS security state might be required for Common Criteria compliance, Payment Card Industry compliance, or other standards.

When iLO is set to this security state:

- iLO operates in a mode intended to comply with the requirements of FIPS 140-2 level 1.

  FIPS is a set of computer security standards that are mandated for use by United States government agencies and contractors.

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

- iLO enforces the use of AES ciphers over the secure channels, including secure HTTP transmissions through the following:
  - Browser
  - SSH port
  - iLO RESTful API
  - RIBCL

  Use a supported cipher to connect to iLO through these secure channels. This security state does not affect communications and connections over less-secure channels.

- User name and password restrictions for the following commands executed from the host system are enforced:
  - iLO RESTful API
  - RIBCL
- Remote console data uses AES-128 bidirectional encryption.
- The HPQLOCFG utility negotiates an SSL connection to iLO and then uses the strongest available cipher to send RIBCL scripts to iLO over the network.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3 .
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.

CNSA

The CNSA security state (also called SuiteB mode) is available only when the FIPS security state is enabled.

When iLO is set to this security state:

- iLO operates in a mode intended to comply with the CNSA requirements defined by the NSA.
- iLO operates in a mode intended to secure systems that hold United States government top secret classified data.
- You cannot connect to the server with network-based tools that do not support TLS 1.2 and TLS 1.3.
- The system maintenance switch setting to bypass iLO security (sometimes called the iLO Security Override switch) does not disable the password requirement for logging in to iLO.
- Any software or utility that you use to connect to iLO must be CNSA-compliant.

  For example:
  - Firmware update utilities
  - SSH clients
  - HPE and third-party scripting and command-line tools
  - HPE and third-party management tools
  - AlertMail, syslog, LDAP, or key manager servers

- Remote support software

- Make sure that you use the HTML5 remote console. This console enforces the use of AES-256 bit CNSA-compliant ciphers. The .NET IRC is not CNSA-compliant.

To verify compliance, check with your software vendor or use a utility such as Wireshark.

Synergy Security Mode

A special security state used by Composer 2. You cannot change the security state on a device that uses this mode.

SSH cipher, key exchange, and MAC support

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

Based on the configured security state, iLO supports the following:

Production

- AES256-CBC, AES128-CBC, 3DES-CBC, AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1 key exchange, and ecdh-sha2-nistp384 key exchange
- hmac-sha1, hmac-sha2-256, and AEAD_AES_256_GCM MACs

FIPS or High Security

- AES256-CTR, AEAD_AES_256_GCM, and AES256-GCM ciphers
- diffie-hellman-group-exchange-sha256 and ecdh-sha2-nistp384 key exchange
- hmac-sha2-256 or AEAD_AES_256_GCM MACs

CNSA

- AEAD_AES_256_GCM and AES256-GCM ciphers
- ecdh-sha2-nistp384 key exchange
- AEAD_AES_256_GCM MAC

Synergy Security Mode

- AEAD_AES_256_GCM and AES256-GCM ciphers
- ecdh-sha2-nistp384 key exchange
- AEAD_AES_256_GCM MAC

SPDM supported algorithms

Based on the configured security state, iLO categorizes the SPDM algorithms as follows:

Production, FIPS, or High Security

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_2048
- TPM_ALG_RSAPSS_2048
- TPM_ALG_RSASSA_3072

- TPM_ALG_RSAPSS_3072
- TPM_ALG_ECDSA_ECC_NIST_P256
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_256
- TPM_ALG_SHA_384
- TPM_ALG_SHA_512

CNSA

BaseAsymAlgo(4)

- TPM_ALG_RSASSA_3072
- TPM_ALG_RSAPSS_3072
- TPM_ALG_RSASSA_4096
- TPM_ALG_ECDSA_ECC_NIST_P384

BaseHashAlgo (4)

- TPM_ALG_SHA_384

SSL cipher and MAC support

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.

When you log in to iLO through a browser, the browser and iLO negotiate a cipher setting to use during the session. The negotiated cipher is displayed on the Encryption page.

The following lists of supported ciphers apply to all iLO SSL connections, including connections to LDAP servers, key manager servers, SSO servers, Insight Remote Support servers, https:// URLs used in virtual media, the iLO RESTful API, CLI commands, and iLO Federation group firmware updates.

Based on the configured security state, iLO supports the following ciphers:

Production

- 256-bit AES-GCM with RSA, ECDH, and an 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 AES-GCM with RSA, DH, and an 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 AES-GCM with RSA, and an 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 AES-GCM with RSA, ECDH, and an 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 AES-GCM with RSA, DH, and an 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 AES-GCM with RSA, and an 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)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

High Security

TLS 1.2 or TLS 1.3 is required for these security states.

- 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

FIPS

TLS 1.2 or TLS 1.3 is required for these security states.

- 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, ECDH, and a SHA384 MAC (ECDHE-RSA-AES256-SHA384)
- 256-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES256-GCM-SHA384)
- 256-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES256-SHA256)
- 128-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, ECDH, and a SHA256 MAC (ECDHE-RSA-AES128-SHA256)
- 128-bit AES-GCM with RSA, DH, and an AEAD MAC (DHE-RSA-AES128-GCM-SHA256)
- 128-bit AES with RSA, DH, and a SHA256 MAC (DHE-RSA-AES128-SHA256)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)
- TLS1.3 128 bits AES_GCM with AEAD MAC (TLS_AES_128_GCM_SHA256)

CNSA

TLS 1.2 or TLS 1.3 is required for this security state.

- 256-bit AES-GCM with ECDSA, ECDH, and an AEAD MAC (ECDHE-ECDSA-AES256-GCM-SHA384)
- Client only: 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)
- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)

Synergy Security Mode

- 256-bit AES-GCM with ECDSA, ECDH, and an AEAD MAC (ECDHE-ECDSA-AES256-GCM-SHA384)
- Client only: 256-bit AES-GCM with RSA, ECDH, and an AEAD MAC (ECDHE-RSA-AES256-GCM-SHA384)

- TLS1.3 256 bits AES_GCM with AEAD MAC (TLS_AES_256_GCM_SHA384)

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.
- Configure iLO to trust the SSO-compliant application.
- Install a trusted certificate if CAC Strict Mode is enabled.

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. iLO supports SSO certificate upto 3 KB in size.

Subtopics

Configuring iLO for HPE SSO

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Security in the navigation tree, and then click the HPE SSO tab.
2. Configure the SSO 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. Click Apply.
5. If you selected Trust by Certificate or Trust by Name, add the trusted certificate or DNS name to iLO.

   For instructions, see Adding trusted certificates or Importing a direct DNS name.
6. (Optional) Log in to your HPE SSO-compliant application and browse to iLO to test the SSO connection.

   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.

   HPE ProLiant RL3xx Gen 11 platforms do not support HPE SIM.

   The list of trusted servers is not used when the SSO Trust Mode is set to Trust None. iLO does not enforce SSO server certificate

revocation.

Subtopics

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, Virtual Media, Host BIOS.
- Administrator—Login, Remote Console, Virtual Power and Reset, Virtual Media, Host BIOS, Configure iLO Settings, Administer User Accounts, Host NIC, and Host Storage.

Adding trusted certificates

Prerequisites

Configure iLO Settings privilege

About this task

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 a specific HPE SSO-compliant application, see the HPE SSO-compliant application documentation.

Procedure

1. Click Security in the navigation tree, and then click the HPE SSO tab.
2. Click Import.

3. 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 in the Direct Import section, and then click Apply.
   - **Indirect import**—Enter the DNS name, IP address, or certificate URL in the text box in the Import From URL section, and then click Apply.

     iLO contacts the HPE SSO-compliant application over the network, retrieves the certificate, and then saves it.

Extracting the HPE SIM SSO certificate

Prerequisites

HPE SIM 7.4 or later

About this task

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

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. Click Security in the navigation tree, and then click the HPE SSO tab.
2. Click Import
3. Enter the DNS name or IP address (up to 64 characters) in the Import Direct DNS Name section, and then click Apply.

Viewing trusted certificates and records

About this task

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

Click Security in the navigation tree, and then click the HPE SSO tab.

Subtopics

Trusted certificate and record details

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 is not compliant with the configured iLO security state or if Disable Weak Ciphers option is enabled in Production mode.
- 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. Click Security in the navigation tree, and then click the HPE SSO tab.
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, delete.

Configuring the Login Security Banner

Prerequisites

Configure iLO Settings privilege

About this task

The Login Security Banner feature allows you to configure the security banner displayed on the iLO web interface and HTML5 standalone remote console login pages. 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.

Procedure

1. Click Security in the navigation tree, and then click Login Security Banner.
2. Enable the Enable Login Security Banner setting.

   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.

System maintenance switch

Hewlett Packard Enterprise servers and compute modules have hardware system maintenance switches, which control different security functions and configurations.

The system maintenance switch is inside the chassis on the system board. To access the switch, you must take the device offline, power down, and remove the access cover.

The following system maintenance switches are off by default. You can set these switches to on when you want to change the product security behavior. The system maintenance switch settings are listed on the access panel label and in the product user guide.

iLO security (position 1)

The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control of the system board.

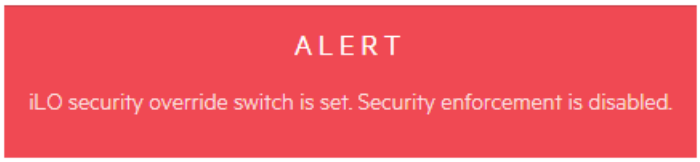
The system maintenance switch position that controls iLO security is sometimes called the iLO Security Override switch.

When this switch is off (default), iLO enforces the configured authentication settings.

Disabling this switch has the following effects:

- When iLO is configured to use the Production security state, all login credential verifications are disabled.

- When iLO is configured to use the High Security, FIPS, or CNSA security state, all login credential verifications are enforced.
- If the host server is reset, the UEFI System Utilities software runs.
- iLO networking, the iLO web interface, and the ROM-based system utility are accessible even if they were previously disabled.
- The System Recovery privilege is enforced. To perform an action that requires this privilege, you must authenticate with a user account that has the privilege enabled.
- 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.

For more information, see the maintenance and service guide for your product.

Subtopics

Reasons to disable iLO security

Reasons to disable iLO security

You might want to use the system maintenance switch to disable iLO security in the following situations:

- 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.
- 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 UEFI System Utilities 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.
  - On servers with the iLO network enablement module, this action enables DHCP and the iLO Dedicated 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.

Configuring iLO management settings

Subtopics

Agentless Management and AMS

Agentless Management and AMS

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.

To collect information from devices and components that cannot communicate directly with iLO, install the Agentless Management Service (AMS).

Information provided by Agentless Management with and without AMS

Component	Agentless Management without AMS	Additional information provided when AMS is installed
Server health	• Fans • Temperatures • Power supplies • Memory • CPU • NVDIMM	N/A
Storage	• Smart Array • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array • Smart Storage Energy Pack monitoring (supported servers only) • NVMe drives that support MCTP	• SMART Drive Monitoring • iSCSI (Windows) • NVMe drives
Network	• MAC addresses for embedded NICs that support NC-SI over MCTP • Physical link connectivity and link up/link down traps for NICs that support NC-SI over MCTP • Fibre Channel adapters that support Hewlett Packard Enterprise vendor-defined MCTP commands	• MAC and IP address for standup and embedded NICs • Link up/link down traps • NIC teaming and bridging information (Windows and Linux) • Supported Fibre Channel adapters • VLAN information (Windows and Linux)
Other	• iLO data • Firmware inventory • Device inventory	• OS information (host SNMP MIB) • Driver/service inventory • Logging events to OS logs [1], [2], [3]
Prefailure warranty alerts	• Memory • Drives (physical and logical)	N/A

1 AMS-based OS logging for Linux (/var/log/messages for Red Hat Enterprise Linux and SUSE Linux Enterprise Server and /var/log/syslog for VMware.
Windows System Log for Windows.
2 Smart Array logging is supported.
3 IML and Security Log events are included in the OS logs for Gen11 servers.

Agentless Management Service

- 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 drivers before installing AMS.
- With iLO 6, AMS includes the optional System Management Assistant. You can use the System Management Assistant if you want to use an OS-based SNMP service to handle information provided by iLO Agentless Management and AMS.
- If AMS is not installed:
  - iLO does not display a full set of data on the component information pages, which are included in the System Information and Firmware & OS Software sections of the navigation tree.
  - iLO does not have access to OS-specific information.

Subtopics

Installing AMS

Verifying AMS installation

Restarting AMS

System Management Assistant

More information

Installing the iLO drivers
System Management Assistant

Installing AMS

Procedure

1. Obtain AMS from one of the following sources:
   - Download the SPP (Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise Server) from the SPP download page at **https://www.hpe.com/servers/spp/download**.
   - Download the software from the Hewlett Packard Enterprise Support Center (Windows, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware) at **https://www.hpe.com/support/hpesc**.
   - Download the software from the vibsdepot section of the Software Delivery Repository website at **https://vibsdepot.hpe.com** (VMware).

     AMS is also included in the customized Hewlett Packard Enterprise VMware ISO images (**https://www.hpe.com/info/esxidownload**).
2. Install the software.

   For instructions on using the SPP, see the SPP documentation at **https://www.hpe.com/info/spp/documentation**.

   For other download types, follow the installation instructions provided with the software.

Verifying AMS installation

Subtopics

Verifying AMS status: iLO web interface

Verifying AMS status: Windows

Verifying AMS status: SUSE Linux Enterprise Server and Red Hat Enterprise Linux

Verifying AMS status: VMware

Verifying AMS status: Ubuntu

Verifying AMS status: iLO web interface

Procedure

Click System Information in the navigation tree.

AMS is listed in the Subsystems and Devices table on the Health Summary page. 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 amsd`.
2. To verify that AMS is running, enter the following command: `systemctl status amsd smad [cpqIde cpqFca cpqScsi cpqiScsi mr_cpqScsi]`.

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 `amsd`.

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/ams.sh status`.

Verifying AMS status: Ubuntu

Procedure

1. To verify that AMS is installed, enter the following command: `dpkg -l amsd`.
2. To verify that AMS is running, enter the following command: `sudo systemctl status smad; systemctl status amsd`.

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: `systemctl restart amsd smad`.
- **VMware**— Enter the following commands:
  - **For ESXi 6.x and 7.0:** `/etc/init.d/amsd.sh restart`
  - **For ESXi 7.0 U1 and later:** `esxcli daemon control restart -s amsd`

System Management Assistant

iLO 6 does not support OS-based SNMP agents. The System Management Assistant (SMA) is an Agentless Management Service feature for users who want to run applications that obtain SNMP information from the OS.

Security

SMA communicates over secure iLO channels.

AMS modes

- **AMS (forward mode)**—The standard configuration of AMS is to pass information from the OS to iLO.
- **SMA (reverse mode)**—When SMA is enabled, information is passed from iLO to the OS.

Installation

SMA is installed as part of the AMS package, and it is disabled by default.

Enabling SMA

Use the default AMS configuration to pass information from the OS to iLO. Enable SMA to pass information from iLO to the OS. The standard configuration of AMS and SMA can be enabled at the same time.

SMA functionality

When SMA is enabled, it does the following:

- **Linux**—Proxies AgentX protocol requests between iLO and a host-based SNMP master.
- **Windows, Linux**—Proxies SNMP protocol requests between iLO and a host-based SNMP service.

  This method is used when the host-based SNMP service does not support AgentX subagents.

- **VMware**—Delivers SNMP traps from iLO and AMS to the trap destination configured through the ESXi host OS SNMP service.

SNMP master

With the default AMS configuration, AMS uses iLO as the SNMP master. SMA requires a host-based service to act as the SNMP master.

Information provided when SMA is enabled

- **Windows and Linux**—SMA provides the same information that is listed in the Agentless Management with AMS column in the Information provided by Agentless Management with and without AMS table.
- **VMware**—SMA provides only SNMP traps.

Subtopics

Using the System Management Assistant (Windows)

Prerequisites

AMS is installed.

About this task

You can choose whether to enable the SMA during an interactive AMS installation, and the SMA is not enabled during a silent installation.

To use SMA, start the SMA service and verify that the Windows SNMP service is installed and configured.

Procedure

1. Install the Windows SNMP service.
   a. Open Server Manager.
   b. Select Add roles and features.
   c. Click Next in the Before You Begin section.
   d. Click Next in Installation Type section.
   e. Click Next in Server Selection section.
   f. Click Next in Server Roles section.
   g. Expand the Remote Server Administration section.
   h. Expand Feature Administration Tools
   i. Ensure that SNMP Tools is selected.
   j. Select the check box to the left of the SNMP Service option.
   k. Click Next.
   l. Click Install and wait for the installation to complete.
2. Configure the Windows SNMP service.

a. Navigate to the Windows Services window.

b. Right-click the SNMP service.

c. Click the Security tab.

d. Click Add in the Accepted Community Names section.

e. Select an access type in the Community Rights section.

f. Enter a community name in the Community Name section.

g. Click Add.

h. Click the Traps tab.

i. Enter a community name in the Community Name section, and then click Add to list.

j. In the Trap Destination section, click Add, and then enter the IP address of a trap destination.

k. Click OK.

3. Start the SMA service.

a. Navigate to the Windows Services window.

b. Right-click the System Management Assistant, and then select Properties.

c. Select Automatic in the Startup type menu, and then click OK.

d. Right-click the System Management Assistant, and then select Start.

NOTE:

You can also start the SMA service by:

- Navigating to `<Program Files>\OEM\AMS\Service` and then running the following command: `EnableSma.bat /f`
- Entering the following commands in a command prompt window: **`sc config sma start=auto`** and **`net start sma`**

Disabling the System Management Assistant (Windows)

Procedure

1. Navigate to the Windows Services window.
2. Right-click the System Management Assistant, and then select Properties.
3. Select Disabled in the Startup type menu, and then click OK.
4. Right-click the System Management Assistant, and then select Stop.

NOTE:

You can also disable the SMA service by navigating to `<Program Files>\OEM\AMS\Service` and then running the following command `DisableSma.bat /f`

Using the System Management Assistant for VMware

Prerequisites

AMS is installed.

Procedure

1. Enable SNMP on the host and specify a trap destination.

   For example:

   ```
   esxcli system snmp set -e 1 -c public -t <trap dest IP address>@162/public
   ```

2. Enter the following command to verify that SNMP is enabled:

   ```
   esxcli system snmp get
   ```

3. Enter the following command to enable and start SMA:

   ```
   esxcli sma enable
   ```

4. Enter the following command to verify that SMA is running:

   ```
   esxcli sma status
   ```

5. Verify that the SMA process (`smad_rev`) is running.

Disabling the System Management Assistant (VMware)

Procedure

Run the following command: `esxcli sma disable`.

Using the System Management Assistant for Linux

Prerequisites

- AMS is installed.
- The host SNMP service is configured.
- The network is configured to pass SNMP packets between the host and the SNMP clients.

Procedure

1. Configure the host to support AgentX subagents by adding the following line as the first noncomment line in the `/etc/snmp/snmpd.conf` file:

   ```
   master agentx
   ```

2. Enable the System Management Assistant.
   - **SUSE Linux Enterprise Server and Red Hat Enterprise Linux** —Enter the following command: `systemctl enable amsd_rev`.
3. Enable and start the Agentless Management Service.
   - **SUSE Linux Enterprise Server and Red Hat Enterprise Linux** —Enter the following command: **`systemctl enable amsd_rev; systemctl start amsd_rev`**.

Configuring SNMP alerts

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. In the SNMP Alerts section, configure the Trap Source Identifier by selecting iLO Hostname or OS Hostname.

3. Configure the following values:

   - SNMPv1 Request
   - SNMPv1 Trap
   - SNMPv3 Request
   - SNMPv3 Trap
   - Cold Start Trap Broadcast
   - Periodic HSA Trap Configuration

4. (Optional) To generate a test alert and send it to the configured SNMP Alert Destinations, click Send Test Alert. This option is disabled if both SNMPv1 Trap and SNMPv3 Trap are disabled.

   Test alerts are used to verify the network connectivity of iLO with the configured SNMP Alert Destination addresses. After the alert is generated, check the alert destination for receipt of the alert.

5. To save the configuration, click Apply.

Subtopics

SNMP alert settings

SNMP alert settings

Trap Source Identifier

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

The host name is an OS construct. 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.

SNMPv1 Request

Enables iLO to receive external SNMPv1 requests.

