Hewlett Packard
Enterprise

iLO Amplifier Pack 1.30 User Guide

Abstract

This guide provides information about installing, configuring, and operating the iLO Amplifier Pack.

Part Number: P04465-004
Published: January 2019
Edition: 1

Notices

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

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

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

Acknowledgments

Intel®, Itanium®, Pentium®, Xeon®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Contents

Introduction

Description

The iLO Amplifier Pack is an advanced server inventory, firmware and driver update solution that enables rapid discovery, detailed inventory reporting, firmware, and driver updates by leveraging iLO advanced functionality. 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.

iLO Amplifier Pack key features

- **Server System Restore**—iLO Amplifier Pack works with iLO 5 v1.17 to initiate and manage system recovery processes for servers.
- **Gen10 server support**—iLO Amplifier Pack supports HPE ProLiant Gen8 and Gen9 servers. As of version 1.10, iLO Amplifier Pack also offers full support for HPE ProLiant Gen10 servers.
- **Baseline importing**—Starting with v1.15, iLO Amplifier Pack provides up to 80 GB of storage for imported baseline images for easy access during deployment.
- **Detailed inventory**—iLO Amplifier Pack scales up to thousands of servers and runs basic and detailed inventory on HPE ProLiant Gen8, Gen9, and Gen10 servers, including firmware, hardware, and iLO licenses in a matter of minutes.
- **SPP compliance report**— iLO Amplifier Pack allows users to generate SPP compliance reports for multiple servers at a time. This report provides information about the compliance status of a server and displays the server compliance of the firmware and software components for an imported SPP.
- **IPv6 support**—As of version 1.30, iLO Amplifier Pack is IPv6 compliant. Users can now use IPv6 addresses when adding servers or configuring various iLO Amplifier Pack network settings.
- **Simplified updates**—iLO Amplifier Pack simplifies update management tasks making it easier and faster with a user interface that is similar to iLO. Users can update multiple servers on both iLO Federation and server groups reducing downtime and personnel requirements.
- **Group management**—iLO Amplifier Pack can create new groups, add servers to existing groups, and manage the updates for federated groups and server groups.
- **InfoSight integration**—iLO Amplifier Pack version 1.30 onwards supports HPE InfoSight integration to manage HPE ProLiant servers. HPE InfoSight is an artificial intelligence (AI) platform that employs cloud-based machine learning to analyze diagnostic data from iLO Amplifier Pack.

iLO Amplifier Pack license segmentation

iLO Amplifier Pack does not require a separate license; it is a free download. Full functionality of the iLO Amplifier Pack is available with an iLO Advanced license. The following features are available for iLO Standard, iLO Essentials, and iLO Scale-Out licenses.

Feature	iLO Standard iLO Essentials iLO Scale-Out	iLO Advanced	Dependencies
Discovery	✓	✓	• iLO 4 v2.30 and later for Gen8 and Gen9 servers • iLO 5 v1.10 and later for Gen10 servers
Inventory	✓	✓	• iLO 4 v2.50 and later for Gen8 and Gen9 servers • iLO 5 v1.10 and later for Gen10 servers
Reports	✓	✓	• iLO 4 v2.50 and later for Gen8 and Gen9 servers • iLO 5 v1.10 and later for Gen10 servers
Core platform firmware update	✓	✓	• iLO 4 v2.30 and later for Gen8 and Gen9 servers • iLO 5 v1.10 and later for Gen10 servers
Core platform firmware update with iLO Federation		✓	• iLO 4 v2.30 and later for Gen8 and Gen9 servers • iLO 5 v1.10 and later for Gen10 servers
Online update for firmware, drivers, and HPE software		✓	• iLO 4 v2.53 and later for Gen8 and Gen9 servers • AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on Gen8 or Gen9 servers • HPE Service Pack for ProLiant • HPE SUT v1.8.0 or later for Gen8, Gen9 servers

Table Continued

Feature	iLO Standard iLO Essentials iLO Scale-Out	iLO Advanced	Dependencies
iLO Repository Online Update		✓	• iLO 5 v1.10 and later for Gen10 servers. • AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux running on Gen10 servers • iSUT 2.0.0 or later • Service Pack for ProLiant
SPP compliance report	✓	✓	• AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on Gen8 or Gen9 servers • AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux running on Gen10 servers
Offline update for firmware and drivers		✓	• iLO 4 v2.50 and later for Gen8 and Gen9 servers • Service Pack for ProLiant
iLO Repository Offline Update		✓	• iLO 5 v1.10 and later for Gen10 servers. • Service Pack for ProLiant.
Server System Restore		✓	• iLO 5 v1.17 and later for Gen10 servers • AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux running on Gen10 servers • iSUT 2.0.0 or later • Service Pack for ProLiant
Alerts	Only in UI	• UI • email • IFTTT	

Table Continued

Feature	iLO Standard iLO Essentials iLO Scale-Out	iLO Advanced	Dependencies
iLO Federation group		✓	
Server group	✓	✓	

When to use iLO Amplifier Pack

You can use iLO Amplifier Pack to help you manage the following types of common scenarios efficiently and with minimal downtime.