SNMPv1 Trap

Enables iLO to send SNMPv1 traps to the remote management systems configured in the alert destination.

SNMPv3 Request

Enables iLO to receive external SNMPv3 requests.

SNMPv3 Trap

Enables iLO to send SNMPv3 traps to the remote management systems configured in the alert destination.

Cold Start Trap Broadcast

The Cold Start Trap is broadcast to a subnet broadcast address when any of the following conditions is met:

- SNMP Alert Destinations are not configured.
- SNMP Alert Destinations are configured, but the SNMP protocol is disabled.
- 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`.

Periodic HSA Trap Configuration

In the default configuration, iLO sends the health status array (HSA) trap only when a component status changes (for example, the fan status changed to failed).

You can configure iLO to send the HSA trap periodically (daily, weekly, or monthly) when a supported component is in a failed or degraded state. This setting is disabled by default.

Configuring SNMPv3 settings

Prerequisites

Configure iLO Settings privilege

About this task

Use the SNMPv3 Settings section to configure the SNMPv3 Engine ID and the SNMPv3 Inform settings.

iLO supports the industry standard SNMPv3 Inform feature. When an SNMPv3 Inform notification is sent, it is saved and sent again at regular intervals until the receiver sends an acknowledgment to iLO, or the maximum number of retries is reached.

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. Enter a value in the SNMPv3 Engine ID box.

   If you do not want to specify a value, you can leave this box blank.

3. To configure the SNMPv3 Inform settings, enter the following values:
   - SNMPv3 Inform Retry
   - SNMPv3 Inform Time Interval
4. Click Apply.

Subtopics

SNMPv3 Settings options

SNMPv3 Settings options

SNMPv3 Engine ID

The unique identifier of an SNMP engine belonging to an SNMP agent entity.

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.

SNMPv3 Inform Retry

The number of times iLO will resend an alert if the receiver does not send an acknowledgment to iLO.

Enter a value from 0 to 5. The default value is 2.

SNMP Inform Time Interval

The number of seconds between attempts to resend an SNMPv3 Inform alert.

Enter a value from 5 to 120 seconds. The default value is 15 seconds.

Configuring SNMP settings

Prerequisites

Configure iLO Settings privilege

About this task

The settings you configure on this page are for the default Agentless Management and AMS configuration. If you use the System Management Assistant and an OS-based SNMP service, similar settings must be configured on the host.

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. Enter the following values in the SNMP Settings section:

   - System Location
   - System Contact
   - System Role
   - System Role Detail
   - Read Community 1
   - Read Community 2
   - Read Community 3

   The SNMP Port and SNMP Status values are read-only on this page. You can change these values on the Access Settings page.

3. To save the configuration, click Apply.

Subtopics

SNMP options

More information

System Management Assistant
Configuring iLO access settings

SNMP options

- 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 1, Read Community 2, and Read Community 3 —The configured SNMP read-only community strings.

  The following formats are supported:

  - 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.

    You can enter an IPv4 address, an IPv6 address, or an FQDN.

  These values can be edited only if SNMPv1 Request is enabled in the SNMP Alerts section.
- Status—The status of the SNMP access setting (Enabled or Disabled). This value is read-only, but can be modified on the Access Settings page.

  To navigate to the Access Settings page, click the Status link.
- SNMP Port—The port used for SNMP communications. This value is read-only, but can be modified on the Access Settings page.

  To navigate to the Access Settings page, click the SNMP Port link.

Adding SNMP Alert Destinations

Prerequisites

- Configure iLO Settings privilege
- SNMPv1 Trap is enabled if you want to configure SNMPv1 alert destinations.
- SNMPv3 Trap is enabled and at least one SNMPv3 user is configured if you want to configure SNMPv3 alert destinations.

About this task

iLO supports up to eight SNMP alert destinations.

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.
2. Click New in the SNMP Alert Destinations section.
3. Enter the following values:
   - SNMP Alert Destination
   - Trap Community (SNMPv1 alert destinations only)
   - SNMP Protocol
   - SNMPv3 User
4. Click Add.

Subtopics

SNMP alert destination options

SNMP alert destination options

- SNMP Alert Destination—The IP address or FQDN of a management system that will receive SNMP alerts from iLO. This value can be up to 255 characters.

  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 enabled, traps will be sent to IPv6 addresses (when available). When iLO Client Applications use IPv6 first is disabled, traps will be sent to IPv4 addresses (when available).

- Trap Community—The configured SNMP trap community string.
- SNMP Protocol—The SNMP protocol to use with the configured alert destination (SNMPv1 Trap, SNMPv3 Trap, or SNMPv3 Inform).

  The SNMPv1 Trap option is available when SNMPv1 Trap is enabled in the SNMP Alerts section.

  The SNMPv3 Trap option is available when SNMPv3 Trap is enabled in the SNMP Alerts section and at least one SNMPv3 user is configured.

  The SNMPv3 Inform option is available when at least one SNMPv3 user is configured.

- SNMPv3 User—The SNMPv3 User to associate with the configured alert destination.

  This value is available only if the SNMP Protocol is set to SNMPv3 Trap or SNMPv3 Inform.

Editing SNMP Alert Destinations

Prerequisites

- Configure iLO Settings privilege
- SNMPv1 Trap option is enabled in the SNMP Alerts section, if you want to change an alert destination to use the SNMPv1 Trap protocol option.
- SNMPv3 Trap option is enabled in the SNMP Alerts section, and at least one SNMPv3 user is configured if you want to change an alert destination to use the SNMPv3 Trap protocol option.
- At least one SNMPv3 user is configured if you want to change an alert destination to use the SNMPv3 Inform protocol option.

About this task

iLO supports up to eight SNMP alert destinations.

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. Select the check box next to an alert destination in the SNMP Alert Destinations section, and then click Edit.
3. Update the following values:
   - SNMP Alert Destination
   - Trap Community (SNMPv1 alert destinations only)
   - SNMP Protocol
   - SNMPv3 User
4. Click Update.

Deleting an SNMP alert destination

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. In the SNMP Alert Destinations section, select the check box next to the SNMP alert destination that you want to delete, and then click Delete.

3. When prompted to confirm the request, click Yes, delete.

SNMPv3 authentication

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 eight user profiles in which you can set the SNMPv3 USM parameters.

Configuring SNMPv3 users

Prerequisites

Configure iLO Settings privilege

About this task

iLO supports up to eight SNMPv3 users.

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. In the SNMPv3 Users section, do one of the following:

   - To add an SNMPv3 user, click New.
   - To edit a configured SNMPv3 user, select the check box next to the user, and then click Edit.

3. Enter the following values:

   - Security Name

- Authentication Protocol
- Authentication Passphrase
- Privacy Protocol
- Privacy Passphrase
- User Engine ID

4. To save the user profile, do one of the following:
   - To save a new user profile, click Add.
   - To save an edited user profile, click Update.

Subtopics

SNMPv3 user options

SNMPv3 user options

- Security Name—The user profile name. Enter an alphanumeric string of 1 to 32 characters.
- Authentication Protocol—Sets the message digest algorithm to use for encoding the authorization passphrase. The message digest is calculated over an appropriate portion of an SNMP message, and is included as part of the message sent to the recipient.

  Select MD5, SHA, or SHA256.

  If iLO is configured to use the FIPS or CNSA security state, MD5 is not supported.
- 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.

  If iLO is configured to use the FIPS or CNSA security state, DES is not supported.
- Privacy Passphrase—Sets the passphrase used for encrypt operations. Enter a value of 8 to 49 characters.
- User Engine ID—Sets the user engine ID for SNMPv3 Inform packets. This value is used only for creating remote accounts used with INFORM messages.

  If this value is not set, INFORM messages are sent with the default value or the configured SNMPv3 Engine ID.

  This value must be a hexadecimal string with an even number of 10 to 64 characters, excluding the first two characters, 0x.

  For example: `0x01020304abcdef`

Deleting an SNMPv3 user

Prerequisites

Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree.

   The SNMP Settings page is displayed.

2. In the SNMPv3 Users section, select the check box next to the user profile that you want to delete, and then click Delete.

> **CAUTION:**
>
> If the selected SNMPv3 user profile is configured for an SNMP alert destination, the alert will not be sent after you delete the user profile.

3. When prompted to confirm the request, click Yes, delete.

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 (with the corresponding Integrated Management Log or iLO Event Log class and code) that are supported by iLO 6 and supported ProLiant servers.

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

To view troubleshooting information for an event, match the event class and code with the values in the IML messages and troubleshooting guide, at the following website: **https://www.hpe.com/support/ilo-docs**.

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
0	N/A	N/A	`Cold Start Trap` SNMP was initialized, the system completed POST, or AMS started.	N/A
4	N/A	N/A	`Authentication Failure Trap` SNMP detected an authentication failure.	N/A
1006	5h	3h	`cpqSeCpuStatusChange` An uncorrectable machine check exception was detected in a processor.	Major
1010	28h	2h	`cpqSeUSBStorageDeviceReadErrorOccurred` A read error occurred on an attached USB storage device.	OK
1011	28h	3h	`cpqSeUSBStorageDeviceWriteErrorOccurred` A write error occurred on an attached USB storage device.	OK

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
1012	28h	4h	`cpqSeUSBStorageDeviceRedundancyLost` USB storage device redundancy was lost.	Warning
1013	28h	4h	`cpqSeUSBStorageDeviceRedundancyRestored` USB storage device redundancy was restored.	OK
1014	28h	5h	`cpqSeUSBStorageDeviceSyncFailed` The sync operation to restore USB storage device redundancy failed.	Warning
1015	33h	5h	`cpqSePCIeDiskTemperatureFailed` The PCIe disk temperature crossed the upper critical threshold.	Critical
1016	33h	5h	`cpqSePCIeDiskTemperatureOk` The PCIe disk temperature is normal.	OK
1017	33h	2h	`cpqSePCIeDiskConditionChange` The PCIe disk status changed.	Critical
1018	33h	3h	`cpqSePCIeDiskWearStatusChange` The PCIe disk wear status changed.	Critical
1019	33h	4h	`cpqSePciDeviceAddedOrPoweredOn` A PCI device was added or powered on.	OK
1020	33h	5h	`cpqSePciDeviceRemovedOrPoweredOff` A PCI device was removed or powered off.	OK
1021	Ah	3152h	`cpqSeNVMeSecureEraseFailed` Secure Erase of NVMe drive failed.	Critical
1022	32h	3020h 3021h	`cpqSePcieTrainingFailed` PCI Express slot failed to train.	Critical
1023	Ah	3158h	`cpqSePciResetFail` The system is unable to perform a reset on the PCI controller in a slot.	Critical
2014	2h	2Dh	`cpqSiIntrusionInstalled` System intrusion hardware installed.	OK
2015	2h	2Eh	`cpqSiIntrusionRemoved` System intrusion hardware removed.	OK
2016	2h	30h	`cpqSiHoodReplaced` System hood replaced.	OK
2017	Ah	401h	`cpqSiHoodRemovedOnPowerOff` System hood removed when server power was off.	Major
2018	35h	1h	`cpqSiSysTelemetryThresholdAlert` The system telemetry metric value exceeded the upper threshold or is lower than the lower threshold.	Informational

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
3033	13h	12h	`cpqDa6CntlrStatusChange` Smart Array controller status change detected.	Critical
3034	13h	21h	`cpqDa6LogDrvStatusChange` Smart Array logical drive status change detected.	Critical
3038	13h	17h	`cpqDa6AccelStatusChange` Smart Array cache module status change detected.	Critical
3039	13h	23h	`cpqDa6AccelBadDataTrap` The Smart Array cache module lost backup power.	Critical
3040	13h	24h	`cpqDa6AccelBatteryFailed` The Smart Array cache module backup power failed.	Critical
3046	13h	14h	`cpqDa7PhyDrvStatusChange` Smart Array physical drive status change detected.	Critical
3047	13h	2Ch	`cpqDa7SpareStatusChange` Smart Array spare drive status change detected.	Critical
3049	13h	15h	`cpqDaPhyDrvSSDWearStatusChange` Smart Array physical drive SSD wear status change detected.	Critical
3903	Ah	3151h	`cpqDaSmartArraySecureEraseFailed` Secure Erase of Smart Array failed.	Critical
5022	13h	1Eh	`cpqSasPhyDrvStatusChange` AMS detected a change in the status of an SAS or SATA physical drive.	Critical
5026	13h	1Fh	`cpqSasPhyDrvSSDWearStatusChange` AMS detected a change in the SSD wear status of an SAS or SATA physical drive.	Critical
6026	2h	38h	`cpqHe3ThermalConfirmation` The server was shut down due to a thermal anomaly and is now operational.	OK
6027	Ah	101h	`cpqHe3PostError` One or more POST errors occurred.	Warning
6032	Bh	36h	`cpqHe3FltTolPowerRedundancyLost` The fault-tolerant power supplies lost redundancy for the specified chassis.	Major
6033	Bh	31h	`cpqHe3FltTolPowerSupplyInserted` A fault-tolerant power supply was inserted.	OK
6034	Bh	2Ch	`cpqHe3FltTolPowerSupplyRemoved` A fault-tolerant power supply was removed.	Major

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
6035	2h	1Ah	`cpqHe3FltTolFanDegraded` The fault-tolerant fan condition was set to Degraded.	Critical
6036	2h	17h	`cpqHe3FltTolFanFailed` The fault-tolerant fan condition was set to Failed.	Critical
6037	2h	23h	`cpqHe3FltTolFanRedundancyLost` The fault-tolerant fans lost redundancy.	Major
6038	2h	1Fh	`cpqHe3FltTolFanInserted` A fault-tolerant fan was inserted.	OK
6039	2h	1Bh	`cpqHe3FltTolFanRemoved` A fault-tolerant fan was removed.	Major
6040	2h	27h	`cpqHe3TemperatureFailed` Temperature exceeded on the server.	Critical
6041	2h	14h	`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.	Critical
6042	2h	13h	`cpqHe3TemperatureOk` The temperature status was set to OK.	OK
6048	Bh	28h	`cpqHe4FltTolPowerSupplyOk` The fault-tolerant power supply condition was set to OK.	OK
6049	Bh	15h	`cpqHe4FltTolPowerSupplyDegraded` The fault-tolerant power supply condition was set to Degraded.	Critical
6050	Bh	28h	`cpqHe4FltTolPowerSupplyFailed` The fault-tolerant power supply condition was set to Failed.	Critical
6051	N/A	N/A	`cpqHeResilientMemMirroredMemoryEngaged` The Advanced Memory Protection subsystem detected a memory fault. Mirrored Memory was activated.	Major
6054	Bh	36h	`cpqHe3FltTolPowerRedundancyRestore` The fault-tolerant power supplies returned to a redundant state.	OK
6055	2h	23h	`cpqHe3FltTolFanRedundancyRestored` The fault-tolerant fans returned to a redundant state.	OK
6061	N/A	N/A	`cpqHeManagementProcInReset` The management processor is resetting.	Minor
6062	N/A	N/A	`cpqHeManagementProcReady` The management processor is ready.	Informational
6064	N/A	N/A	`cpqHe5CorrMemReplaceMemModule` Memory errors were corrected. Replace the memory module.	Major

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
6069	Bh	52h	`cpqHe4FltTolPowerSupplyACpowerloss` The fault-tolerant power supply in the specified chassis and bay reported AC power loss.	Critical
6070	Bh	3Eh	`cpqHeSysBatteryFailed` The HPE Smart Storage Battery failed.	Warning
6071	Bh	1Eh	`cpqHeSysBatteryRemoved` The HPE Smart Storage Battery was removed.	Warning
6072	27h	4h	`cpqHeSysPwrAllocationNotOptimized` iLO could not determine the power requirements. The server power allocation is not optimized.	Warning
6073	Bh	24h	`cpqHeSysPwrOnDenied` The server could not power on because the hardware cannot be identified.	Critical
6074	14h	7h	`cpqHePowerFailureError` A device power failure was detected.	Critical
6075	29h	1h	`cpqHeInterlockFailureError` A device is missing or improperly seated on the system board.	Critical
6076	Ah	340h	`cpqHeNvdimmBackupError` An NVDIMM backup error was detected.	Critical
6077	Ah	341h	`cpqHeNvdimmRestoreError` An NVDIMM restore error was detected.	Critical
6078	Ah	342h	`cpqHeNvdimmUncorrectableMemoryError` An uncorrectable memory error was detected.	Critical
6079	Ah	343h	`cpqHeNvdimmBackupPowerError` An NVDIMM backup power error occurred. Backup power is not available and a future backup is not possible.	Critical
6080	Ah	344h	`cpqHeNvdimmNVDIMMControllerError` An NVDIMM controller error occurred and the OS will not use the NVDIMM.	Critical
6081	Ah	345h	`cpqHeNvdimmEraseError` An NVDIMM could not be erased and future backups are not possible.	Critical
6082	Ah	346h	`cpqHeNvdimmArmingError` An NVDIMM could not be armed and future backups are not possible.	Critical
6083	Ah	355h	`cpqHeNvdimmSanitizationOk` This NVDIMM-N was selected for sanitizing/erasing. All data saved in the NVDIMM was erased.	OK

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
6084	Ah	356h	`cpqHeNvdimmSanitizationError` This NVDIMM-N was selected for sanitizing/erasing, but the process was unsuccessful.	Critical
6085	Ah	364h	`cpqHeNvdimmControllerFirmwareError` An NVDIMM controller firmware error occurred. The controller firmware is corrupted and the OS will not use the NVDIMM.	Critical
6086	Ah	374h	`cpqHeNvdimmErrorInterleaveOn` A memory initialization or uncorrectable error occurred. All NVDIMMs on the processor are disabled.	Critical
6087	Ah	375h	`cpqHeNvdimmInterleaveOff` A memory initialization or uncorrectable error occurred. NVDIMM is disabled.	Critical
6088	Ah	394h	`cpqHeNvdimmEventNotifyError` Unable to set event notification for this NVDIMM.	Critical
6089	Ah	395h	`cpqHeNvdimmPersistencyLost` NVDIMM persistency is lost and future data backup is not available.	Critical
6090	Ah	396h	`cpqHeNvdimmPersistencyRestored` NVDIMM persistency is restored and future data backup is available.	Informational
6091	Ah	397h	`cpqHeNvdimmLifecycleWarning` NVDIMM life cycle warning. The NVDIMM lifetime is reached.	Major
6092	Ah	430h	`cpqHeNvdimmLogicalNvdimmError` Logical NVDIMM errors occurred.	Major
6093	Ah	354h	`cpqHeNvdimmConfigurationError` NVDIMM configuration errors occurred.	Critical
6094	Ah	351h	`cpqHeNvdimmBatteryNotChargedwithWait` The smart battery is not sufficiently charged to support the installed NVDIMMs.	OK
6095	Ah	352h	`cpqHeNvdimmBatteryNotChargedwithNoWait` Smart battery is not sufficiently charged to support the installed NVDIMMs.	OK
6096	Ah	388h	`cpqHeDimmMemoryMapChanged` Uncorrectable Memory Error—The failed memory module could not be determined.	Warning
6098	Ah	483h	`cpqHeNvdimmInitializationError` One or more NVDIMMs cannot be initialized due to an internal error.	Warning
6099	Bh	54h	`cpqHePwrSupplyError` A system power supply error occurred.	Warning

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
6100	Bh	54h	`cpqHePwrSupplyErrorRepaired` A system power supply error was repaired.	OK
6101	Bh	55h	`cpqHeBbuError` A battery backup unit error occurred.	Warning
6102	Bh	55h	`cpqHeBbuErrorRepaired` A battery backup unit error was repaired.	OK
6103	Bh	1Ch	`cpqHeNoPowerSupplyDetected` No power supply or power backplane was detected.	Major
6104	Bh	1Bh	`cpqHePowerProtectionFault` A system board power protection fault occurred.	Critical
6105	14h	9h	`cpqHePowerFuseDegraded` A degraded power event was detected and the server system board should be replaced.	Critical
6106	Ah	3134h	`cpqHeTPMSecureEraseFailed` Secure Erase of Trusted Platform Module failed.	Critical
6107	Ah	3140h	`cpqHeSPISecureEraseFailed` Secure Erase of system firmware configuration failed.	Critical
6109	28h	6h	`cpqHeNANDSecureEraseFailed` Secure Erase of the management processor embedded media device failed.	Critical
6110	Ah	3143h 3145h 3146h	`cpqHeSedPassphrasefail` Device encryption error. Enabling or disabling encryption or modifying passphrase failed.	Critical
6111	Ah	3148h	`cpqHeSedUnlockfail` Three incorrect attempts were made to unlock a self-encrypting device. The device will be locked until the next reboot.	Major
6116	0xA	0x460	`cpqHePMMCorrErrThreshold` Correctable memory error threshold exceeded	Major
6118	2h	39h	`cpqHeInletAmbientPreCautionThresAlert` The Inlet Ambient sensor reading equals or exceeds the user defined value.	Minor
6119	0x2	0x3C	`cpqHeCoolingModuleDegraded` The cooling module condition was set to degraded for the specified chassis.	Major
6120	0x2	0x3B	`cpqHeCoolingModuleFailed` The cooling module condition was set to failed for the specified chassis.	Critical

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
6121	0x2	0x3D	`cpqHeCoolingModuleRedundancyLost` The cooling module lost redundancy for the specified chassis.	Major
6122	0x2	0x3D	`cpqHeCoolingModuleRedundancyRestored` The cooling module returned to a redundant state for the specified chassis.	Informational
6123	0xB	0x90	`cpqHeUnsupportedPwrSupplyDetected` Unsupported power supply configuration.	Critical
6124	0xB	0x90	`cpqHeUnSupportedPwrSupplyRemoved` Unsupported power supply removed.	Informational
6125	0x2	0x3F	`cpqHeUserTempThreshWarning` User defined caution temperature threshold exceeded.	Minor
6126	0x2	0x40	`cpqHeUserTempThreshCritical` User defined critical temperature threshold exceeded.	Critical
8029	13h	28h	`cpqSs6FanStatusChange` The storage enclosure fan status changed.	Critical
8030	13h	29h	`cpqSs6TempStatusChange` The storage enclosure temperature status changed.	Critical
8031	13h	2Ah	`cpqSs6PwrSupplyStatusChange` The storage enclosure power status changed.	Critical
8032	13h	2Bh	`cpqSsConnectionStatusChange` The storage enclosure status changed.	Critical
9001	23h	5h	`cpqSm2ServerReset` The server power was reset.	Critical
9003	23h	1100h	`cpqSm2UnauthorizedLoginAttempts` The maximum unauthorized login attempt threshold was exceeded.	Informational
9005	23h	1101h	`cpqSm2SelfTestError` iLO detected a self-test error.	Critical
9012	23h	104h	`cpqSm2SecurityOverrideEngaged` iLO detected that the security override jumper was toggled to the engaged position.	Informational
9013	23h	105h	`cpqSm2SecurityOverrideDisengaged` iLO detected that the security override jumper was toggled to the disengaged position.	Informational
9017	23h	3h	`cpqSm2ServerPowerOn` The server was powered on.	OK

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
9018	23h	1h	`cpqSm2ServerPowerOff` The server was powered off.	OK
9019	23h	1102h	`cpqSm2ServerPowerOnFailure` A power-on request occurred, but the server could not be powered on because of a failure condition.	Critical
9020	23h	1138h	`cpqSm2IrsCommFailure` Communication with Insight Remote Support failed.	Warning
9021	32h	3h	`cpqSm2FirmwareValidationScanFailed` Firmware validation failure (iLO, IE, or SPS firmware).	Critical
9022	32h	3h	`cpqSm2FirmwareValidationScanErrorRepaired` A reported firmware integrity scan issue was repaired.	OK
9023	32h	4h	`cpqSm2FirmwareValidationAutoRepairFailed` Firmware recovery failed.	Warning
9024	14h	2h	`cpqSm2AutoShutdownInitiated` iLO initiated an automatic operating system shutdown.	Major
9025	14h	2h	`cpqSm2AutoShutdownCancelled` An automatic operating system shutdown was canceled.	OK
9026	23h	448h	`cpqSm2FwUpdateUploadFailed` A firmware update or upload failed.	Warning
9027	23h	464h	`cpqSm2SecurityStateChange` The iLO security state changed.	OK
9028	23h	B3h	`cpqSm2WDTimerReset` iLO detected a watchdog timer timeout. The failsafe timer was not periodically addressed after it was armed in the operating system.	Major
9029	23h	491h	`cpqSm2OverallSecStateAtRisk` System security state at risk.	Major
9030	23h	490h	`cpqSm2OverallSecStatusChange` Overall security status changed.	Major
11003	1h	1h	`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.	Informational
11018	23h	CEh	`cpqHo2PowerThresholdTrap` A power threshold was exceeded.	Major
11020	N/A	N/A	`cpqHoMibHealthStatusArrayChangeTrap` A server health status change occurred.	N/A

Trap ID	Event Class	Event Code	Trap name and Description	Trap Severity
14004	13h	20h	`cpqIdeAtaDiskStatusChange` AMS detected an ATA disk drive status change.	Critical
14007	Ah	3150h	`cpqIdeAtaSecureEraseFailed` Secure erase of SATA drive failed.	Critical
16028	11h	Bh	`cpqFca3HostCntlrStatusChange` AMS detected a Fibre Channel host controller status change.	Critical
18011	11h	Ah	`cpqNic3ConnectivityRestored` Connectivity was restored to a logical network adapter.	OK
18012	11h	Ah	`cpqNic3ConnectivityLost` The status of a logical network adapter changed to Failed.	Warning
18013	11h	Ch	`cpqNic3RedundancyIncreased` AMS detected that a previously failed physical adapter in a connected logical adapter group returned to OK status.	OK
18014	11h	Ch	`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.	Warning
18015	11h	Dh	`cpqNicAllLinksDown` All links are down on a network adapter.	Major
18016	Bh	Eh	`cpqNicAllLinksDownRepaired` One or more links on a network adapter were repaired.	OK
18017	32h	3023h	`cpqNicFlexLomTrainingFailed` Flexlom slot failed to train.	Critical
169001	12h	1h	`cpqiScsiLinkUp` The iSCSI link is up.	OK
169002	12h	2h	`cpqiScsiLinkDown` The iSCSI link is down.	Major

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

cpqida.mib	Drive array
cpqhost.mib	Server host system details
cpqhlth.mib	Server health system
cpqsm2.mib	Remote Insight/Integrated Lights-Out
cpqide.mib	IDE subsystem
cpqscsi.mib	SCSI system
cpqiscsi.mib	iSCSI system
cpqnic.mib	System NIC
cpqstsys.mib	Storage systems
cpqstdeq.mib	Server standard equipment
cpqfca.mib	Fibre Channel array
cpqsinfo.mib	System Information
cpqstsys.mib	Smart Array storage

REST alerts

The following table lists the REST alerts supported by iLO 6 and supported ProLiant servers. 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	ProcessorStatusUnknown	Warning
	ProcessorStatusOK	OK
	ProcessorStatusDegraded	Warning
	ProcessorStatusDisabled	Warning
	ProcessorStatusFailed	Critical
1010	USBStorageDeviceReadError	OK
1011	USBStorageDeviceWriteError	OK
1012	USBStorageDeviceRedundancyLost	Warning
1013	USBStorageDeviceRedundancyRestored	OK
1014	USBStorageDeviceSyncFailed	Warning
1015	PCIeDiskTemperatureFailed	Critical

Trap ID	REST Alert ID	REST Severity
1016	PCIeDiskTemperatureOk	OK
1017	PCIeDriveConditionOk	OK
	PCIeDriveConditionDegraded	Warning
	PCIeDriveConditionFailed	Critical
1018	PCIeDriveWearStatusOk	OK
	PCIeDriveWearStatusFiftySixDayThreshold	Warning
	PCIeDriveWearStatusFivePercentThreshold	Warning
	PCIeDriveWearStatusTwoPercentThreshold	Warning
	PCIeDriveWearStatusWearOut	Critical
1019	PCIeDriveAddedOrPowerOn	OK
1020	PCIeDriveRemovedOrPowerOff	OK
1021	NVMeSecureEraseFailed	Critical
1022	N/A	N/A
1023	PciResetFail	Critical
1193	BIOSSafeModeEngaged	OK
1194	N/A	N/A
1197	IntelligentDiagnosticsEnabled	OK
1198	IntelligentDiagnosticsExit	OK
1328	BIOSSafeModeExit	OK
1329	N/A	N/A
2014	IntrusionHWInstalled	OK
2015	IntrusionHWRemoved	OK
2016	HoodReplaced	OK
2017	HoodRemovedOnPowerOff	Warning
2018	MetricValueExceededUpperThreshold	Warning
	MetricValueBelowLowerThreshold	Warning
3033	DrvArrControllerFailed	Critical
	DrvArrControllerOK	OK

Trap ID	REST Alert ID	REST Severity
3034	DrvArrLogDrvFailed	Critical
	DrvArrLogDrvUnconfigured	Critical
	DrvArrLogDrvRecovering	Warning
	DrvArrLogDrvReadyRebuild	Warning
	DrvArrLogDrvRebuilding	Warning
	DrvArrLogDrvWrongDrive	Critical
	DrvArrLogDrvBadConnect	Critical
	DrvArrLogDrvOverheating	Warning
	DrvArrLogDrvShutdown	Critical
	DrvArrLogDrvExpanding	OK
	DrvArrLogDrvNotAvailable	Warning
	DrvArrLogDrvQueuedForExpansion	Warning
	DrvArrLogDrvMultiPathAccessDegraded	Warning
	DrvArrLogDrvErasing	Warning
	DrvArrLogDrvPredictiveSpareRebuildReady	OK
	DrvArrLogDrvRapidParityInitializationInProgress	Warning
	DrvArrLogDrvRapidParityInitializationPending	Warning
	DrvArrLogDrvNoAccessEncryptedMissingKey	Critical
	DrvArrLogDrvUnencryptedToEncryptedTransformationInProgress	Warning
	DrvArrLogDrvRekeyInProgress	Warning
	DrvArrLogDrvNoAccessEncryptedWithControllerEncryptionNotEnabled	Critical
	DrvArrLogDrvUnencryptedToEncryptedTransformationNotStarted	OK
	DrvArrLogDrvNewLogDrvKeyRekeyRequestReceived	OK
	DrvArrLogDrvOK	OK

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_SnapshotInProgress	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
	DrvArrPhysDrvErasing	Warning
	DrvArrPhysDrvNotAuthenticated	Warning
	DrvArrPhysDrvEraseDone	Warning
	DrvArrPhysDrvEraseQueued	Warning
	DrvArrPhysDrvOK	OK
3047	DrvArrSpareDriveFailed	Critical
	DrvArrSpareDriveInactive	OK
	DrvArrSpareDriveBuilding	Critical
	DrvArrSpareDriveActive	OK
3049	DrvArrSolidStateDiskFiftySixDayThresholdPassed	Warning
	DrvArrSolidStateDiskFivePercentThresholdPassed	Warning
	DrvArrSolidStateDiskTwoPercentThresholdPassed	Warning
	DrvArrSolidStateDiskWearOut	Critical
	DrvArrSolidStateDiskWearOK	OK
3903	SmartArraySecureEraseFailed	Critical
5022	N/A	N/A
5026	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
6040	ThermalStatusFailure	Critical
6041	ThermalStatusDegradedSysShutdown	Critical
	ThermalStatusDegradedSysContinue	Critical
6042	ThermalStatusOK	OK

Trap ID	REST Alert ID	REST Severity
6048	PowerSupplyOK	OK
6049	PowerSupplyDegraded	Critical
6050	PowerSupplyFailed	Critical
6051	MirroredMemoryEngaged	Warning
6054	PowerRedundancyRestored	OK
6055	FanRedundancyRestored	OK
6061	N/A	N/A
6062	N/A	N/A
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
6076	NvdimmBackupError	Critical
6077	NvdimmRestoreError	Critical
6078	NvdimmUncorrectableMemoryError	Critical
6079	NvdimmBackupPowerError	Critical
6080	NvdimmControllerError	Critical
6081	NvdimmEraseError	Critical
6082	NvdimmArmingError	Critical

Trap ID	REST Alert ID	REST Severity
6083	HeNvdimmSanitizationOk	Warning
6084	NvdimmSanitizationError	Critical
6085	HeNvdimmControllerFirmwareError	Critical
6086	NvdimmInterleaveOn	Critical
6087	NvdimmInterleaveOff	Critical
6088	NvdimmEventNotifyError	Critical
6089	NvdimmPersistencyLost	Critical
6090	NvdimmPersistencyRestored	OK
6091	HeNvdimmLifecycleWarning	Warning
6092	NvdimmLogicalNvdimmError	Warning
6093	NvdimmConfigurationError	Critical
6094	NvdimmBatteryNotChargedwithWait	Warning
6095	NvdimmBatteryNotChargedwithNoWait	Warning
6096	NvdimmMemoryMapChanged	Warning
6097	NvdimmPersistantMemoryAddressError	Critical
6098	NvdimmInitializationError	Warning
6099	PwrSupplyError	Warning
6100	PwrSupplyErrorRepaired	OK
6101	BatteryBackupUnitError	Critical
6102	BatteryBackupUnitErrorRepaired	OK
6103	NoPowerSupplyDetected	Critical
6104	PowerProtectionFault	Critical
6105	PowerDegradedEventDetected	Critical
6106	TPMSecureEraseFailed	Critical
6107	SPISecureEraseFailed	Critical
6108	AEPSecureEraseFailed	Critical
6109	EmbeddedMediaSecureEraseFailed	Critical
6110	SEDPassPhraseFailed	Critical
6111	SEDUnlockFailed	Warning
6118	InletAmbientPreCautionThresAlert	OK

Trap ID	REST Alert ID	REST Severity
6125	cpqHeUserTempThreshWarning	Warning
6126	cpqHeUserTempThreshCritical	Critical
8029	StorageSystemFanFailed	Critical
	StorageSystemNoFan	Warning
	StorageSystemFanDegraded	Critical
	StorageSystemFanOK	OK
8030	StorageSystemTemperatureFailed	Critical
	StorageSystemTemperatureDegraded	Critical
	StorageSystemNoTemperature	Warning
	StorageSystemTemperatureOK	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
9018	ServerPoweredOff	OK
9019	ServerPowerOnFailure	Critical
9020	ILOToInsightRemoteSupportCommunicationFailure	Warning
9021	FirmwareValidationScanFailed	Critical
9022	FirmwareValidationScanErrorRepaired	OK
9023	FirmwareValidationAutoRepairFailed	Warning
9024	AutoShutdownInitiated	Critical
9025	AutoShutdownCancelled	OK
9026	N/A	N/A
9027	N/A	N/A
9028	IPMIWatchdogTimerReset	Warning
9029	OverallSecStateAtRisk	Warning
9030	OverallSecStatusChange	Warning

Trap ID	REST Alert ID	REST Severity
11003	TestAlert	OK
11018	PowerThresholdBreach	Warning
11020	N/A	N/A
14004	N/A	N/A
14007	IdeAtaSecureEraseFailed	Critical
16028	N/A	N/A
18011	NicConnectivityRestored	OK
18012	NicConnectivityLost	Warning
18013	N/A	N/A
18014	N/A	N/A
18015	NicAllLinksDown	Critical
18016	NicAllLinksDownRepaired	OK
18017	N/A	N/A
169001	N/A	N/A
169002	N/A	N/A
999927	EnclosureManagerFirmwareMismatch	Critical
80321	StorageSystemNotConnected	Critical
80323	StorageSystemConnected	OK
80322	StorageSystemNotSupported	Warning
6120	LiquidCoolingModuleFailed	Critical
6119	LiquidCoolingModuleDegraded	Critical
6121	LiquidCoolingModuleRedundancyLost	Warning
6122	LiquidCoolingModuleRedundancyRestored	OK
6123	UnsupportedPowerSupplyUnitDetected	Critical
6124	UnsupportedPowerSupplyUnitRemoved	OK
140083	DriveSmartError	Critical
140084	DriveFailed	Critical
140085	DriveWearOut	Warning
140082	DriveOk	OK
140086	DriveRemoved	Warning

Trap ID	REST Alert ID	REST Severity
140087	`DriveInserted`	Warning
140096	`SsdWearOut`	Critical

IPMI alerts

#	Name	IPMI SEL Event (Y/N)	IPMI SEL Event Details	SNMP support? (Y/N)	OID
1	CPU failure	Y	IERR | Asserted Uncorrectable Machine check exception | Asserted Configuration Error | Asserted	Y	`cpqSeCpuUncorrectableError` `cpqSeCpuStatusChange`
3	Memory ECC error	Y	Uncorrectable ECC | Asserted	Y	`cpqHe5CorrMemReplaceMemModule`
4	Correctable memory error	Y	Correctable ECC | Asserted	N	N/A
5	Memory failure	Y	Memory Device Disabled | Asserted Configuration Error | Asserted	Y	`cpqHe5CorrMemReplaceMemModule`
9	Power supply failure	Y	Failure detected | Asserted Power Supply AC lost | Asserted	Y	`cpqHe4FltTolPowerSupplyFailed` `cpqHePwrSupplyError` `cpqHe4FltTolPowerSupplyACpowerloss` `cpqHeNoPowerSupplyDetected`
10	Power supply removed	Y	Presence detected | Deasserted	Y	`cpqHe3FltTolPowerSupplyRemoved`
14	Hard disk failure	Y	Drive Fault | Asserted Predictive Failure | Asserted In Failed Array | Asserted	Y	`cpqDa7PhyDrvStatusChange`
16	Fan failure	Y	Transition to OK | Asserted Transition to Non-Critical from OK | Asserted Transition to Non-Recoverable from less severe | Asserted Transition to Non-Critical from more severe | Asserted	Y	`cpqHe3FltTolFanDegraded` `cpqHe3FltTolFanFailed` `cpqHe3FltTolFanRedundancyLost` `cpqHe3FltTolFanInserted`
17	Fan removed	N	–	Y	`cpqHe3FltTolFanRemoved`

iLO Mail

iLO Mail enables you to configure iLO to send alert conditions detected independently of the host operating system to one or more email addresses, and to enable SMTP for Two Factor Authentication. iLO AlertMail messages include major host system events that appear in the IML. For example, if a fan failure occurs, an event is recorded in the IML and an email message with the details is sent to the configured email addresses.

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. To work around this issue, Hewlett Packard Enterprise recommends enabling a secure SMTP connection (SSL/TLS) and configuring a sender email address that is recognized by the configured SMTP server.

Subtopics

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: **https://www.hpe.com/support/ilo-docs**.
- For configurations with Enable SMTP Authentication enabled, you have the user name and password of an email account on the SMTP Server.
- For configurations with Enable SMTP Secure Connection (SSL/TLS) enabled, SSL/TLS is enabled on the server.
- If you use a public or ISP SMTP server, make sure that the email addresses you will use for the recipient addresses are configured to allow less secure applications.

Procedure

1. Click Management in the navigation tree, and then click the Mail tab.
2. Set the Enable iLO AlertMail option to enabled.
3. Enter the following information:
   - Recipient Email Address
   - Sender Domain or Email Address
   - SMTP Port

     If the Enable SMTP Secure Connection (SSL/TLS) option will be used, Hewlett Packard Enterprise recommends setting this value to 587.
   - SMTP Server
4. To send AlertMail messages over a secure connection, enable the Enable SMTP Secure Connection (SSL/TLS) option.
5. To authenticate the SMTP connection with an email account user name and password, enable the Enable SMTP Authentication option.
6. If Enable SMTP Secure Connection (SSL/TLS) and Enable SMTP Authentication are enabled:
   a. Enter the user name for an email account on the configured SMTP server in the SMTP Username box.
   b. Select the Change SMTP Password check box.
   c. Enter the password for the email account user name in the New SMTP Password and Confirm SMTP Password boxes.

7. To save the changes, click Apply.
8. (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.
9. (Optional) If you sent a test message, check the iLO event log to confirm that it was sent successfully.

Subtopics

AlertMail options

AlertMail options

Recipient Email Address

One or more destination email addresses to receive iLO email alerts. You can enter multiple email addresses separated by a Comma or Semicolon. Enter the addresses in standard email address format. You can enter up to 260 characters in the Recipient Email Address box.

If you use a public or ISP SMTP server, make sure that the email addresses you enter are configured to allow less secure applications.

Sender Domain or Email Address

The sender (from) email address (up to 63 characters). This value can be formed by using the following methods:

- Enter a sender domain to be combined with the iLO Hostname. When you use this method, the sender email address is < iLO Hostname>@<Sender Domain>.
- Enter a custom email address that includes your internal network domain. For example, <name>@<internal domain>.com.
- Enter a custom email address that uses a public email server. For example, <name>@<email provider>.com.