Discovering
“Current update tools are complicated and time-consuming to use. Is there an alternative?”

iLO Amplifier Pack has a clean, intuitive GUI that is easy to use and can add servers and groups one at a time or thousands at a time. Discovery takes only a few minutes and does not require server downtime.

- **Adding a server**
- **Adding the servers in an iLO Federation Group from the Discovery page**
- **Adding servers in an IPv4 address range**
- **Adding servers from a CSV file**

Monitoring
“How do I efficiently monitor the thousands of HPE servers and groups in my infrastructure?”

iLO Amplifier Pack allows you to monitor the overall health of your infrastructure from a single page in your browser. Drill down for detailed information about individual servers or groups.

- **Viewing the dashboard**
- **Viewing the server list**
- **Viewing inventory details**
- **Viewing iLO Federation groups**
- **Viewing server groups**
- **Viewing server alerts**

Reporting
“How can I keep accurate and up-to-date reports on all my servers without it becoming my full-time job?”

Use the options from the **Reports** menu to view and download up-to-date reports.

- **Viewing the firmware report**
- **Viewing the iLO license report**
- **Viewing the basic device report**

- **Viewing the Hardware Inventory Report**
- **Viewing the Custom Report**

Managing
“I want a simple tool to manage server and group tasks without having to debug and update a script library.”

Customized scripts can be time-consuming to maintain. You can use iLO Amplifier Pack to accomplish the same tasks on a large scale with no customized upkeep required.

- **Managing server UID status**
- **Managing server power status**
- **Configuring remote syslog**
- **Mounting virtual media**
- **Managing iLO Federation groups**
- **Managing server groups**

Updating
“How can I update firmware and drivers across my data center without requiring too much downtime?”

iLO Amplifier Pack simplifies updating tasks by automating the update process requiring limited user interaction and minimal downtime.

- **About online updates**
- **Performing an Express Interactive Update**
- **Performing a Baseline Automatic Update**
- **Performing an offline firmware update**
- **iLO Repository Updates**

Server System Restore
“Is there a way to recover compromised servers or corrupted firmware?”

iLO Amplifier Pack uses recovery events from iLO 5 v1.17 or later to initiate the recovery process for servers with iLO Advanced licenses, according to user-created recovery policies.

- **Recovery Management**
- **Recovery Administration**

Performing first time setup

Perform the following tasks to set up the iLO Amplifier Pack for the first time:

Procedure

1. **Verifying prerequisites**
2. **Performing initial registration**
3. **Installing the iLO Amplifier Pack**
4. **Performing initial setup on the iLO Amplifier Pack**
5. **Activating iLO Amplifier Pack**
6. **Verifying the installation**

Verifying prerequisites

Devices supported

iLO Amplifier Pack supports the following HPE ProLiant servers:

- HPE ProLiant Gen8 (Rack, Tower, Blade, and Apollo) server
- HPE ProLiant Gen9 (Rack, Tower, Blade, and Apollo) server
- HPE ProLiant Gen10 (Rack, Tower, Blade, and Apollo) server

Operating systems

NOTE: The following Operating Systems are supported for online updates only.

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 R2 Foundation Edition
- Microsoft Windows HPC Server 2008 R2
- Microsoft Windows Server 2008 x64
- Red Hat Enterprise Linux 7 Server
- Red Hat Enterprise Linux 6 Server (x86-64)
- SUSE Linux Enterprise Server 15
- SUSE Linux Enterprise Server 12

- SUSE Linux Enterprise Server 11 (AMD64/EM64T)
- VMware ESXi Server 6.5
- VMware ESXi Server 6.0

Browser requirements

NOTE: Internet Explorer is not a recommended browser.

The following browsers are supported for running the iLO Amplifier Pack web interface:

- Chrome v69.0 or later
- Firefox v62.0 or later

The following settings must be enabled in the browser:

- **JavaScript**—Client-side JavaScript is used by this application.
- **Cookies**—Ensure to enable cookies for certain features to function correctly.
- **Pop-up windows**—Ensure to enable pop-up windows for certain features to function correctly. Verify that pop-up blockers are disabled.
- **TLS**—Ensure to enable TLS in the browser to access the web interface.

Languages

Languages supported for this release:

English

Prerequisites to host iLO Amplifier Pack

Ensure that the host machine meets the hardware requirements to run VMware ESXi Server v.5.5 or later. For more information, see the documentation on the VMware website.