  This address must be a valid email address that is recognized by the configured SMTP server.

SMTP Port

The port the SMTP server will use for authenticated or unauthenticated SMTP connections. The default value is 25. For secure connections, Hewlett Packard Enterprise recommends port 587.

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. You can enter an IPv4 address, an IPv6 address, or an FQDN. This string can be up to 63 characters.

Enable SMTP Secure Connection (SSL/TLS)

Enable this option to send AlertMail messages over a secure connection. When a message is sent, iLO and the configured SMTP Server negotiate to select a common SSL/TLS connection.

iLO supports only explicit/opportunistic TLS SMTP servers (STARTTLS SMTP servers).

This value is enabled by default.

Enable SMTP Authentication

Enable this option to authenticate against the configured SMTP Server after connecting through a secure connection. To use this option, Enable SMTP Secure Connection (SSL/TLS) must be enabled and you must provide the user name and password for an email account on the SMTP server.

SMTP Username

The username (up to 63 characters) for an account on the configured SMTP Server. This value is required if Enable SMTP Authentication is enabled.

To clear this value, disable the Enable SMTP Authentication option, delete the text in this box, and then click Apply.

Change SMTP Password

Click this check box to enter or update and confirm the password for the SMTP Username account. This value is required if Enable SMTP Authentication is enabled, and it can be up to 63 characters long.

The password value cannot be viewed or copied from the iLO web interface.

To clear the password, disable the Enable SMTP Authentication option, apply blank password and password confirmation values, and then click Apply.

Disabling AlertMail

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: **https://www.hpe.com/support/ilo-docs**.
- Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree, and then click the Mail tab.
2. Set the Enable iLO AlertMail option to disabled.
3. To save the changes, click Apply.

Enabling SMTP for Two Factor Authentication

Prerequisites

- Configure iLO Settings privilege
- Configure SMTP server

Procedure

1. Click Management in the navigation tree, and then click the Mail tab.
2. Set the Enable SMTP for Two Factor Authentication option to enabled.
3. To save the changes, click Apply.

Disabling SMTP for Two Factor Authentication

Prerequisites

- Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree, and then click the Mail tab.
2. Set the Enable SMTP for Two Factor Authentication option to disabled.

   Disabling SMTP for Two Factor Authentication will disable Two factor authentication for LDAP users.
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.
```

Subtopics

Enabling iLO remote syslog

Disabling iLO remote syslog

Remote Syslog alert levels (Linux)

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: **https://www.hpe.com/support/ilo-docs**.
- The remote syslog server is configured to use UDP.

Procedure

1. Click Management in the navigation tree, and then click the Remote Syslog tab.
2. Set the Enable iLO Remote Syslog option to enabled.
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.

Subtopics

Remote syslog options

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 511 characters in the Remote Syslog Server box.

  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: **https://www.hpe.com/support/ilo-docs**.
- Configure iLO Settings privilege

Procedure

1. Click Management in the navigation tree, and then click the Remote Syslog tab.
2. Set the Enable iLO Remote Syslog option to disabled.
3. To save the changes, click Apply.

Remote Syslog alert levels (Linux)

Some status values in iLO differ from the standard Linux syslog status values. The following table shows the equivalent values.

iLO status	Linux syslog status
Critical	Critical
Caution	Warning
Repaired	Notice
Informational	Informational

Configuring Compute Ops Management

Subtopics

HPE Compute Ops Management

HPE Compute Ops Management

HPE Compute Ops Management enables iLO to connect to the cloud-based management services for Gen10 and later servers.

HPE Compute Ops Management is built on a unique cloud-native architecture that abstracts and orchestrates infrastructure and compute

workflows, transforming complex compute operations into a simplified experience across edge-to-cloud to accelerate agility. You can manage servers with Compute Ops Management through HPE GreenLake. For more details see, **https://hpe.com/solutions/compute-ops-management**.

Connecting to HPE Compute Ops Management

Prerequisites

- Configure iLO Settings privilege.
- Configure DNS server.
- Configure Web proxy.
- Ensure that the server has Serial number, Universally Unique Identifier (UUID), and Product ID.
- Ensure that the Date and Time of iLO is set correctly.

About this task

Procedure

1. Click Compute Ops Management in the navigation tree.

   HPE Compute Ops Management page is displayed.

   NOTE:

   Hewlett-Packard Enterprise recommends configuring Web proxy while connecting to **HPE Compute Ops Management**. You can configure or edit the Web proxy settings on the Access Settings page.

2. Click to edit the **HPE Compute Ops Management** settings.

   HPE Compute Ops Management Settings page is displayed.

3. Use the toggle button to enable **HPE Compute Ops Management**.

   If the system is managed by HPE OneView, enabling **HPE Compute Ops Management** will disconnect from HPE OneView.

4. Select from the following key type: Activation key, HPE GreenLake Workspace ID, or No key.

5. (Optional) Enter the Activation key or HPE GreenLake Workspace ID.

   If you have selected HPE GreenLake Workspace ID, log in to **HPE GreenLake**, on the **HPE GreenLake** platform header, click the workspace menu and then select Manage Workspace. Double click the Workspace ID to select it, and then copy it. The activation key must be alphanumeric and the maximum length is 32 characters.

   If you have selected Activation key, log in to **HPE GreenLake** and launch the Compute Ops Management service. In the Overview page, in the Add servers section, click Get key to generate a key.

   The Activation Key is not mandatory to initiate connection to **HPE Compute Ops Management**. If **HPE Compute Ops Management** accepts the connection request without Activation Key, the connection status will be Connected. If **HPE Compute Ops Management** needs Activation Key, the connection status will be ActivationKeyRequired. On receiving this status, user must retry with valid Activation Key.

6. Click Save to initiate a connection to **HPE Compute Ops Management**.

   The Connection label shows the connection state between iLO and **HPE Compute Ops Management**.

   After iLO is connected to **HPE Compute Ops Management**, irrespective of the connection status (Success or Failure), **HPE Compute Ops Management** will be set as Enabled.

   During reset, iLO automatically triggers a connection to **HPE Compute Ops Management**. **HPE Compute Ops Management** will be set as Disabled only if the user manually disables **HPE Compute Ops Management**.

Disconnecting from HPE Compute Ops Management

Procedure

1. Click Compute Ops Management in the navigation tree.

   HPE Compute Ops Management page is displayed.

2. Click  to edit the **HPE Compute Ops Management** settings.

   HPE Compute Ops Management Settings page is displayed.

3. Use the toggle button to disable **HPE Compute Ops Management**.

4. Click Save. **HPE Compute Ops Management** is disabled.

   The following actions are initiated when **HPE Compute Ops Management** is disabled:
   - iLO disconnects from **HPE Compute Ops Management**.
   - All configuration settings are cleared, except web proxy settings.

   You must reconfigure the settings to connect to **HPE Compute Ops Management**.

HPE Compute Ops Management connection states

This section shows the connection status for HPE Compute Ops Management.

The possible status values are:

- Disabled—HPE Compute Ops Management is not enabled.
- In Progress—Connection to the HPE Compute Ops Management is in progress.
- Connected—iLO is connected to HPE Compute Ops Management successfully.
- ActivationKeyRequired—iLO attempted to connect to HPE Compute Ops Management without an Activation Key. The request is rejected to retry with an Activation Key.
- Failed—iLO failed to connect to the HPE Compute Ops Management. For more details, see the iLO AHS log.
- Not Connected —iLO lost connection to HPE Compute Ops Management due to a network interruption. An automatic reconnect is attempted in every one hour to re-establish the connection. Click Connect for an instant attempt to reconnect.

NOTE:

- If iLO reset happens, the HPE Compute Ops Management status changes from Connected to Not Enabled. This is an expected behavior. It takes iLO around 120 seconds after the iLO reset to show the HPE Compute Ops Management status.
- Changing or disabling DNS configuration, Web proxy configuration values will impact the connectivity and HPE Compute Ops Management connection status.

Using the lifecycle management features

Subtopics

Always On Intelligent Provisioning

Always On Intelligent Provisioning is a web interface that you can use to perform OS deployments and review hardware configuration details.

Starting Intelligent Provisioning from iLO

Prerequisites

- Remote Console privilege
- Host BIOS privilege
- Intelligent Provisioning is installed on the server.

Procedure

1. Click Lifecycle Management in the navigation tree.

   The Intelligent Provisioning page is displayed.

   The installed version of Intelligent Provisioning is listed on the Intelligent Provisioning page.

2. Click Always On to start Intelligent Provisioning.

   The Intelligent Provisioning web interface starts in a new browser window.

   For information about using Intelligent Provisioning, see the Intelligent Provisioning documentation at the following website: **https://www.hpe.com/info/intelligentprovisioning/docs**.

One-button secure erase

If you want to decommission a server or prepare it for a different use, you can use the One-button secure erase feature.

One-button secure erase follows the NIST Special Publication 800-88 Revision 1 in the Guidelines for Media Sanitization guide. The appendix recommends minimum sanitization levels for media. For more information about the specification, see Section 2.5, **Guidelines for Media Sanitization**.

One-button secure erase implements the NIST SP 800-88 Revision 1 Sanitization Recommendations for **Purging** user data and returns the server and supported components to the default state. This feature automates many of the tasks that you follow in the Statement of Volatility document for a server.

HPE ProLiant RL3xx platforms do not support One-button secure erase.

One-button secure erase access methods

You can initiate the One-button secure erase process from the following products:

- iLO
- Intelligent Provisioning
- The iLO RESTful API and iLOREST

This topic describes the One-button secure erase access methods from iLO.

Prerequisites for initiating the One-button secure erase process

Prerequisites

- Verify that your iLO user account is assigned all the iLO user account privileges including recovery set.
- Install an iLO license that supports this feature.

  For information about the available license types and the features they support, see the licensing documentation at the following

website: **https://www.hpe.com/support/ilo-docs**.

- If the following features are enabled, disable them:
  - Server Configuration Lock

    For instructions, see the **UEFI System Utilities user guide and HPE Synergy.**

    For instructions, see the UEFI System Utilities user guide.

  - Smart Array Encryption

    For instructions, see the "Clearing the encryption configuration" section in the **HPE Smart Array SR Secure Encryption Installation and User Guide**.

    For instructions, see the instructions for clearing the encryption configuration in the Secure Encryption installation and user guide.

  - Intel VROC Encryption

    For instructions, see the Cleaning the security and encryption configurations section in the Intel Virtual RAID on CPU User Guide.
- On HPE Synergy systems, remove HPE OneView or Virtual Connect profiles assigned to the system.
- Verify that the iLO security setting on the system maintenance switch is in the OFF position.
- The storage drives that you want to erase support a native sanitize method.

  Examples include the `SANITIZE` command for SATA and SAS drives and `FORMAT` for NVM Express drives. The NIST publication recommends these commands for purging data on these device types. Using these commands is more secure than using software to overwrite data on storage drives.

  If an attached storage device does not support native sanitize methods, it will not be erased during the One-button secure erase process. An Integrated Management Log (IML) entry will report an erase failure for the device.

  HPE ProLiant RL3xx platforms do not support Smart Array Encryption, SATA and SAS drives, and Intel VROC.
- Hewlett Packard Enterprise recommends disconnecting or detaching the removable drives, external storage, or shared storage that you do not want to erase.
- Hewlett Packard Enterprise recommends configuring SNMP alerts, Mail Settings, or iLO RESTful API alerts before initiating the One-button secure erase process.

  If errors occur when individual components are erased, an IML entry is logged for each error. You can review the IML log using SNMP alerts, Mail Settings, or iLO RESTful API alerts. The IML is erased later during the One-button secure erase process. After the IML is erased, high-level status information is provided in the secure erase report.
- If you use LDAP Directory Authentication with the HPE Extended Schema, you have another method for logging in to iLO to initiate the One-button secure erase process.

  Supported methods include local accounts, Kerberos authentication, CAC Smartcard, and schema-free directory accounts.

  The HPE Extended Schema does not support the user privileges required to initiate the One-button secure erase process.
- Disable Microsoft® Secured-core Support.

Initiating the One-button secure erase process

Prerequisites

Your environment meets the Prerequisites for initiating the One-button secure erase process .

> **CAUTION:**
> Use this feature only when you want to decommission a system or use it for a different purpose. This process resets the server and supported components to the factory state. Depending on the storage capacity, securely erasing the server and components might take up to a day or more to finish. Once you initiate this process, it cannot be undone. Until the process is complete, avoid interactions with iLO or the system that involve configuration changes and powering off the system.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.
2. Click Erase System.

   iLO prompts you to confirm the request.
3. Select the I have understood the implications of Secure Erase and ready to decommission this system check box, and then click Yes, permanently erase system.

   The server restarts and the One-button secure erase process begins. During the server reboot, BIOS deletes the data that it controls. After BIOS deletes the data, the server is powered off. iLO then deletes the remaining data.

   The One-button secure erase progress is displayed in the banner area on all iLO web interface pages. The displayed information includes the percent complete and the estimated time left. Individual hardware or software component details are displayed in the Secure Erase Status table.

   Do not make configuration changes during the One-button secure erase process. iLO prevents firmware updates and iLO resets during this process.

   When the One-button secure erase is complete, iLO is reset, and it becomes unavailable on the network.

   On HPE Synergy compute modules, the iLO network settings might be reassigned after the process is complete, and the system might power on.
4. (Optional) Return the system to an operational state .
5. (Optional) View, save, or delete the One-button secure erase report.

   Hewlett Packard Enterprise recommends completing this step.
6. (Optional) If a device failed the erase process, or the device does not support a native sanitize method, do one of the following:
   - Isolate these devices and use other methods to delete the data.
   - Securely dispose of the devices according to your organization security policies.

   Hewlett Packard Enterprise recommends completing this step.

One-button secure erase status values

When you initiate the One-button secure erase process, the overall progress is displayed in the iLO banner. The status of individual components is displayed in the Secure Erase Status table.

- Idle—The process has not started.
- Initiated—The process has started.
- In Progress—Erasing is in progress.
- Success—The process completed successfully.
- Error—The process completed and errors occurred.
- Failed—The process failed.

> **NOTE:**
>
> In the Secure Erase Status table, iLO Settings includes the results for Embedded NAND Flash and NVRAM. An erase failure in one of these components results in an overall failure for iLO Settings.
>
> In the Secure Erase Status table, BIOS Settings includes the results for the UEFI configuration store and RTC (system date and time). An erase failure in one of these components results in an overall failure for BIOS Settings.

Returning a system to operational state after One-button secure erase

About this task

After a system is erased with the One-button secure erase process, use the following procedure to return it to an operational state.

Procedure

1. Configure the iLO network settings.
2. Install Intelligent Provisioning using an Intelligent Provisioning recovery image.

   For more information, see the Intelligent Provisioning user guide.
3. Install an OS.
4. Optional: Install an iLO license.
5. Configure the BIOS settings and the iLO settings that apply to your environment.
6. (Optional) Create a System Recovery Set.

Viewing the One-button secure erase report

Prerequisites

- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.

   If the One-button secure erase process completed on the server, the View Last Erase Report button is available.
2. Click View Last Erase Report.

   The Secure Erase Report is displayed.
3. (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.
4. (Optional) Save the One-button secure erase report .

   Hewlett Packard Enterprise recommends saving a copy of the erase report for future reference.
5. (Optional) Delete the One-button secure erase report .

   Hewlett Packard Enterprise recommends deleting the erase report before decommissioning a server or using it for a different purpose.

One-button secure erase report details

- Server Serial Number—The server serial number.
- Initiated By—The user who initiated the One-button secure erase process.

The following information is listed for each device type:

- Device Type—The device type that was erased.

  For information about the affected device types, see Impacts to the system after One-button secure erase completes .

  The Secure Erase Report includes only the Embedded NAND Flash and NVRAM status.
- Location—The location of the device in the server.
- Serial Number—The device serial number.
- Status—The One-button secure erase status for the device.
- Erase Type—The type of erase operation. For more information about the operations that were performed, see One-button secure erase FAQ.

- Start Time—The One-button secure erase start time for the specific device.
- End Time—The One-button secure erase end time for the specific device.

Saving the One-button secure erase report to a CSV file

Prerequisites

- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.

About this task

When you use the One-button secure erase feature, Hewlett Packard Enterprise recommends saving a copy of the erase report for future reference.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.
2. Click  .

   The CSV Output window is displayed.
3. Click Save, and then follow the browser prompts to save or open the file.

Deleting the One-button secure erase report

Prerequisites

- Configure iLO Settings privilege
- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.
- If you want a copy of the One-button secure erase report for future reference, you saved the report.

About this task

When you decommission or repurpose a server, you might not want the One-button secure erase report to remain available in the iLO web interface.

Hewlett Packard Enterprise recommends deleting the erase report before decommissioning a server or using it for a different purpose.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.

   If the One-button secure erase process completed on the server, the View Last Erase Report button is available.
2. Click View Last Erase Report.

   The Secure Erase Report is displayed.
3. Click  .

   iLO securely erases the report file, and then resets immediately.

   The event log, IML, security log, and configuration settings made up to this point are reset to the factory default settings. iLO might attempt an auto-restore operation when it starts. For more information, see iLO backup and restore.

Impacts to the system after One-button secure erase completes

The One-button secure erase feature reverts the system and supported components to the factory state. To use the system, reprovision the server.

- All data on the impacted storage drives and Persistent Memory are erased and not recoverable. All RAID settings, disk partitions, and OS installations are removed.

The following BIOS and iLO 6 settings are erased or reset to the factory default settings.

- Factory provisioned server identity (iLO IDevID), User defined server identity (iLO LDevID), and Factory provisioned TCG compliant system identity (System IDevID) are erased.
- Platform certificate, System IAK certificate and all other enrolled certificates (other than factory pre-installed UEFI Secure boot certificates are erased.
- iLO network and other settings are erased and must be reconfigured.
- Installed iLO licenses are removed and the license status reverts to iLO Standard.

  If the iLO Advanced license is preinstalled at the factory with the #0D1 option, the license is reinstated when the One-button secure erase process is finished. For more information about this license option, see the HPE iLO Licensing Guide.
- The System Recovery Set is removed and must be recreated.
- iLO user accounts are removed. After the process is complete, log in with the default factory Administrator account and password.
- The Active Health System, Integrated Management Log, Security Log, and iLO Event Log are cleared.
- BIOS and SmartStorage Redfish API data is removed and then recreated on the next boot.
- Secure Boot is disabled and enrolled certificates are removed (other than the factory installed certificates).
- Boot options and BIOS user-defined defaults are removed.
- Passwords, pass-phrases, and encryption keys stored in the TPM or BIOS are removed.
- The date, time, DST, and time zone are reset.
- The system will boot with the most recent BIOS revision flashed.

- Intelligent Provisioning will not boot and must be reinstalled.

Hardware components that are reverted to the factory state

The following components are reverted to the factory state during the One-button secure erase process.

- UEFI Configuration store
- RTC (System Date and Time)
- Trusted Platform Module
- NVRAM
  - BIOS Settings
  - iLO configuration settings
  - iLO Event Log
  - Integrated Management Log
  - Security Log
- HPE SR controllers, MR controllers, NS controllers and connected storage drives.

  For more information about controllers, see, Supported storage products section in the iLO User Guide.
- Intel VROC
- Drive data (for drives that support native sanitize methods).
  - SATA, SAS drives (SSD and HDD)
  - NVM Express
- Embedded Flash

- iLO RESTful API data
- Active Health System
- Firmware repository

Hardware components that are not reverted to the factory state

The following components are not affected by the One-button secure erase process.

- USB drives
- SD cards
- iLO virtual media
- Configuration on PCI controllers
- SAS HBAs and connected drives
- SATA, SAS, and NVM Express drives that do not support native sanitize methods.
- FCoE, iSCSI storage
- GPGPUs
- Other FPGAs, accelerators, offload engines that have keys or storage

One-button secure erase FAQ

Does One-button secure erase purge USB devices and internal SD cards?

No. One-button secure erase does not erase USB devices and internal SD cards.

If an HDD does not support the Purge function, does One-button secure erase attempt to purge it?

No. One-button secure erase skips a drive that does not support the purge function.

Does One-button secure erase support Smart Array controllers?

HPE SR controllers, MR controllers, and NS controllers are supported for One-button secure erase.

Does One-button secure erase erase drives that do not support Purge?

RAID controllers can wipe drives (overwrite with a pattern) that do not support the purge operation. One-button secure erase does not request the controller to perform this nonsecure wipe. To wipe data on such drives, use the Intelligent Provisioning “System Erase and Reset” feature.

Does One-button secure erase erase battery backed cache?

See the table following for more information.

How does One-button secure erase process the erase commands?

See the following table for information on how One-button secure erase purges or overwrites data.

What privileges do users need to launch One-button secure erase?

Users need all iLO privileges to launch One-button secure erase.

Does One-button secure erase remove the serial number and product ID?

No, these items are not erased by One-button secure erase.

How long does the process take?

The duration depends on the hardware. Sanitization of HDDs takes longer than SSDs.

How One-button secure erase affects supported drives

Device	Operation requested	Result

Device	Operation requested	Result
NVRAM	3-pass write: 0x5a, 0xa5, 0xff	All battery backed iLO SRAM memory is overwritten.
Embedded Flash (NAND)	eMMC 5.1 (JEDEC 84-B51) Secure Erase command with SECURE_REMOVAL_TYPE in Extended CSD register set to physical memory erase, if supported by the device.	Data in physical memory is erased.
Intel Optane DC PMM	Secure Erase + Overwrite DIMM	Cryptographic keys are removed and data in all physical memory blocks (both user accessible and in spare blocks) is overwritten with zeros. PCD regions containing all configuration and metadata is also overwritten.
UEFI configuration store	3-pass: Chip erase (0xff), 0x00, Chip erase (0xff)	All physical sectors are overwritten.
RTC	Reset time to 01-01-2001 00:00:00	Date, Time, Time zone, and DST are reset to defaults.
TPM	TPM Clear + Clear NV indices + Delete Platform Symmetric key	All data in TPM is cleared including any nonvolatile information.
HPE Smart Array SR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize **Note:** Before initiating the One-button secure erase, the Security reset function must be performed manually through the Smart Storage Administrator, if Smart Array Secure Encryption was enabled.	• The security reset function removes the drive keys that are stored on the key manager for remote key management. All secrets, keys, and passwords from the controller and drives are cleared. This operation does not remove the controller key on the key manager. • All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. • Flash backup is cleared and data in the DRAM write back cache is lost when the power is removed. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE Smart Array MR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. Encryption keys are cleared. • Flash backup is cleared and data in the DRAM write back cache is lost when the power is removed. All attached drives are requested to be sanitized. See below for operations requested on the drives.

Device	Operation requested	Result
HPE NS Boot Controller	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. All attached drives are requested to be sanitized. See below for operations requested on the drives.
SATA HDD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten with zeros, including physical sectors that are not user accessible. Any previous data in caches are also made inaccessible.
SATA SSD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with BLOCK ERASE option	Previous data in all physical memory blocks, including physical memory blocks that are not user accessible, becomes irretrievable. Any previous data in caches are also made inaccessible.
SAS HDD	A single pass of SCSI SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten, including physical sectors that are not user accessible. Any data in caches are also sanitized.
SAS SSD	A single pass of SCSI SANITIZE with BLOCK ERASE option	All physical memory blocks, including physical memory blocks that are not user accessible, are set to a vendor-specific value. Any data in caches are also sanitized.
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2, if supported.	This is a cryptographic erase accomplished by deleting the encryption key.
	NVM Express SANITIZE if supported (for drives supporting NVM Express version 1.3 or later) A single pass of NVM Express FORMAT with SES = 1. This option is used if the drive does not support the SANITIZE.	All data and metadata associated with all namespaces is destroyed. All user content present in the NVM subsystem is erased.

These drives might be connected to HPE SR controllers and MR controllers or the Chipset SATA controller.

[1] Supported devices that fail the erase process and unsupported devices are not erased securely. These devices might contain sensitive data. Isolate devices that are not erased and use other methods to delete the data, or securely dispose of the devices according to your organization security policies.

iLO backup and restore

Automatic backup and restore

When iLO goes through the initialization process, 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 or data corruption is detected, iLO tries to restore the configuration information from the backup file. Automatic restore operations are recorded in the IML.

When iLO security is disabled with the system maintenance switch, the SRAM data is not restored automatically.

The backup file created by the automatic backup and restore process is not user-accessible. It cannot be used to perform a manual restore operation.

NOTE: Backup and Restore functionality will not be available through iLO RESTful API, while host OS is booting up. The functionality will be available through iLO web interface irrespective of the boot state of the host.

Manual backup and restore

iLO supports manually restoring the configuration information stored in the battery-powered SRAM memory device. This feature is intended for use on a system with the same hardware configuration as the system that was backed up. It is not meant to duplicate a configuration and apply it to a different iLO system.

Hewlett Packard Enterprise does not expect that you will have a reason to perform a restore operation. However, there are cases in which having a backup of the configuration expedites the return to a normal operating environment.

As with any computer system, backing up your data is a recommended practice to minimize the impact from failures. Hewlett Packard Enterprise recommends performing a backup each time that you update the iLO firmware.

iLO firmware requirements for backup and restore

- iLO firmware supports backup and restore operations in which the backup and restore tasks are performed on systems with the same or different iLO firmware versions.

Information that is restored during a backup and restore operation

The iLO configuration includes many categories such as power, network, security, license keys, and the user database. Most configuration information is stored in the battery-powered SRAM memory device, and it can be backed up and restored.

NOTE:

When environment variables are restored, a server reset is required for the restored settings to take effect.

For example, the Performance settings are restored, but they do not take effect until a server reset is complete.

Information that is not restored during a backup and restore operation

Some information is not suitable to be restored during backup and restore operations. The information that cannot be restored is not part of the iLO configuration, but instead is related to the iLO or server system state.

The following information is not backed up or restored:

Security state

Allowing a restore operation to change the iLO security state would defeat the principles of security and enforcement of security.

Integrated Management Log

To preserve information about events that occurred between the backup and the event that required the restore, this information is not restored.

iLO Event Log

To preserve information about events that occurred between the backup and the event that required the restore, this information is not restored.

Security Log

To preserve information about security events that occurred between the backup and the event that required the restore, this information is not restored.

Active Health System data

To preserve the information recorded during the backup and restore process, this information is not restored.

Server state information

- Server power state (ON/OFF)
- Server UID LED states
- iLO and server clock settings

Reasons to manually restore the iLO configuration

You might want to restore the iLO configuration in the following situations:

Battery failure or removal

Various configuration parameters are stored in the battery-powered SRAM. Although rare, the battery can fail. In some situations, battery removal and replacement might be required. To avoid the loss of configuration information, restore the iLO configuration from a backup file after the battery is replaced.

Reset to factory defaults

In some cases, you might need to reset iLO to the factory default settings to erase settings external to iLO. Resetting iLO to the factory default settings erases the iLO configuration. To recover the iLO configuration quickly, restore the configuration from a backup file after the factory default reset is complete.

Accidental or incorrect configuration change

In some cases, the iLO configuration might be changed incorrectly, causing important settings to be lost. This situation might occur if iLO is reset to the factory default settings or user accounts are deleted. To recover the original configuration, restore the configuration from a backup file.

System board replacement

If a system board replacement is required to address a hardware issue, you can use this feature to transfer the iLO configuration from the original system board to the new system board.

Lost license key

If a license key is accidentally replaced, or you reset iLO to the factory default settings, and you are not sure which key to install, you can restore the license key and other configuration settings from a backup file.

Backing up the iLO configuration

Prerequisites

- Configure iLO Settings privilege
- iLO is configured to use the Production or High Security security state. Backing up and restoring the configuration when iLO is configured to use a higher security state is not supported.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click Backup & Restore.
2. Click Backup.
3. (Optional) To password protect the backup file, enter a password in the Backup file password box.

   The password can be up to 32 characters long.
4. Click Download.

   The file is downloaded and this activity is recorded in the event log.

   The file name uses the following format: `<server serial number>_<YYYYMMDD>_<HHMM>.bak`.

Restoring the iLO configuration

Prerequisites

- Configure iLO Settings privilege

- Administer User Accounts privilege
- A backup file exists.
- The default iLO account credentials are available if you previously reset iLO to the factory default settings.
- The iLO security state you want to use is configured.

  When you configure a higher security state than Production or High Security, iLO is reset to the factory default settings. If you do not configure these security states before performing a restore, the restored information is deleted when you update the security state.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click Backup & Restore.
2. Click Restore.
3. Depending on your browser, click Browse or Choose File, and then navigate to the backup file.
4. If the backup file is password protected, enter the password.
5. Click Upload and Restore.

   iLO prompts you to confirm the request.
6. Click Restore.

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

More information

iLO backup and restore
iLO default DNS name and user account
iLO encryption settings

Restoring the iLO configuration after system board replacement

Prerequisites

- Configure iLO Settings privilege
- Administer User Accounts privilege
- A backup file exists.
- The default iLO account credentials are available if you previously reset iLO to the factory default settings.
- The iLO security state you want to use is configured.

  When you configure a higher security state than Production or High Security, iLO is reset to the factory default settings. If you do not configure these security states before performing a restore, the restored information is deleted when you update the security state.

About this task

When you replace a system board, you can restore the configuration from the replaced system board.

Procedure

1. Replace the system board and transfer the hardware components from the old system board to the new system board.
2. Power on the system and ensure that all components are working correctly.
3. Log in to iLO with the default user credentials for the new system board.
4. Restore the configuration from the backup file.

More information

iLO backup and restore

iLO default DNS name and user account

iLO encryption settings

Using iLO with other software products and tools

Subtopics

iLO and remote management tools

IPMI server management

Using iLO with HPE SIM

iLO and remote management tools

PE ProLiant RL3xx Gen 11 platforms do not support HPE OneView.

iLO 6 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.
  ```