The iLO Amplifier Pack guest VM requires the following resources to be available on the ESXi server:

- 4 vCPUs
- 8 GB RAM
- 100 GB of free HDD space
- 1.0 Gbps network port (2)

Prerequisites for managed servers

Servers must have the following firmware versions to be managed by iLO Amplifier Pack:

Gen8 and Gen9 servers	Gen10 servers
• iLO 4 v2.30 or later (HPE recommends upgrading to iLO 4 v2.54 or later)[1] • AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux • HPE SUT v1.8.0 or later (HPE recommends upgrading to iSUT v2.0.0 or later)	• iLO 5 v1.10 or later • AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux • iSUT v2.0.0 or later

[1] iLO 4 v2.54 or later is required to update firmware with iLO Amplifier Pack..

For more information about obtaining the required software, see the following websites:

- **iLO: www.hpe.com/servers/iLO**
- **AMS: www.hpe.com/us/en/product-catalog/detail/pip.5219980.html**
- **SUT/iSUT: http://www.hpe.com/servers/sut**

Prerequisites for performing updates

- For Gen8 and Gen9 servers - SPP (Service Pack for ProLiant) Version 2018.11.0 or later downloaded from **www.hpe.com/servers/SPP**.
- For ESXi servers - SPP (Service Pack for ProLiant) Version 2018.11.0 or later downloaded from **www.hpe.com/servers/SPP**.
- If you are planning to use a web server for firmware updates, ensure that the web server includes the following:
  - An HTTP/HTTPS share that hosts SPP iso images and files.
  - The following file extensions added to the MIME Types setting to ensure correct downloading:
    - .bin
    - .iso
    - .xml
    - .pdb

IMPORTANT: Before commencing online updates, ensure that AMS is running and SUT Mode is set to **AutoDeployReboot** or **AutoDeploy**.

Prerequisites for performing recovery

Recovery can be performed only on Gen10 servers with:

- iLO 5 v1.17 or later (iLO Advanced license)
- SPP consisting of iLO 5 v1.17 core server platform firmware.
- iLO Amplifier user with privilege "Config Manager with Security"

NOTE: The default user in iLO Amplifier Pack does not have the "Configure Manager with Security" privilege.

Performing initial registration

Prerequisites

Valid email address to receive activation key.

Procedure

1. Go to the iLO Amplifier Pack registration webpage at **http://www.hpe.com/downloads/iloamplifierpack**.
2. Enter your first and last name and your email address.
3. Click **Yes** or **No** to receiving future email offers and event news from HPE.
4. Select the number of server licenses you want to register.
5. Enter your company name, city or town, state or province, country/region, and your business phone number.
6. Click **Yes** or **No** to receiving future phone calls with offers and event news from HPE.
7. Read the HPE Software Terms of Use and then select the check box.
8. Click **Register**.

   A message stating that your license registration is successful appears on the registration page, and HPE sends an email containing the following information:

   - A link to download the appliance installation image (**`iLOAmplifierPack.ova`**)
   - An Activation Key

Installing iLO Amplifier Pack

Prerequisites

- Registration email from HPE containing the download link and activation key
- A host server configured with VMware ESXi v5.5 or later
- A laptop or desktop system that has VMware vSphere Client installed or a supported web browser

Procedure

1. Click the download link in the license registration email.
2. Download and save the **`iLOAmplifierPack_1.30.zip`** and corresponding checksum file.

   NOTE: Use an appropriate checksum verification tool to verify the integrity of the downloaded files.

3. Extract the **`iLOAmplifierPack.ova`** from the zip file.
4. Use the VMware vSphere Client or a supported web browser to connect to any VMware ESXi server (v5.5 and later).

5. Do one of the following:

   - If using the VMware vSphere Client, click **File**, click **Deploy OVF Template**, and then follow the onscreen instructions.
   - If using a web browser, click **Create/Register VM**, click **Deploy a virtual machine from an OVF or OVA file**, and then follow the onscreen instructions.

   NOTE: HPE recommends that you select Thick disk provisioning when configuring deployment options for your VM.

6. Once the image is imported, power on the VM.

   The VM might take some time to boot up. If DHCP is not supported, then it might take up to 5 minutes to boot up.

   After the VM has restarted, the first-time setup screen displays on the console.

Performing initial setup on the iLO Amplifier Pack

Prerequisites

- A VM deployed with the iLO Amplifier Pack OVF.
- The VM reboot has been completed.
- The Welcome screen is displayed on the console.

Procedure

1. On the Welcome screen, click **Initial Setup**.
2. Read the End User License Agreement (EULA), and then click **Accept**.
3. Enter the following network settings, and then click **Next**. Use the arrow keys to navigate between settings and use Enter to modify the selected setting.

   a. Enable NIC 1 or NIC 2 or both as required.

   b. Optional. Enable or disable DHCPv4 or DHCPv6. If DHCP is disabled, enter the following:

      I. Enter the static IPv4 or IPv6 address.

      II. Enter the Subnet Mask for an IPv4 configuration or Prefix Length for an IPv6 configuration.

      III. Enter the Default Gateway.

   c. Select the Management Network Port. NIC 1 is selected by default.

   d. Optional. Enter the Primary IPv4 or IPv6 DNS Server.

   e. Optional. Enter the Secondary IPv4 or IPv6 DNS Server.