- A page called <Remote Management Tool Name> is added to the iLO navigation tree.

Subtopics

Starting a remote management tool from iLO

Deleting a remote manager configuration

Using iLO with HPE OneView

Adding hotfixes to create an HPE OneView custom firmware bundle

Starting a remote management tool from iLO

About this task

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. Click <Remote Management Tool Name> in the navigation tree.
2. Click Launch.

   The remote management tool starts in a separate browser window.

More information

Starting a remote management tool from the login page

Deleting a remote manager configuration

About this task

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. Refresh the iLO web interface window after removing the server from HPE OneView.

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. Click <Remote Management Tool Name> in the navigation tree.
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 does not support HPE ProLiant RL3xx Gen 11 platforms.

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 6, 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 firmware could cause it to become out of synchronization with HPE OneView.

Subtopics

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

About this task

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**.

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 or off operations
- Logging capabilities for abnormal events such as over-temperature readings or fan failures
- Inventory capabilities such as identification of failed hardware components

NOTE:
On HPE ARM-based Gen11 servers like HPE ProLiant RL3xx Gen 11, the server `AssetTag` configured through RBSU does not impact the iLO interfaces using Redfish or IPMI, for example, postman and ipmitool. Similarly, an `AssetTag` configured through iLO interfaces using Redfish or IPMI does not impact the `AssetTag` settings in the BIOS.

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 **https://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 **https://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 **https://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: **https://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: **https://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 must 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`.

Subtopics

Advanced IPMI tool usage on Linux

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 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.

HPE ProLiant RL3xx Gen 11 platforms do not support 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.

Agentless Management

iLO, combined with Agentless Management, provides remote access to system management information through the iLO web interface.

Support for SNMP management

HPE SIM can access SNMP information through iLO.

Subtopics

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 enabling the Anonymous Data setting on the Access Settings page.

Subtopics

Viewing iLO status in HPE SIM

iLO links in HPE SIM

Viewing iLO in HPE SIM System lists

More information

Configuring iLO access settings

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

About this task

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. Click Management in the navigation tree.

b. Configure the SNMP Settings and SNMP Alerts.

   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.

More information

Adding SNMP Alert Destinations

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 6, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser

More information

Configuring iLO access settings

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

Subtopics

Kerberos authentication with iLO

Directory integration benefits

Choosing a directory configuration to use with iLO

Schema-free directory authentication

HPE Extended Schema directory authentication

User login using directory services

Tools for configuring multiple iLO systems at a time

Directories Support for ProLiant Management Processors (HPLOMIG)

Configuring directory authentication with HPLOMIG

Directory services schema

Kerberos authentication with iLO

NOTE: iLO 6 1.05 does not support Kerberos.

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.

Subtopics

Configuring Kerberos authentication

Configuring the iLO hostname and domain name for Kerberos authentication

Preparing the domain controller for Kerberos support

Generating a keytab file for iLO in a Windows environment

Verifying that your environment meets the Kerberos authentication time requirement

Configuring supported browsers for single sign-on

Configuring Kerberos authentication

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 Kerberos parameters in iLO.
7. Configure iLO directory groups.
8. Configure supported browsers for single-sign-on

Configuring the iLO hostname and domain name for Kerberos authentication

About this task

Use the following procedure if a DHCP server does not provide the domain name or DNS servers you want to use.

Procedure

1. Click iLO Dedicated Network Port in the navigation tree.
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.

Subtopics

iLO hostname and domain name requirements for Kerberos authentication

More information

Configuring the iLO Hostname Settings
iLO hostname and domain name limitations
iLO hostname and domain name requirements for Kerberos authentication

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

About this task

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.
2. 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`
3. Ensure that a user account exists in the domain directory for each user who is allowed to log in to iLO.
4. 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.

Subtopics

Ktpass

Setspn

More information

Ktpass
Setspn

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.

`-crypto <encryption>`

Specifies the encryption of the keys generated in the `.keytab` file.

If iLO is configured to use the High Security, FIPS, or CNSA security state, you must use an AES Kerberos key type.

`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

About this task

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.

Subtopics

Enabling single sign-on in Mozilla Firefox

Single-sign on with Google Chrome

Enabling single sign-on in Microsoft Edge

Verifying the single sign-on (Zero Sign In) configuration

Verifying that login by name works

More information

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

About this task

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.

More information

Schema-free directory authentication
HPE Extended Schema directory authentication

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.

Subtopics

Configuring directory integration (schema free configuration)

Prerequisites for using schema-free directory integration

Configuring directory integration (schema free configuration)

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.

Subtopics

Directory services support

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 directory integration (HPE Extended Schema configuration)

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. Install the required software:
      - Install Directories Support for ProLiant Management Processors (HPLOMIG)
      - Install HPE Management Devices Schema Extender (Schema Extender)
      - Install HPE Management Devices Directory Snap-ins (x86 and x64)

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.

More information

Configuring Active Directory and HPE Extended Schema (Example configuration)

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

About this task

You can download the directory support software from HPE Support Center:

- Installing Directories Support for ProLiant Management Processors (HPLOMIG)
- HPE Management Devices Schema Extender (Schema Extender)
- Installing HPE Management Devices Directory Snap-ins

Subtopics

Installing Directories Support for ProLiant Management Processors (HPLOMIG)

Installing HPE Management Devices Schema Extender

Installing HPE Management Devices Directory Snap-ins

Directories Support for ProLiant Management Processors install options

More information

Directories Support for ProLiant Management Processors (HPLOMIG)
Running the Schema Extender

Management options added by the HPE Active Directory snap-ins

Installing Directories Support for ProLiant Management Processors (HPLOMIG)

About this task

Procedure

1. Download Directories Support for ProLiant Management Processors (HPLOMIG) from **Directories Support for ProLiant Management Processors**.
2. In the Welcome window, click Next.
3. In the License Agreement window, select I Agree, and then click Next.
4. In the Select Installation Folder window, select the installation directory and user preference, and then click Next.
5. When prompted to confirm the installation request, click Next.

   The Click Close. Installation Complete window opens.
6. Click Close.

Installing HPE Management Devices Schema Extender

About this task

Procedure

1. Download HPE Management Devices Schema Extender (Schema Extender) from **HPE Management Devices Schema Extender**.
2. In the Welcome window, click Next.
3. In the License Agreement window, select I Agree, and then click Next.
4. In the Select Installation Folder window, select the installation directory and user preference, and then click Next.
5. When prompted to confirm the installation request, click Next.

   The Click Close. Installation Complete window opens.
6. Click Close.

Installing HPE Management Devices Directory Snap-ins

About this task

Procedure

1. Download the required software from HPE Support Center:
   a. **HPE Management Devices Directory Snap-ins 32-bit(Snap-in x86)**
   b. **HPE Management Devices Directory Snap-ins 64-bit (Snap-in x64)**
2. In the Welcome window, click Next.
3. In the License Agreement window, select I Agree, and then click Next.

4. Read the details in the Information window, and then click Next.
5. When prompted to confirm the installation request, click Next.

   The Click Close. Installation Complete window opens.
6. Click Close.

   After the snap-ins are installed, you can create iLO objects and iLO roles in the directory. Install HPE Management Devices Directory Snap-ins on each computer that will be used to manage directory objects. For more information, see Directory services objects.

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.

Subtopics

Schema Extender required information

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.

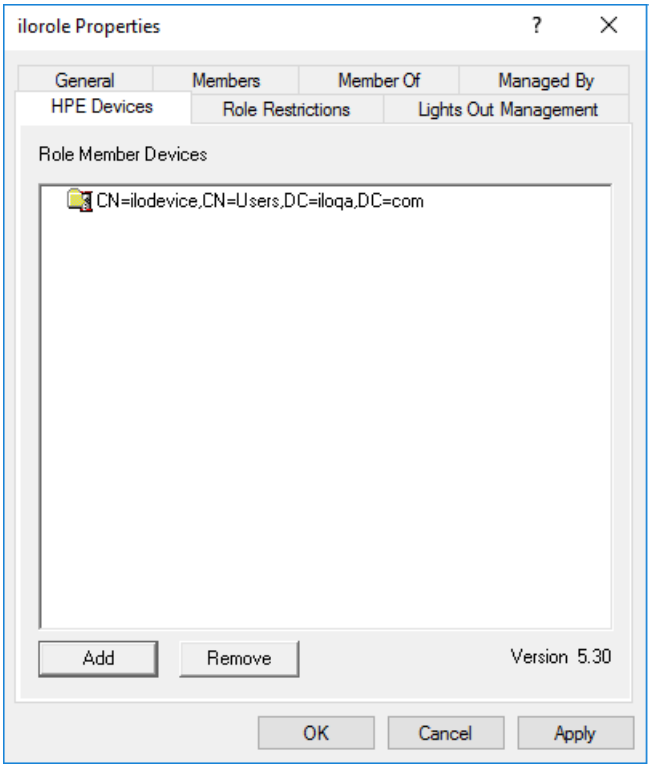
More information

Configuring Active Directory and HPE Extended Schema (Example configuration)
Management options added by the HPE Active Directory snap-ins
Directory-enabled remote management (HPE Extended Schema configuration)
Roles based on organizational structure

Management options added by the HPE Active Directory snap-ins

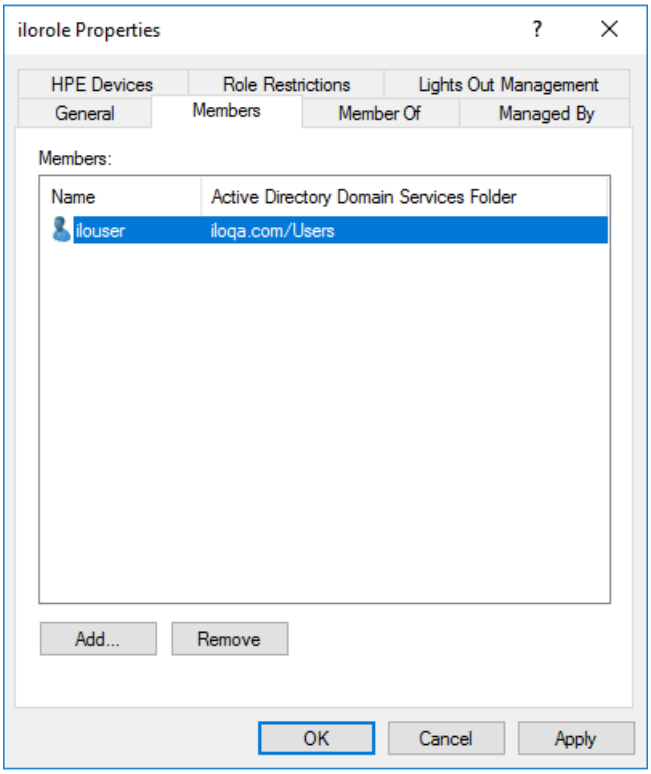
The following management options are available in Active Directory Users and Computers after you install the Hewlett Packard Enterprise snap-ins.