4. Change the time zone and NTP settings or accept the defaults, and then click **Next**.
5. Set up the Administrator account by entering a Display Name and password, and then click **Finish**.

The user name and password you enter here are the credentials you use to set up an initial Administrator account. Once the initial setup is complete, you can use iLO Amplifier Pack management settings to add additional users.

6. When prompted, click **Reboot**.

   The system restarts and then a welcome screen appears displaying the IP address of the iLO Amplifier Pack management appliance.

Activating iLO Amplifier Pack

Prerequisites

- iLO Amplifier Pack user with either of the following privileges:
  - Configure Manager
  - Configure Manager with Security
- An installation of iLO Amplifier Pack on a VM that has been rebooted.

Procedure

1. Browse to the IP address shown on the welcome screen on the VM console.
2. Log on to the iLO Amplifier Pack management appliance using the credentials you entered when you set up the initial user account.
3. When prompted, copy the Activation Key from your registration email and paste it into the **License Key** field.
4. Click **Activate**.

   The iLO Amplifier Pack management dashboard appears.

Verifying the installation

Prerequisites

- User privileges
  - Configure Manager
  - Configure Manager with Security
- An activated installation of the iLO Amplifier Pack

Procedure

1. On the dashboard page, click the information icon in the upper right corner of the page. The **About** screen appears.
2. Verify your information, and then click **OK**.

Viewing the dashboard

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login

Procedure

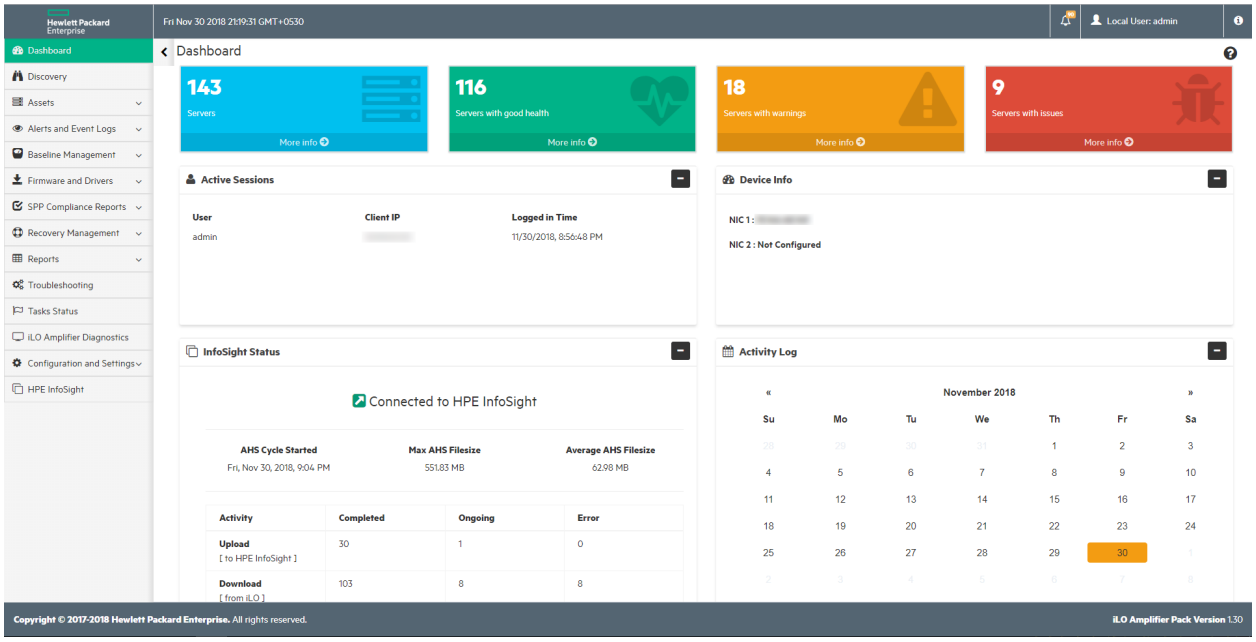
1. Click **Dashboard** from the left navigation menu.

   The Dashboard page displays the server health summary, active sessions, activity calendar, device information, and HPE InfoSight status.

2. Do any of the following to view additional information:

   - Click a tile in the server health summary to view the list of servers with a specific health status.
   - Click a date in the **Activity Log** calendar to view the Activity Log details for that date.
   - Click a minus sign icon to expand or collapse a section of the Dashboard page.

Dashboard details



- **Server health**—The following information is displayed at the top of the dashboard. Click **More info** to see the server list filtered for each alert category.