Devices tab



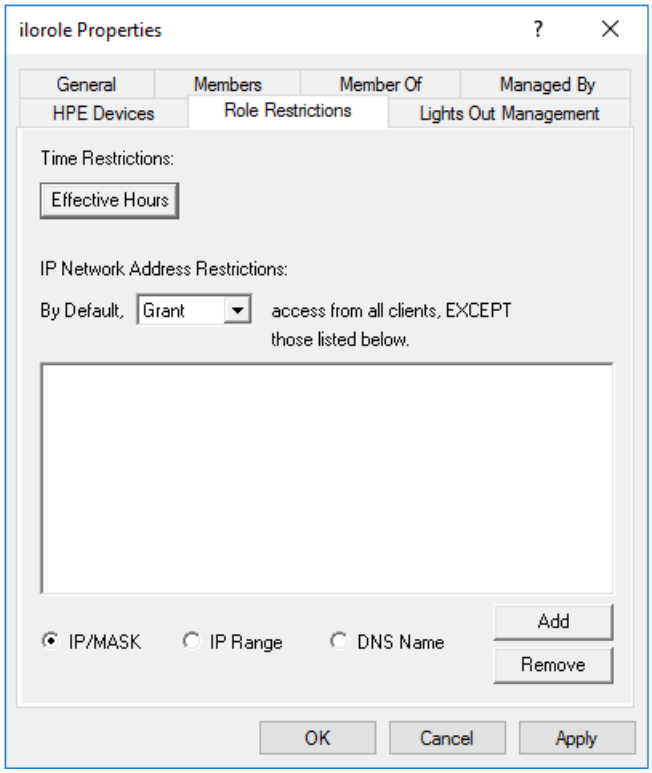
This tab enables you to add the Hewlett Packard Enterprise devices to be managed within a role. Clicking Add enables you to navigate to a device and add it to the list of member devices. Selecting an existing device and clicking Remove removes the device from the list of valid member devices.

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.

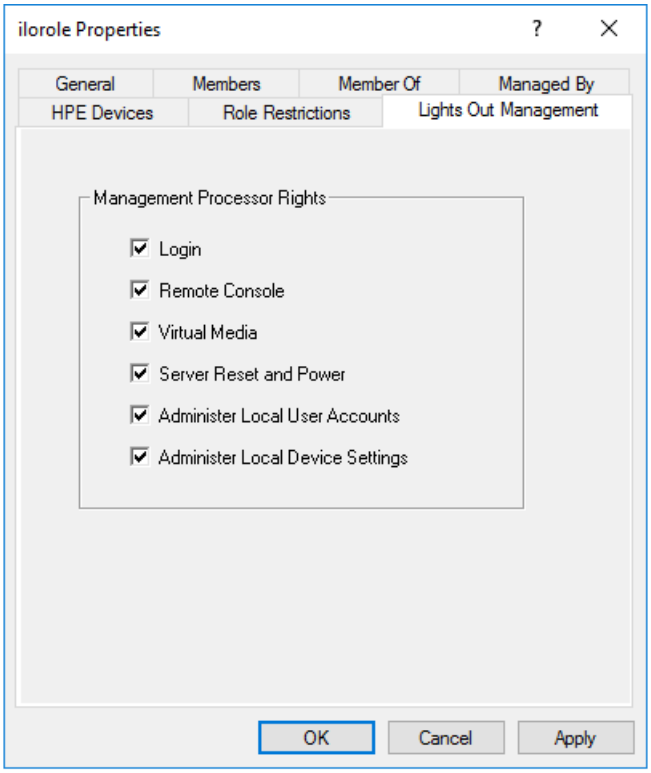
Role Restrictions tab



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.

NOTE:
The System Recovery, Host NIC, Host Storage, and Host BIOS privileges are not available in the Schema Extender.

Subtopics

Setting a client IP address or DNS name restriction

Setting a client IP address or DNS name restriction

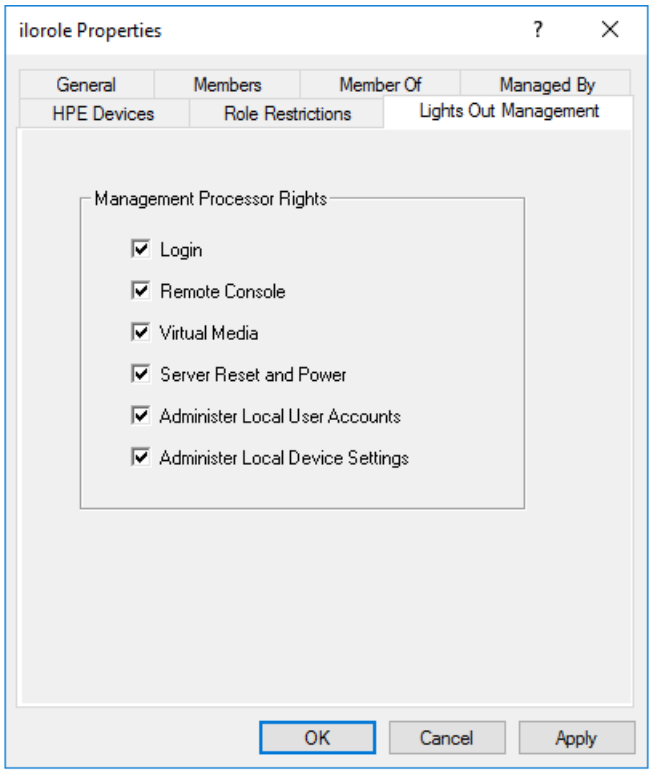
Procedure

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.

Subtopics

Roles based on organizational structure

How role access restrictions are enforced

User access restrictions

Role access restrictions

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

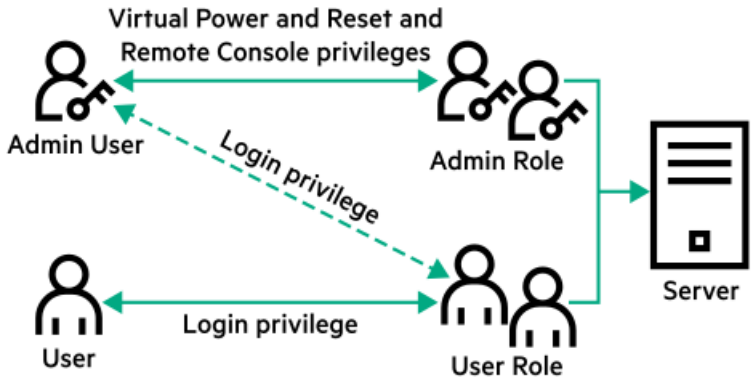
Most deployments do not require that the same user must be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can 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.

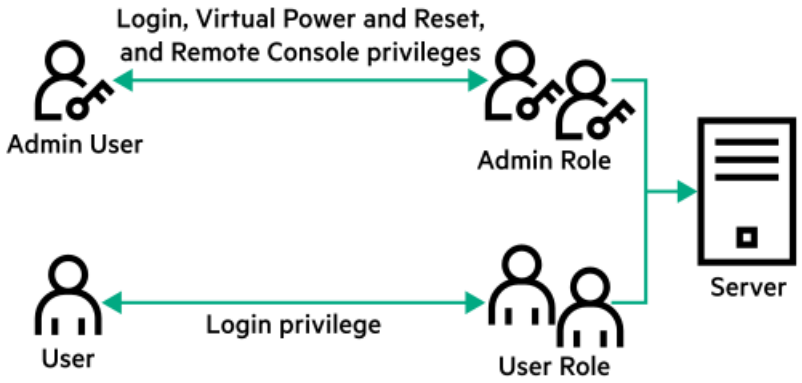
Multiple roles (overlapping) shows an example in which the Admin user gains the Login privilege from the User role, and advanced privileges are assigned through the Admin role.

Figure 1. 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 Multiple roles (separate).

Figure 2. Multiple roles (separate)

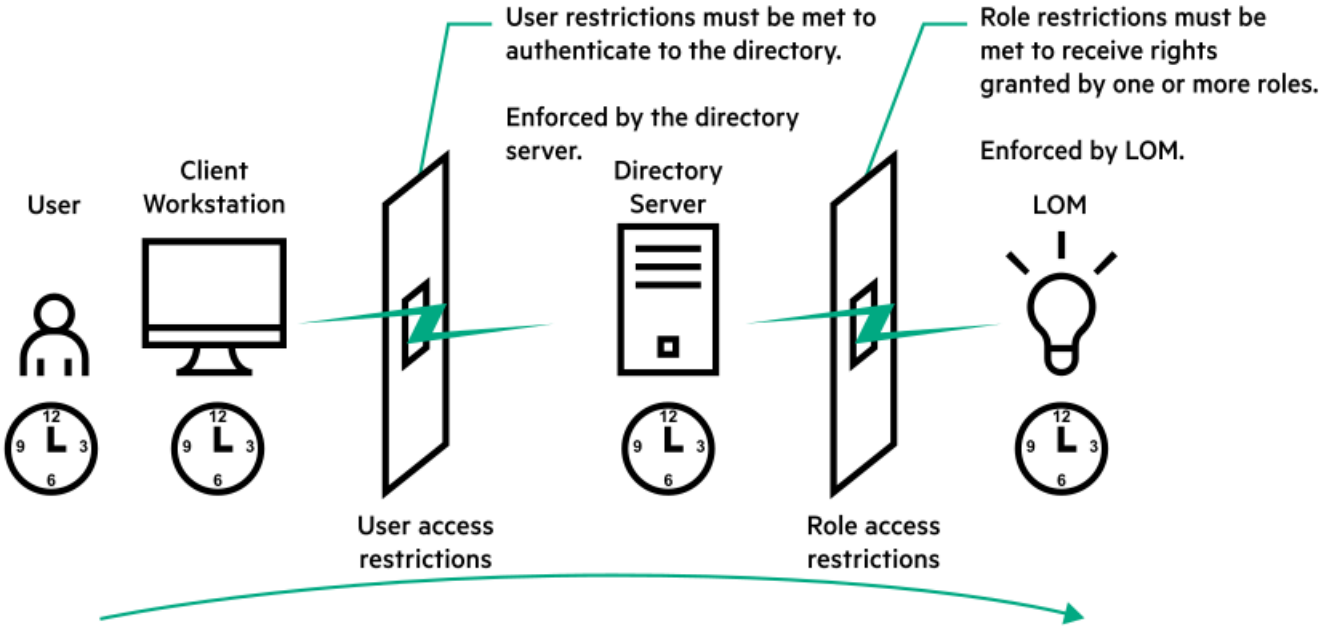


How role access restrictions are enforced

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 1. 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.

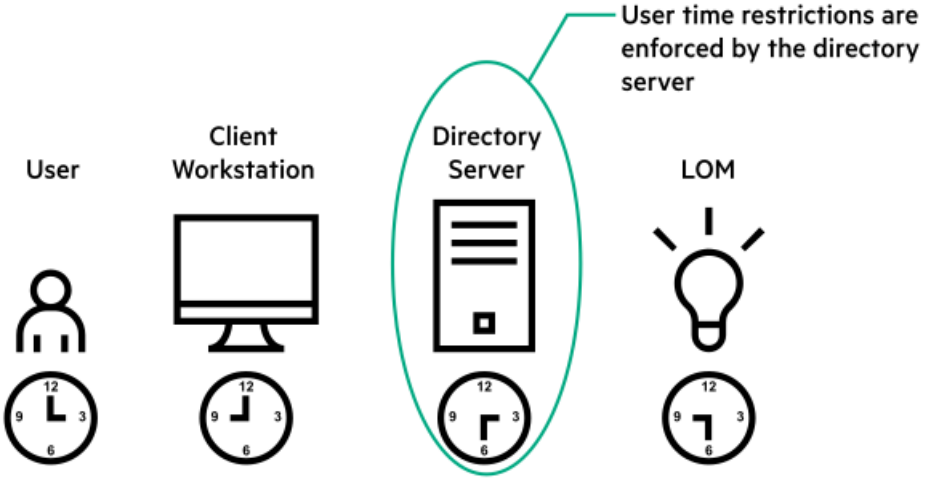
Using DNS-based restrictions might create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address 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 1. User time restrictions



Role access restrictions

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users 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

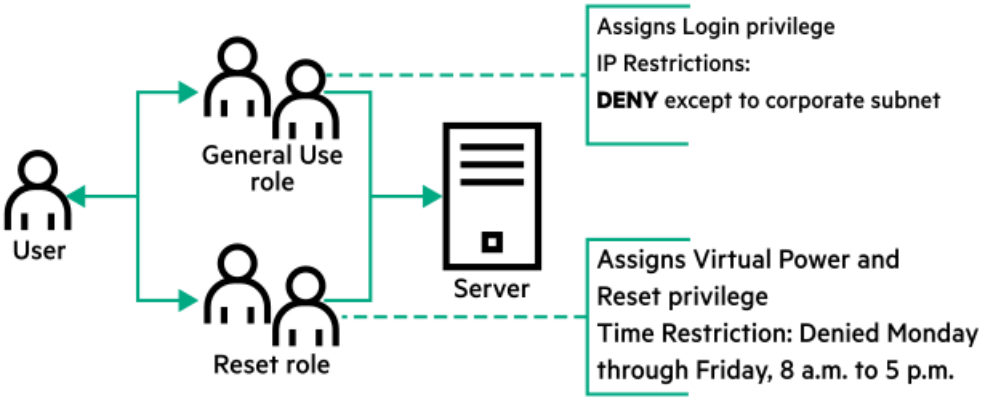
The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships 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.

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.

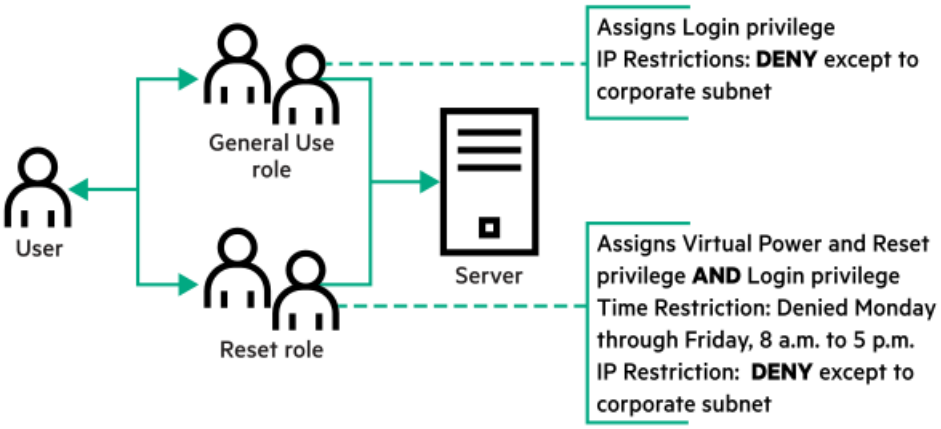
Figure 1. Creating restrictions and roles



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 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 Restricting the Reset and General Use roles.

Figure 2. Restricting the Reset and General Use roles



Configuring Active Directory and HPE Extended Schema (Example configuration)

About this task

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.

Subtopics

Creating and configuring directory objects for use with iLO in Active Directory

Configuring iLO and associating it with a Lights-Out Management object

Creating and configuring directory objects for use with iLO in Active Directory

About this task

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.

Subtopics

Creating the iLOs organizational unit and adding LOM objects

Creating the Roles organizational unit and adding role objects

Assigning rights to the roles and associating the roles with users and devices

More information

Management options added by the HPE Active Directory snap-ins
Directory services objects

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
```

More information

Configuring HPE Extended Schema directory settings in iLO

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.

More information

Directories Support for ProLiant Management Processors (HPLOMIG)
Configuring directory authentication with HPLOMIG
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: **https://www.hpe.com/support/ilo6**

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 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Requirements

If enhanced security features, such as the FIPS, CNSA, or High Security security states, 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.

  NOTE: For TLS 1.3, minimum .NET framework version is 4.8

- The operating system supports TLS v1.1, TLS v1.2, or TLS v1.3.

The following table lists the OS and Windows .NET Framework requirements for using HPLOMIG:

Operating system	Windows .NET Framework	HPLOMIG with the Production security state enabled in iLO.	HPLOMIG with the High Security, FIPS, or CNSA security state enabled in iLO.
Windows 7	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 Microsoft Windows Server 2022	4.0 or earlier	Supported	Not Supported
	4.5	Supported	Supported

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.

Subtopics

Discovering management processors

(Optional) Upgrading firmware on management processors (HPLOMIG)

Selecting directory configuration options

Naming management processors (HPE Extended Schema only)

Configuring directories when HPE Extended Schema is selected

Configuring management processors (Schema-free configuration only)

Setting up management processors for directories

Importing an LDAP CA Certificate

(Optional) Running directory tests with HPLOMIG

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.

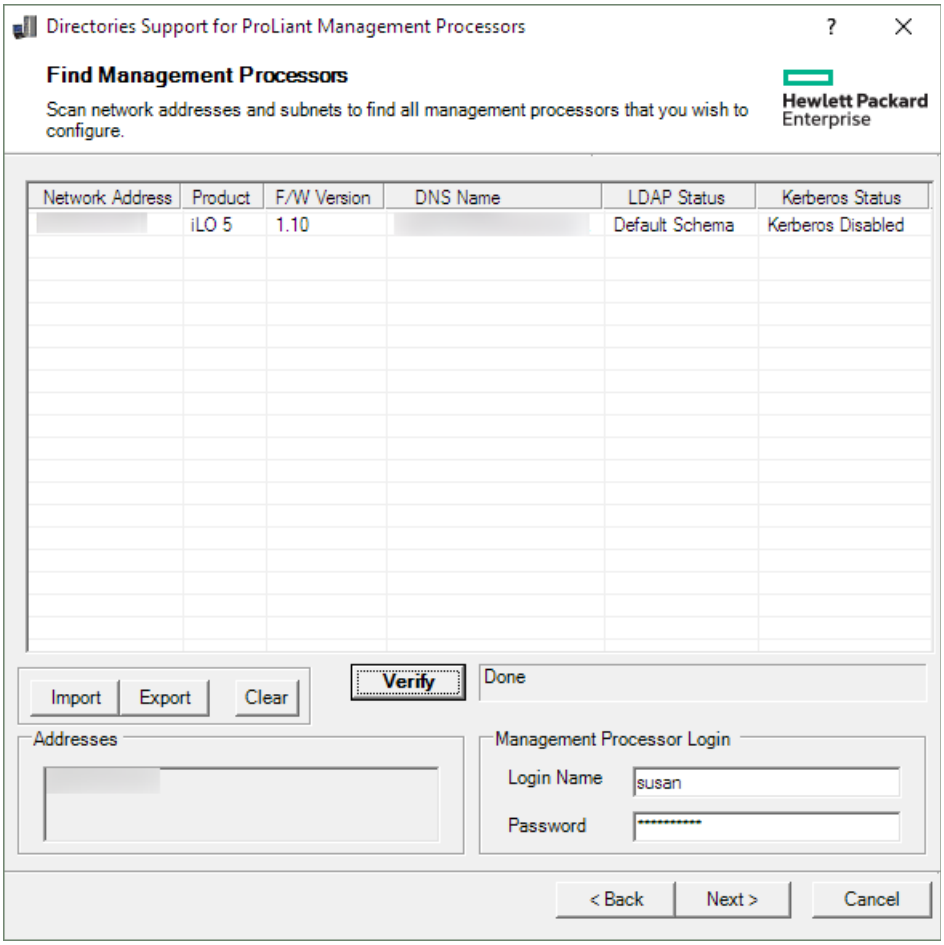
   TIP:

   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.



Subtopics

[HPLOMIG management processor search criteria](#)

[HPLOMIG management processor import list requirements](#)

HPLOMIG management processor search criteria

You can search for management processors by using DNS names, IP addresses, or IP address wildcards.

The following rules apply when you enter values in the Addresses box:

- DNS names, IP addresses, and IP address wildcards must be delimited either with semicolons or commas, not both.
- The IP address wildcard uses the asterisk (*) character in the third and fourth octet fields. For example, IP address `16.100.*.*` is valid, and IP address `16.*.*.*` is invalid.
- Ranges can be specified by using a hyphen. For example, `192.168.0.2-10` is a valid range. A hyphen is supported only in the rightmost octet.
- After you click Find, HPLOMIG begins pinging and connecting to port 443 (the default SSL port) to determine whether the target network address is a management processor. If the device does not respond to the ping or connect appropriately on port 443, the utility determines that it is not a management processor.

HPLOMIG management processor import list requirements

You can import a simple text file with one management processor listed on each line.

The supported columns, which are delimited with semicolons, follow:

- Network Address
- Product
- F/W Version
- DNS Name
- TPM Status
- User Name
- Password
- LDAP Status
- Kerberos Status
- License Type
- FIPS Status

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;Enabled
```

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)

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 **https://www.hpe.com/support/ilo6**.