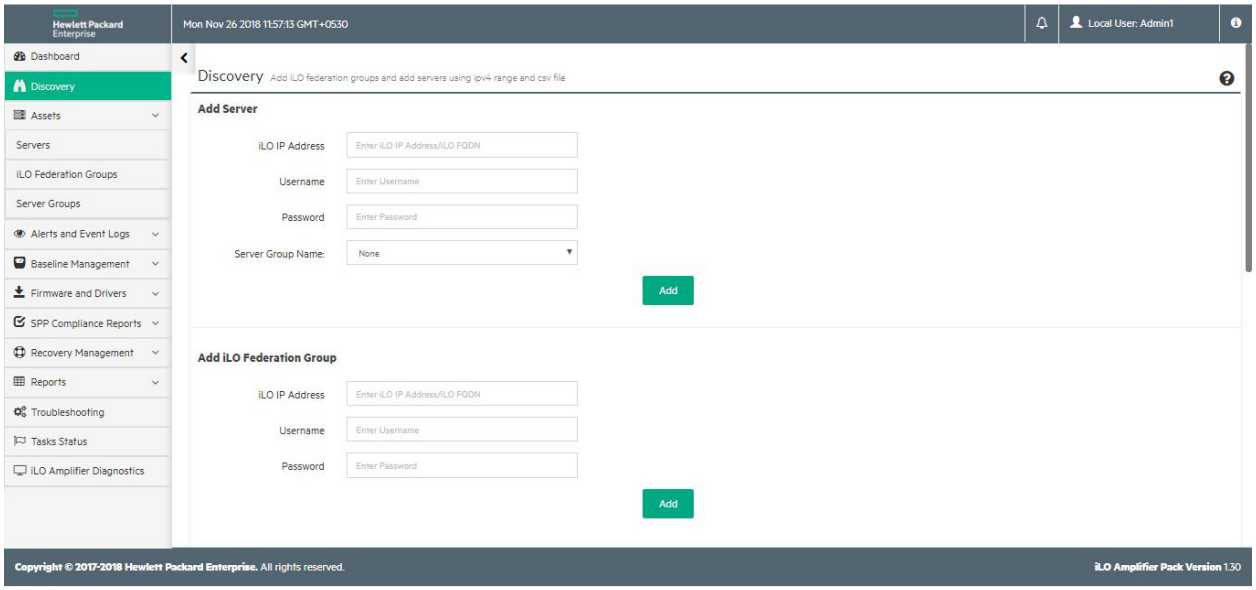
- Total number of servers
- Number of servers with good health
- Number of servers with warnings
- Number of servers with issues

- **Active Sessions**—The following information is displayed for each user logged into iLO Amplifier Pack.
  - **User**—The display name assigned to the user account.
  - **Client IP**—The IP address of the client computer used to log into iLO Amplifier Pack.
  - **Logged in Time**—The date and time of the most recent login.
- **Activity Log**—Activity logs are recorded daily. Click the highlighted dates on the calendar to view the recorded activity for that date.
- **InfoSight status**—The connection status to HPE InfoSight. Other information about the AHS logs like the maximum and average file size is also shown here. The AHS cycle time stamp refreshes each time the AHS collection is initiated for the day. Maximum AHS file size is the maximum file size of the AHS logs that are downloaded across all the servers that are added in iLO Amplifier Pack for that day. The average AHS file size is the average file size of the AHS logs that are downloaded across all the servers that are added in iLO Amplifier Pack for that day. Information about the download status of the AHS logs from the iLO and the upload status of all logs to HPE InfoSight is also displayed here.
- **Device Info**—The IP addresses of the appliance network adapters (if configured).
- **Notification bell**—Provides the count of the alerts received from the managed systems. Also lists the event names of the last five alerts.

Discovery

The Discovery page allows you to add assets to manage with iLO Amplifier Pack. Use the Discovery page to discover individual servers, servers in iLO Federation groups, servers within an IPv4 address range, and servers listed in a CSV file.

Adding a single server from the Discovery page



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE ProLiant Gen8 or Gen9 server with iLO 4 version 2.30 or later
- HPE ProLiant Gen10 server with iLO 5 version 1.10 or later

Procedure

1. Click **Discovery** from the left navigation menu.
2. Enter the following information in the **Add Server** section:
   - **iLO IP Address**—The IPv4 or IPv6 address of a supported server or the FQDN (fully qualified domain name) of the iLO.
   - **Username**—The user name for an iLO account on the server.

- **Password**—The password for the specified iLO user account.
- **Server group name (Optional)**—Select the server group you want the server to be a part of.

3. Click **Add.**

   iLO Amplifier pack starts the discovery and inventory processes for the server.

4. Optional: Click **Assets** in the navigation tree, and then click **Servers** to view the status of the added server.

Adding an iLO Federation Group from the Discovery page

Prerequisites

NOTE: For more information about iLO Federation requirements, see the *iLO Federation User Guide* at **http://www.hpe.com/support/ilo4_federation_ug_en**.

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- An existing iLO Federation group made up of HPE ProLiant Gen8, Gen9, or Gen10 servers with a dedicated iLO NIC. Servers with shared a NIC port do not support iLO Federation.
- iLO Federation enabled on all servers with the following multicast options in the iLO Federation settings.

  NOTE: The menu option is different for Gen8/Gen9 and Gen10.

  - iLO Federation management and multicast discovery enabled on all servers
  - **Multicast Announcement Interval** set to **30 seconds**
  - **IPv6 Multicast Scope** set to **Site**
  - **Multicast TTL** set to **255**

Procedure

1. Click **Discovery** from the left navigation menu.
2. Enter the following information in the **Add iLO Federation Group** section:
   - **iLO IP Address**—The IPv4 address of a server in an iLO Federation group.
   - **Username**—The user name of an iLO account on the specified server.
   - **Password**—The password for the specified iLO user account.
3. Click **Add**.

If the specified iLO system is a member of more than one iLO Federation group, iLO Amplifier Pack prompts you to select the groups to discover.

4. Select a group, and then click **OK**.
5. Optional: Click **Assets** in the navigation tree, and then click **iLO Federation Groups** to view the status of the added groups.

   To view the status of the individual servers in the added groups, click **Assets** in the navigation tree, click **Servers**, click **iLO Federation Groups** from the **Filters** menu, and then click the group name.

Adding servers in an IPv4 address range

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE ProLiant Gen8 or Gen9 server with iLO 4 version 2.30 or later
- HPE ProLiant Gen10 server with iLO 5 version 1.10 or later

Procedure

1. Click **Discovery** on the left navigation menu.
2. Enter the following information in the **Add IPv4 Range** section:
   - **iLO IP Range**—The starting and ending IP addresses in the range.
   - **SSL Port**—The SSL Port used to communicate with the iLO.
   - **Username**—The user name for an iLO account on the server.
   - **Password**—The password for an iLO account on the server.

     NOTE: Use credentials that are common across all servers in the IPv4 range.

   - **Server group name (Optional)**—Select the server group you want the server to be a part of.
3. Click **Add**.

   Servers in the IPv4 range with the specified user account are discovered and inventoried.

   Servers in the IPv4 range that do not have the specified user account are added as unmanaged servers. To Add user account credentials for unmanaged servers, see **Updating an unmanaged server**.
4. Optional: Click **Assets** in the navigation tree, and then click **Servers** to view the status of the added servers.

Adding servers from a CSV file

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE ProLiant Gen8 or Gen9 server with iLO 4 version 2.30 or later
- HPE ProLiant Gen10 server with iLO 5 version 1.10 or later
- The location of a CSV file that contains the following:
  - a list of servers in the following format:

    `<iLO IPv4 or IPv6 addresses or FQDN>, <iLO username>, <iLO password>`
  - no headers
  - no blanks in the iLO IP address or FQDN and username fields
  - iLO FQDN address that does not exceed 49 characters

  Click **SampleFile.csv** on the **Discovery** page to see a sample of a CSV file with correct formatting.

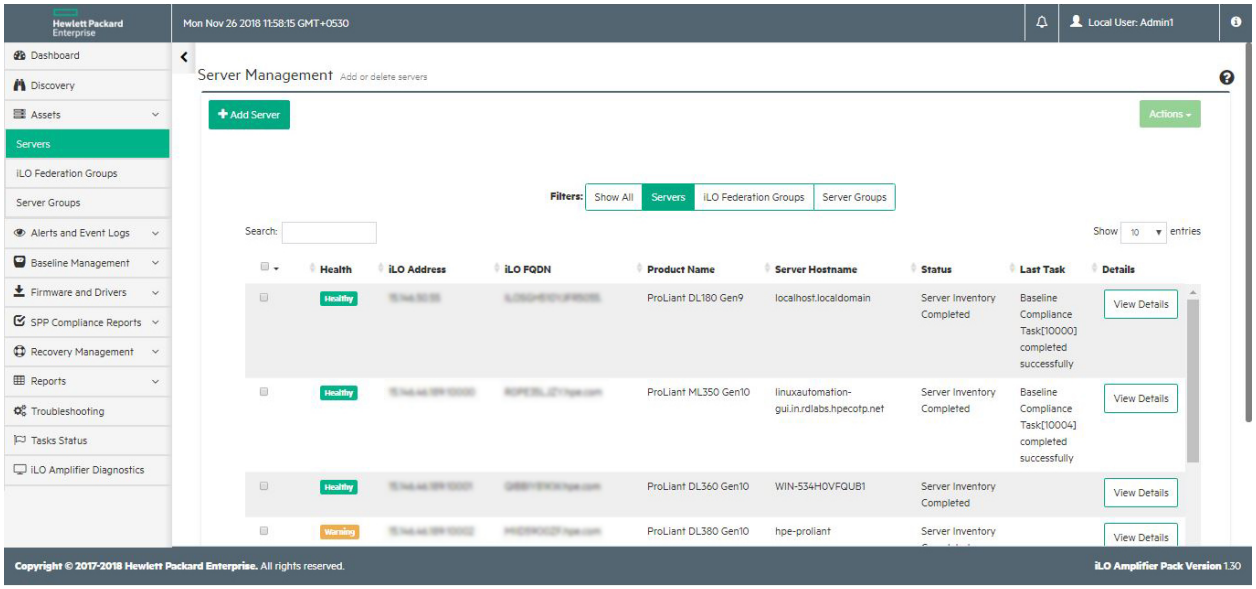
Procedure

1. Click **Discovery** in the left navigation menu.
2. In the **Add from a file** section, click **Choose File**, and then select the CSV file to use.
3. Optional: Select the server group you want the servers to be a part of.
4. Click **Upload**.