About this task

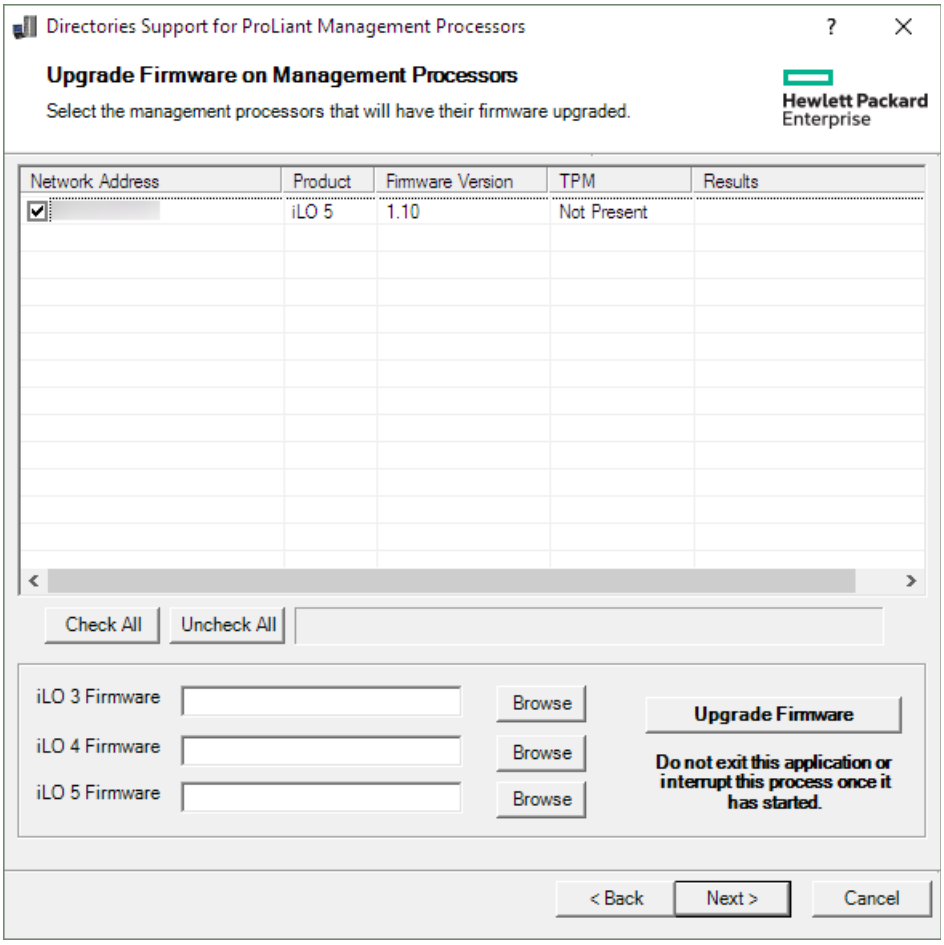
After you click Next in the Find Management Processors window, the next task is to update the iLO firmware, if needed. The upgrade process might take a long time, depending on the number of selected management processors. The firmware upgrade of a single management processor might take up to 5 minutes 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.

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.

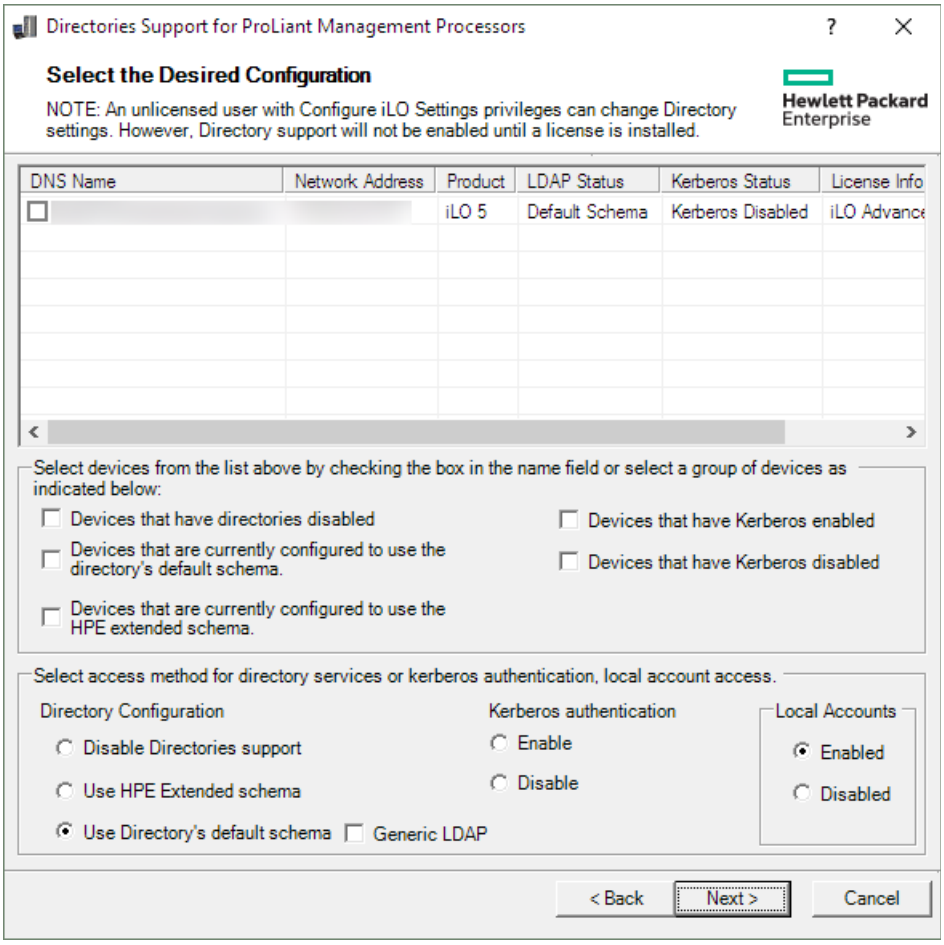
Selecting directory configuration options

About this task

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).

Subtopics

Management processor selection methods

Directory access methods and settings

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)

About this task

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.

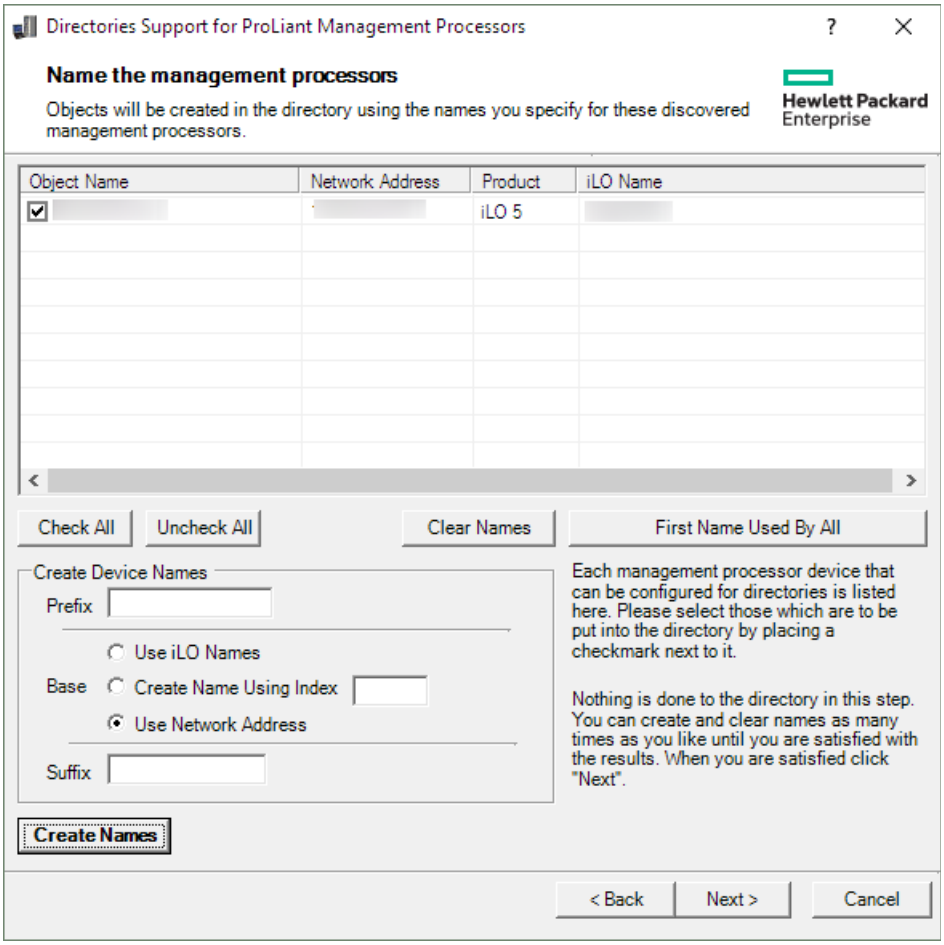
You can create names by using one or more of the following:

- 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.

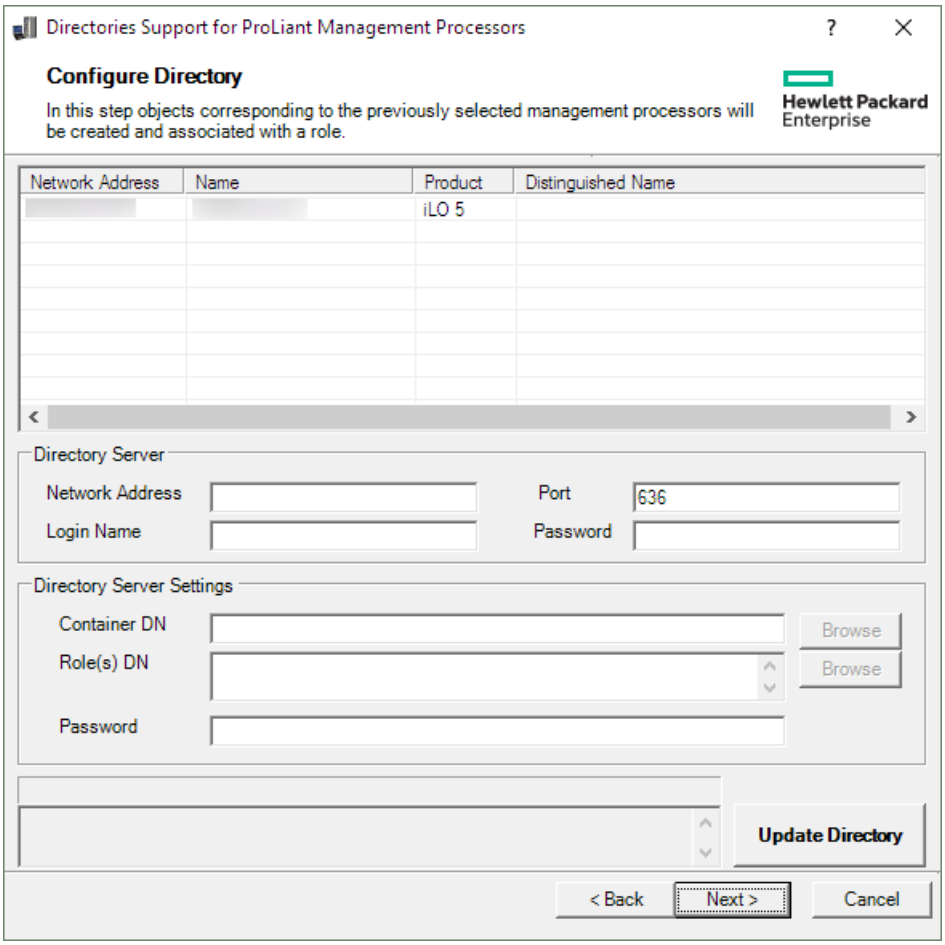
4. (Optional) To change the names, click Clear Names, and rename the management processors.
5. When the names are correct, click Next.

   The Configure Directory window opens. Continue with Configuring directories when HPE Extended Schema is selected.

Configuring directories when HPE Extended Schema is selected

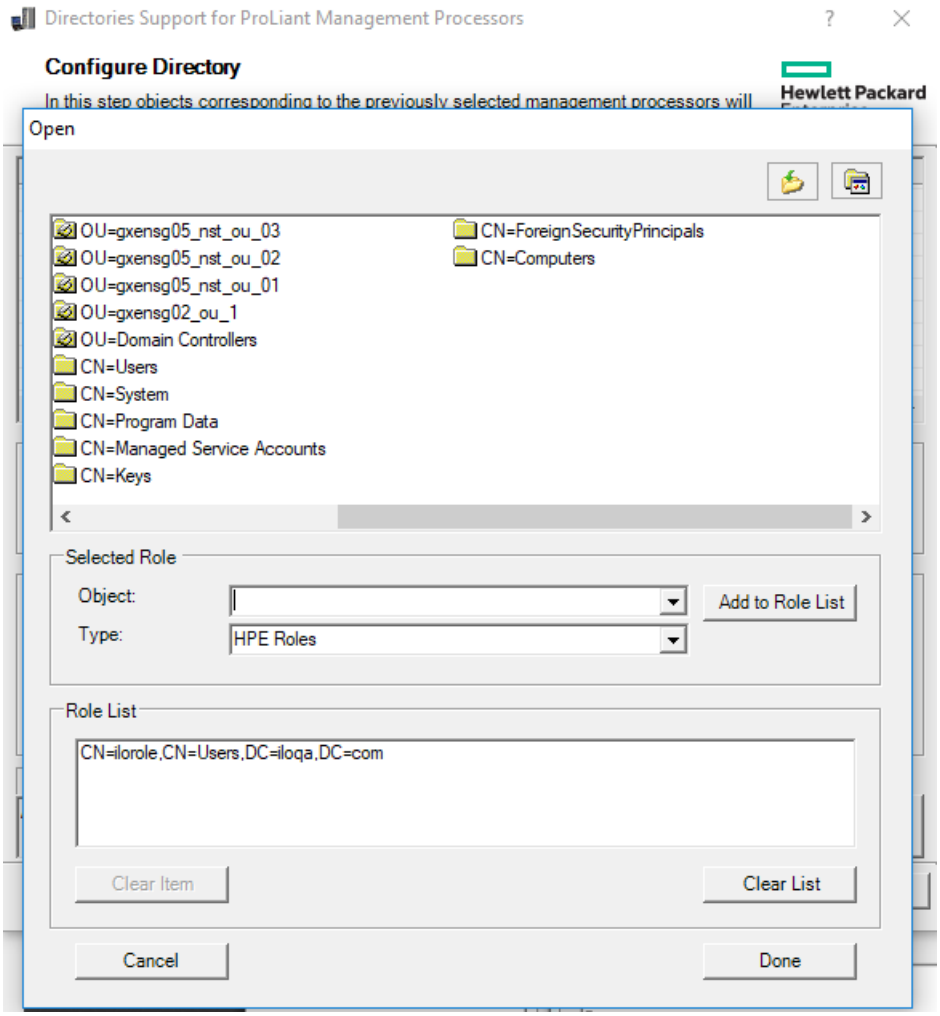
About this task

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.

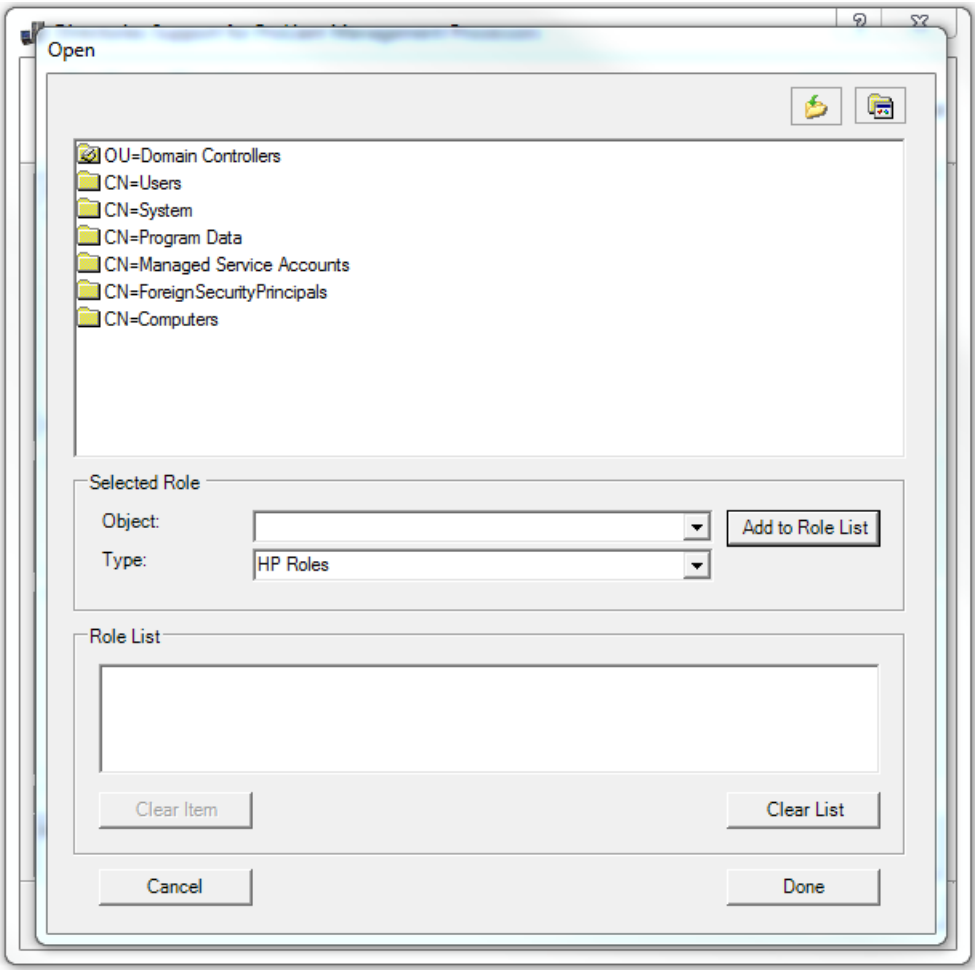


Procedure

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.

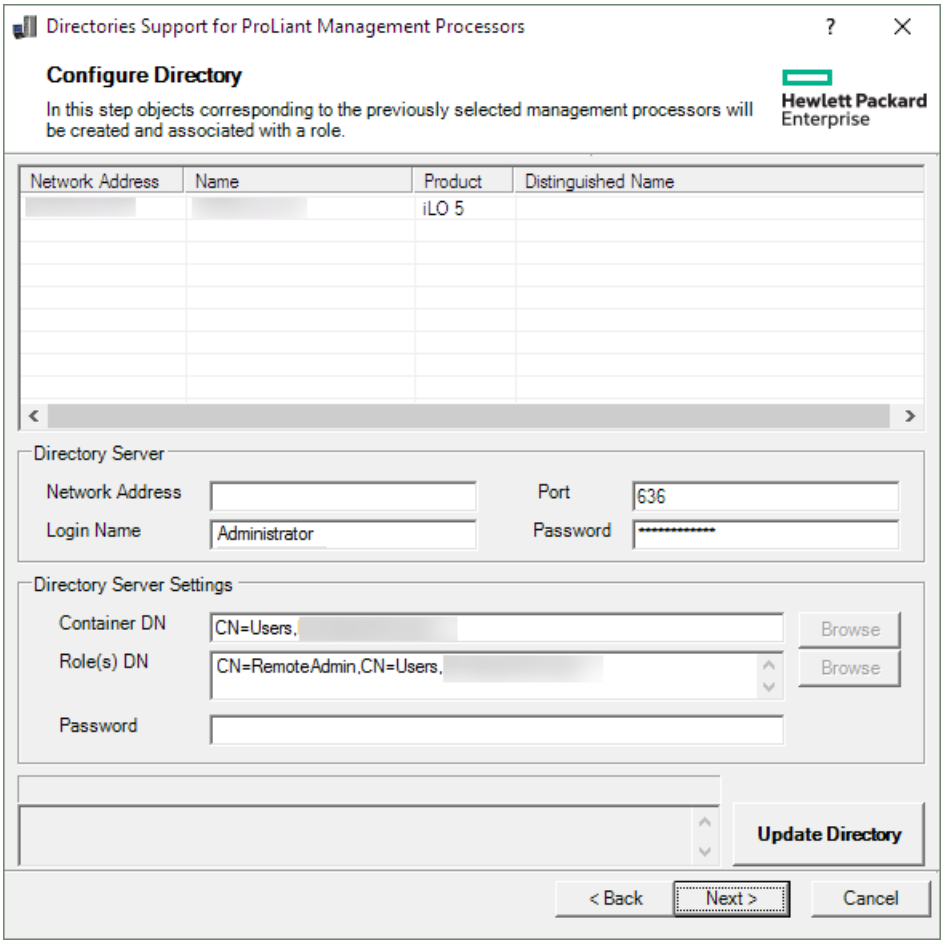


4. Click Update Directory.

   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 .