   iLO Amplifier Pack processes the file and starts the discovery and inventory processes.
5. Optional: Click **Assets** in the navigation tree, and then click **Servers** to view the status of the added servers.

Managing servers

Viewing the server list



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login

Procedure

1. Click **Assets** on the navigation menu, and then click **Servers**. The **Server Management** page appears displaying the following information:

   - **Health**—The server health indicator. This value summarizes the condition of the monitored subsystems, including overall status and redundancy (ability to handle a failure). Click to view the **Health Summary** tab in the server list details pane.
   - **iLO Address**—The network IPv4 or IPv6 address (and port, when applicable) of the iLO subsystem or the FQDN (fully qualified domain name) of the iLO.
   - **iLO FQDN**—The FQDN (fully qualified domain name) of the iLO.
   - **Product Name**—The server model.
   - **Server Hostname**—The hostname assigned to the server.

- **Status**—The inventory status of the server in iLO Amplifier Pack.

  NOTE: Servers that are managed by HPE OneView are identified in the **Status** field. HPE OneView servers appear on the server list for inventory purposes, but cannot be updated by iLO Amplifier Pack.

- **Last Task**—The last completed iLO Amplifier Pack task and task status.
- **Details**—Click **View Details** to see more information about an individual node.

2. Optional: Use the **Filters**, **Search**, and **Show entries** controls to customize how the server list is displayed.
3. Optional: Use the following actions to manage servers from this page:

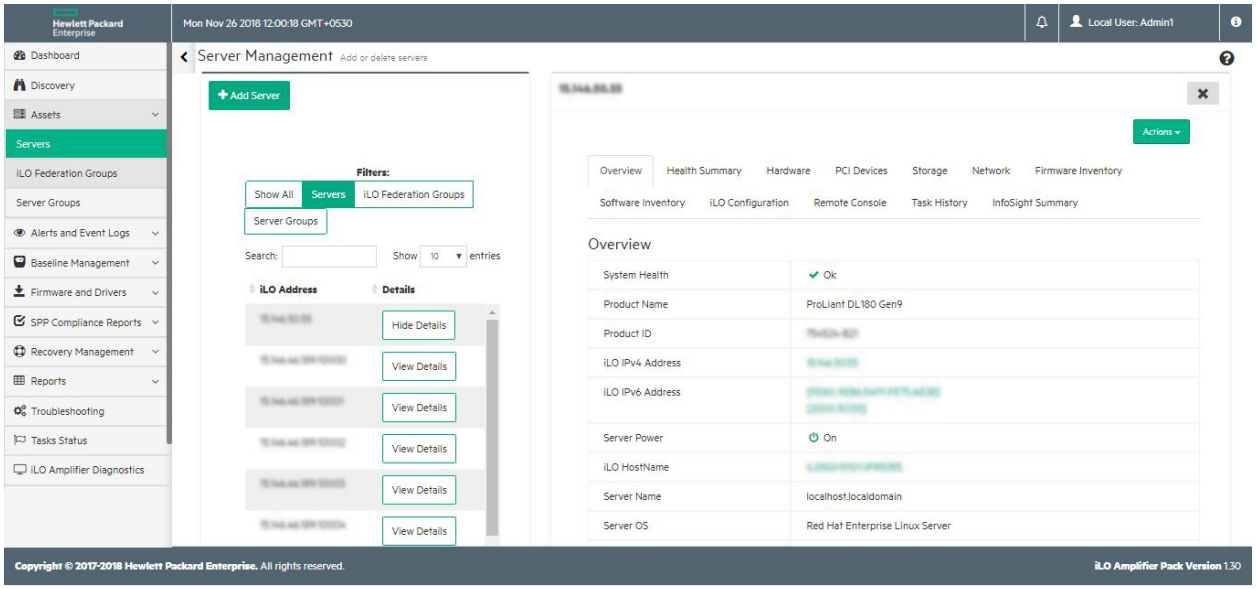
   NOTE: Users with **Login** privileges cannot manage servers.

   - **Add Server**—Click to add a server to the list. For more information, see **Adding a server**.
   - **Actions**—Click a check box to select a server from the server list, and then select an action from the menu:
     - **UID Control**—see **Managing server UID status**.
     - **Power Options**—see **Managing server power status**.
     - **Firmware Update**—see **Server firmware and driver updates**.
     - **Remote Syslog**—see **Configuring remote syslog**.
     - **Virtual Media**—see **Mounting virtual media**.
     - **Delete**—see **Deleting a server**.
     - **Refresh**—see **Refreshing the server list** .