Subtopics

Configure directory window options

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.

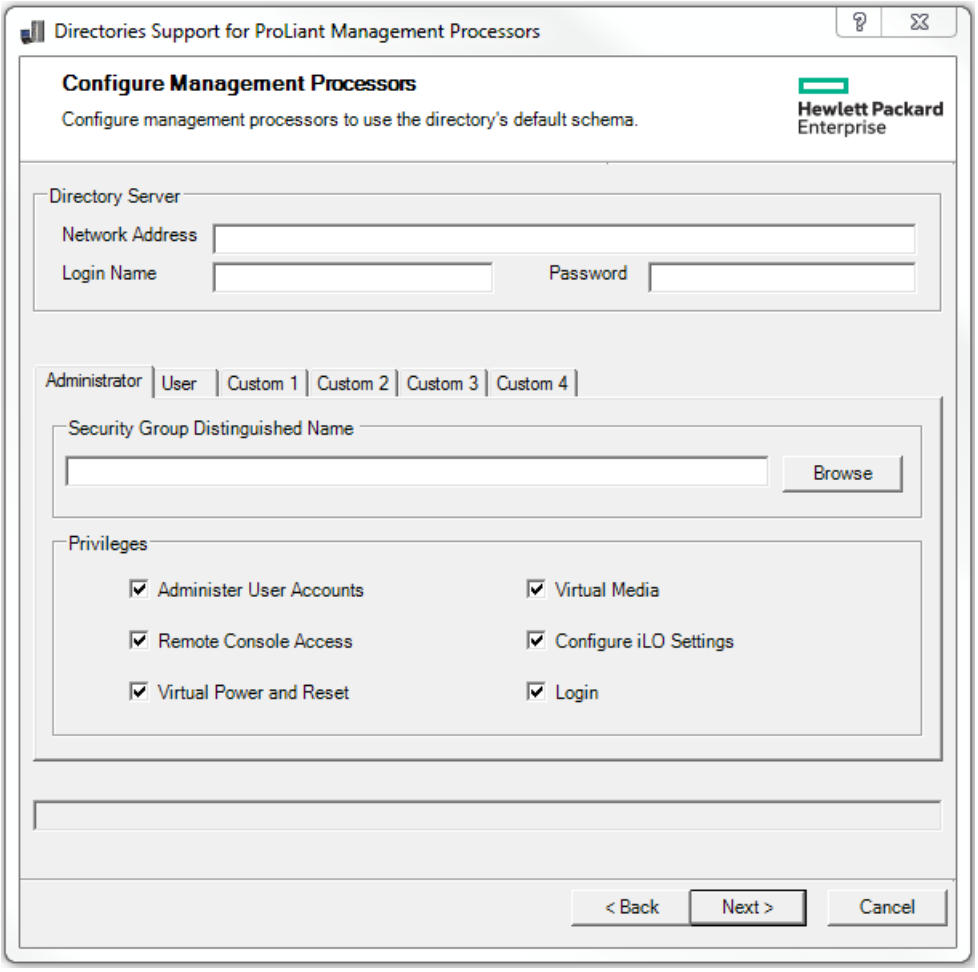
Configuring management processors (Schema-free configuration only)

About this task

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 .

Subtopics

Management processor settings

Management processor settings

- Network Address—The network address of the directory server, which can be a valid DNS name or IP address.

- Login Name and Password—Enter the login name (DN) and password for an account that has domain administrator access to the directory.
- Security Group Distinguished Name—The DN of the group in the directory that contains a set of iLO users with a common set of privileges. If the directory name, login name, and password are correct, you can click Browse to navigate to and select the group.
- Privileges—The iLO privileges associated with the selected group. If the user is a member of the group, the login privilege is implied.

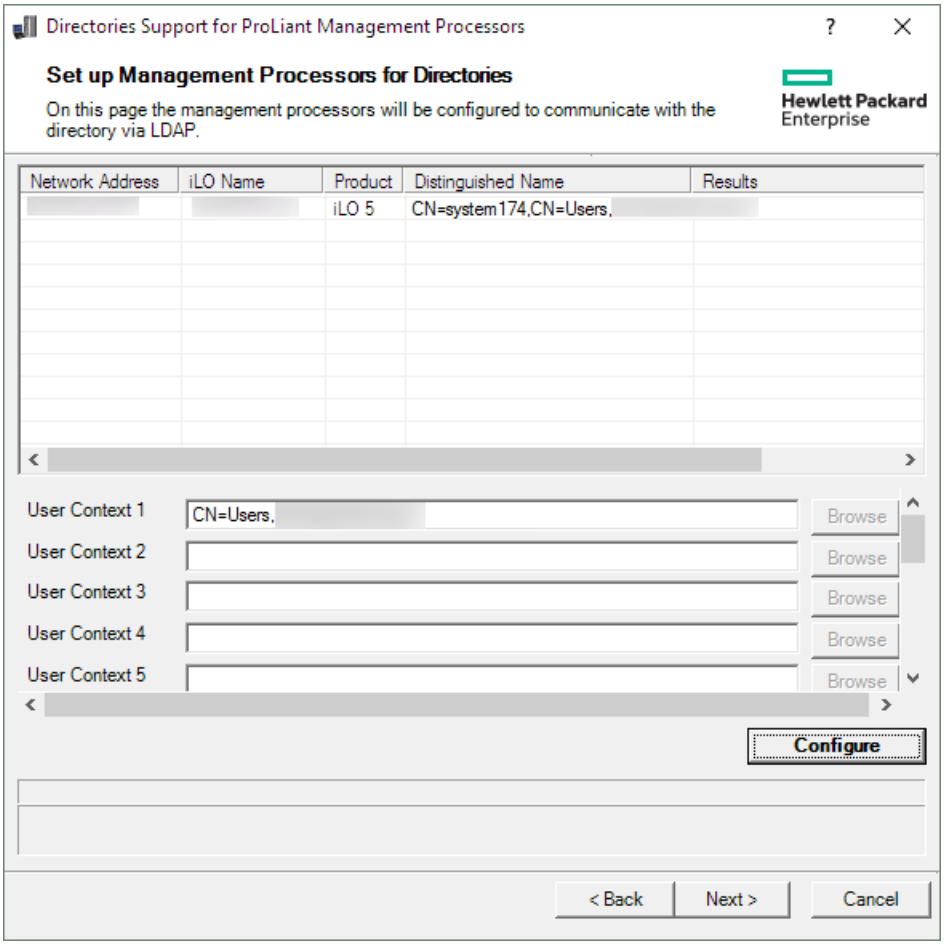
Setting up management processors for directories

About this task

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.

More information

Directory user contexts

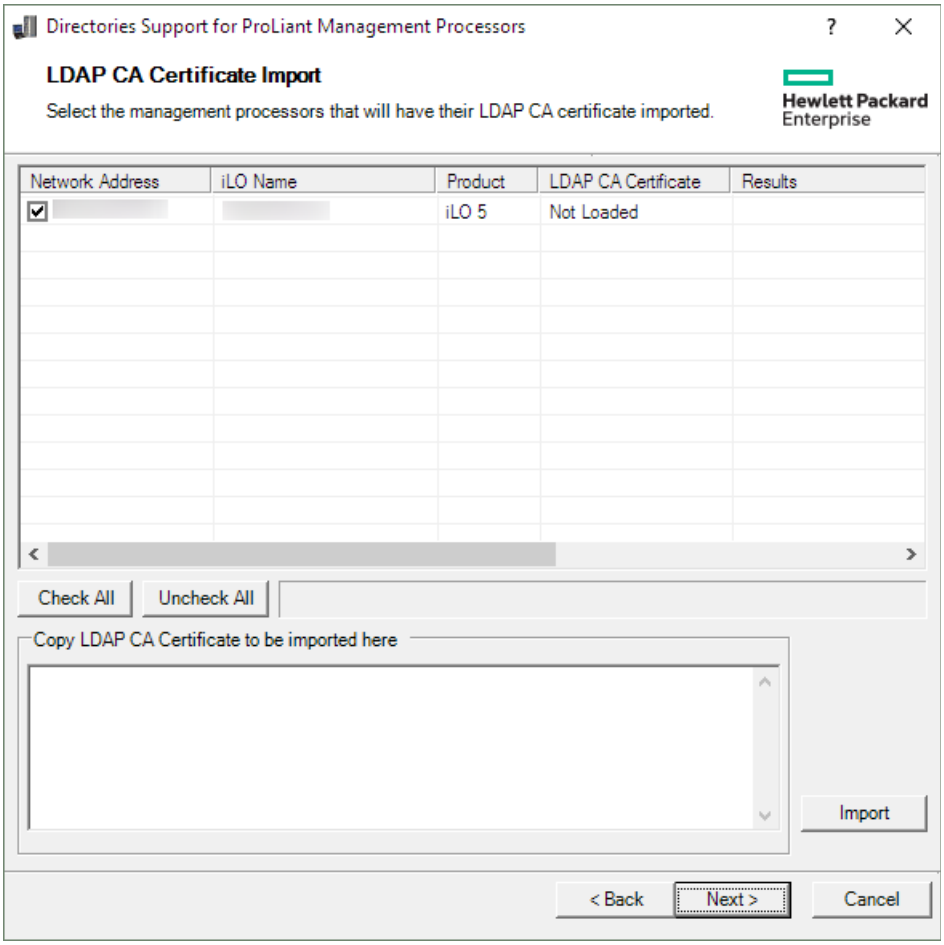
Importing an LDAP CA Certificate

About this task

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.

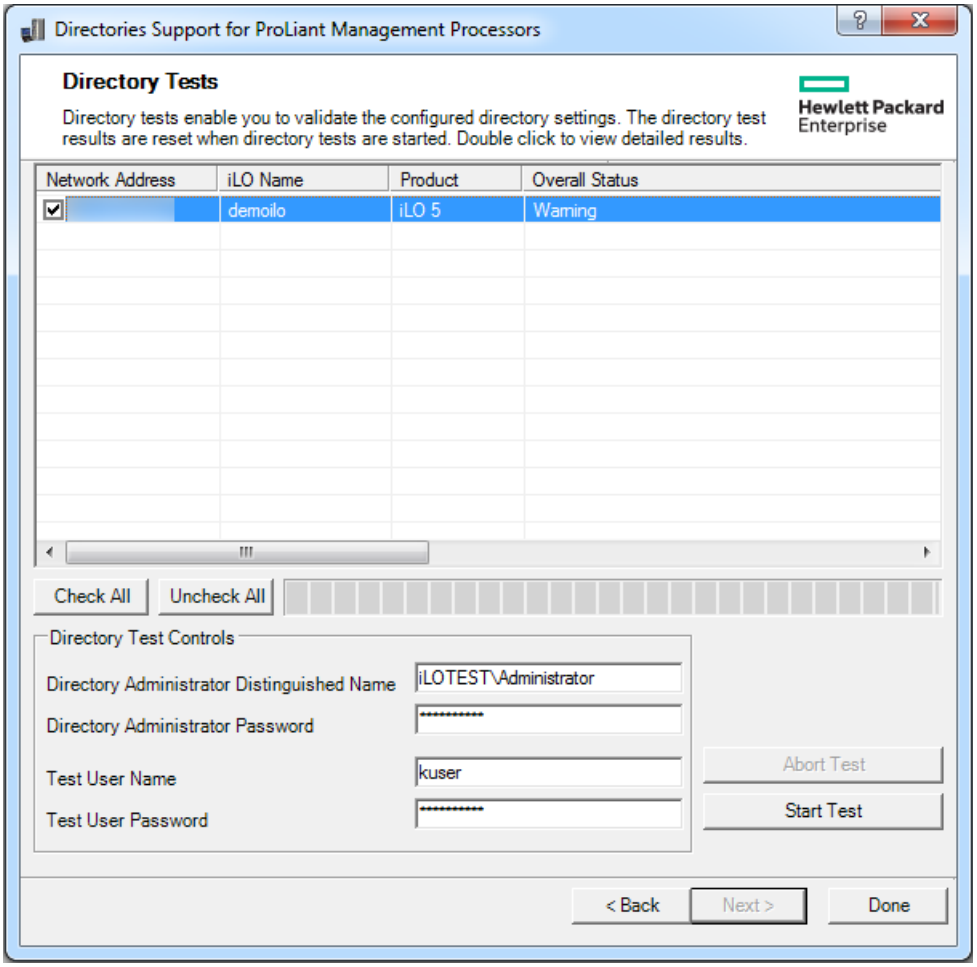
(Optional) Running directory tests with HPLOMIG

About this task

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.

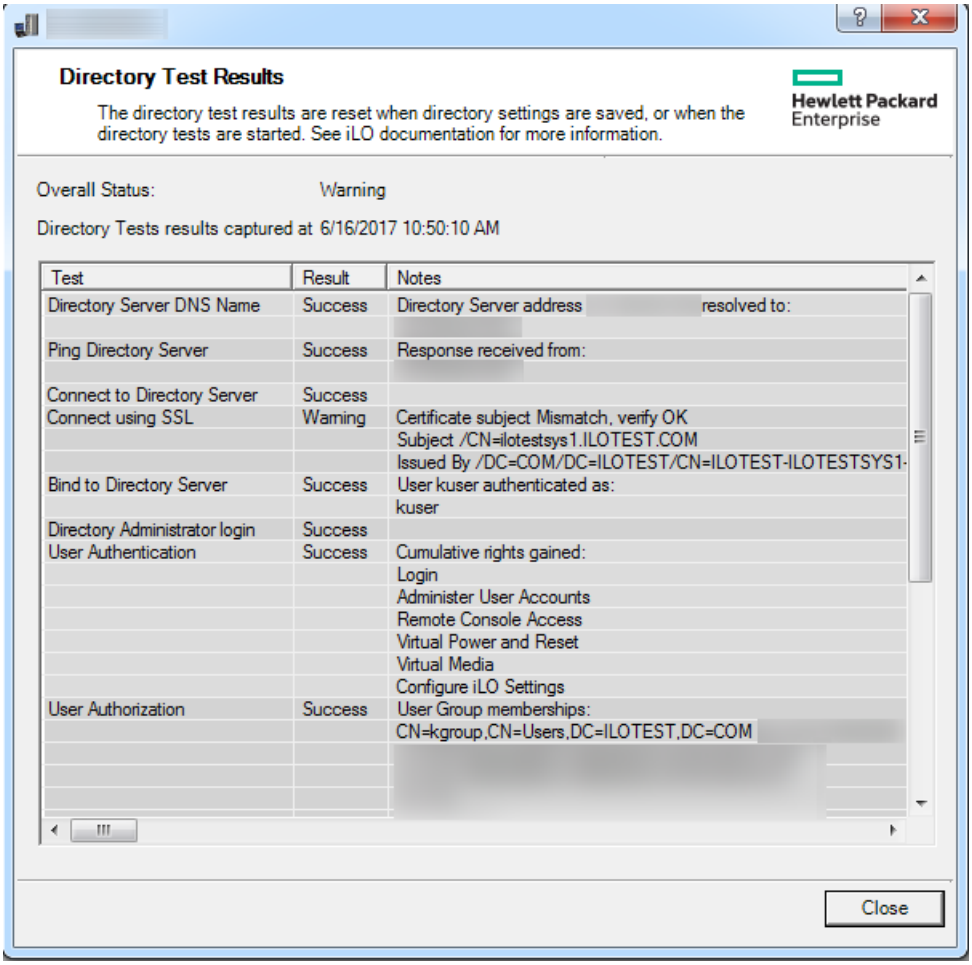


2. Test the directory settings.
   a. Select one or more iLO systems
   b. In the Directory Test Controls section, enter the following:
      - Directory Administrator Distinguished Name and Directory Administrator Password—Searches the directory for iLO objects, roles, and search contexts. This user 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.

Subtopics

HPE Management Core LDAP OID classes and attributes

Core class definitions

Core attribute definitions

Lights-Out Management specific LDAP OID classes and attributes

Lights-Out Management attributes

Lights-Out Management class definitions

Lights-Out Management attribute definitions

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 1. 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 1. 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.

iLO factory default reset

In some cases, you might need to reset iLO to the factory default settings. For example, you must reset iLO to the factory default settings when you disable the FIPS security state.

Factory default reset methods

- iLO 6 Configuration Utility—Access this feature through 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 instructions, see the HPE iLO 6 Scripting and Command Line Guide.

Subtopics

Resetting iLO to the factory default settings (iLO 6 Configuration Utility)

More information

Resetting iLO to the factory default settings (iLO 6 Configuration Utility)

Resetting iLO to the factory default settings (iLO 6 Configuration Utility)

About this task

> **CAUTION:**
>
> When you reset iLO to the factory default settings, all iLO settings are erased, including user and license data, configuration settings, and logs. If the server has a factory installed license key, the license key is retained.
>
> Events related to the reset are not logged to the iLO Event Log and Integrated Management Log because this step clears all the data in the logs.

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, click System Configuration, and then click iLO 6 Configuration Utility.
5. Select Yes in the Set to factory defaults menu.

   The iLO 6 Configuration Utility prompts you to confirm the request.
6. Click OK.
7. iLO resets to the factory default settings. If you are managing iLO remotely, the Remote Console session is automatically ended. You cannot access the iLO 6 Configuration Utility again until after the next system reboot.
8. Resume the boot process:
   a. (Optional) If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The iLO 6 Configuration Utility screen is still open from the previous session.
   b. Press Esc until the main menu is displayed.
   c. Click Exit and resume system boot.
   d. When prompted to confirm the request, click OK to exit the screen and resume the boot process.
9. (Optional) Use the default iLO account information to log in to iLO after the reset.
10. Reboot the server operating system.

    During the reset to the factory default settings, SMBIOS records are cleared. Memory and network information will not be displayed in the iLO web interface until the server OS reboot is complete.

    The performance management Processor Jitter Control Optimization feature is unavailable until the server OS reboot is complete.

    HPE ProLiant RL3xx Gen 11 platforms do not support Processor Jitter Control.

Websites

iLO

https://www.hpe.com/info/ilo

iLO 6 documentation

https://www.hpe.com/support/ilo6

RL300Gen11 documentation

https://www.hpe.com/info/RL300Gen11-docs

iLO helpful links and resources

https://www.hpe.com/support/ilo-resource-ref-en

HPE iLO Free Online Training

https://www.hpe.com/ww/iloBundle

HPE iLO Documentation Map

https://www.hpe.com/support/ilo-server-lifecycle-management

HPE ProLiant training

https://www.hpe.com/ww/learnproliant

UEFI System Utilities

https://www.hpe.com/info/ProLiantUEFI/docs

SUM

https://www.hpe.com/info/sum-docs

SPP

https://www.hpe.com/info/spp/documentation

Intelligent Provisioning

https://www.hpe.com/info/intelligentprovisioning/docs

iLO RESTful API and RESTful Interface Tool

https://www.hpe.com/support/restfulinterface/docs

Remote Support

https://www.hpe.com/info/insightremotesupport/docs

HPE InfoSight for Servers

https://www.hpe.com/servers/infosight

iLO Amplifier Pack

https://www.hpe.com/servers/iloamplifierpack

HPE OneView

https://www.hpe.com/info/oneview/docs

HPE SIM

https://www.hpe.com/info/insightmanagement/sim/docs

Support and other resources

Subtopics

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

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

https://www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Account set up with relevant entitlements.

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which initiates a fast and accurate resolution based on the service level of your product. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Tech Care Service

https://www.hpe.com/services/techcare

HPE Complete Care Service

https://www.hpe.com/services/completecare

Warranty information

To view the warranty information for your product, see the warranty check tool.

Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

https://www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the Feedback button and icons (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.