Viewing server details

Clicking **View Details** iLO Amplifier Pack uses the information provided by iLO and displays it here for more convenient access during update planning.

NOTE: Servers that are managed by HPE OneView are identified with a banner at the top of the **View Server details** pane. Servers managed by HPE OneView appear for inventory purposes, but cannot be updated by iLO Amplifier Pack.



- **Overview** tab—displays high-level details about the server and the iLO subsystems.
- **Health Summary** tab—displays the health status of server components and the Agentless Management Service. Click each of the health status icons to view further details about the component.
- **Hardware** tab—displays details of the server hardware for the CPU, memory, fan, and power supply.
- **PCI Devices** tab—displays details about the PCI devices for the server, including type, location, and firmware version.
- **Storage** tab—displays storage inventory information such as drive serial numbers, capacity, location, and health status.
- **Network** tab—displays the network adapter name and firmware version, port, MAC, IPv4, and IPv6 addresses, health status, and state.
- **Firmware Inventory** tab—displays firmware names and version numbers.
- **Software Inventory** tab—displays names, version numbers, descriptions of the software installed on the server.
- **iLO Configuration** tab—displays iLO license and remote syslog details.
- **Remote Console** tab—describes the iLO .Net and Java IRC and provides links for using them.
- **Task History** tab—displays the name, progress percentage, status, and time completed for server tasks.
- **InfoSight summary** tab—displays the upload status and details of logs sent to HPE and the download status and details of logs received from iLO.

Adding a single server from the Servers page

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

- HPE ProLiant Gen8 or Gen9 server with iLO 4 version 2.30 or later
- HPE ProLiant Gen10 server with iLO 5 version 1.10 or later

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Click **Add Server**.
3. Select the **Add Server** option.
4. Enter the iLO IPv4 or IPv6 address.
5. Enter the username for an iLO user account on the node.
6. Enter the user account password.
7. Optionally select the server group you want the server to be a part of.
8. Click **Add**.

Adding servers in an IPv4 address range from the Servers page

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE ProLiant Gen8 or Gen9 server with iLO 4 version 2.30 or later
- HPE ProLiant Gen10 server with iLO 5 version 1.10 or later

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Click **Add Server**.
3. Select the **Add IPv4 Range** option.
4. Enter the starting and ending IP addresses in the iLO IP range.
5. Enter the SSL port used to communicate with the iLO.
6. Enter the username and password for an iLO user account on the node.

NOTE: Use credentials that are common across all the servers in the IPv4 range.

7. Optionally select the server group you want the server to be a part of.
8. Click **Add**.

   Servers in the IPv4 range with the specified user account are discovered and inventoried.

   Servers in the IPv4 range that do not have the specified user account are added as unmanaged servers. To Add user account credentials for unmanaged servers, see **Updating an unmanaged server**.

Updating an unmanaged server

During IPv4 range discovery, if a server is added to iLO Amplifier Pack without valid credentials, it is added as an unmanaged server. To change an unmanaged server to a managed server, provide valid credentials.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Locate a server with a status of **Unknown**.
3. Click **Manage**.
4. Enter the iLO username and password.
5. Click **Apply**.

Managing server UID status

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to manage.

3. Click **Actions**, and then select **UID Control**.
4. Select the UID setting in the **Set UID** menu.
   - **Off**—UID button is disabled
   - **Lit**—UID button is enabled
5. Click **Apply** to apply the setting or click **Close** to return to the **Servers** page.

Managing server power status

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to manage.
3. Click **Actions**, and then select **Power Control**.
4. Select the power setting in the **Set Power** menu.
   - **On**—Turn on the system (default).
   - **Force Off**—Perform an immediate (non-graceful) shutdown.
   - **Force Restart**—Perform an immediate (non-graceful) shutdown, followed by a restart of the system.
   - **Push Power Button**—Simulate the pressing of the physical power button on this system.
5. Click **Apply** to apply the setting or click **Close** to return to the **Servers** page.

Server power options

When you manage the power status of servers, the following power options are available:

- **On**—Turn the system on (default).

  The same as pressing the physical power button.
- **Force Off**—Perform an immediate (non-graceful) shutdown.

  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.
- **Force Restart**—Perform an immediate (non-graceful) shutdown, followed by a restart of the system.

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.

- **Push Power Button**—Simulate the pressing of the physical power button on this system.

  If the server is powered off, a momentary press will turn on the server power.

Updating server firmware from the Servers page

Use the **Firmware Update** option from the **Servers** page when you want to update the following firmware types:

- iLO firmware
- HPE System ROM
- System Programmable Logic Device
- SL/XL Chassis firmware
- Language Packs

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- A core platform firmware binary image.

  The binary image can be extracted from a core platform component in SPP, or obtained from HPE support portal.

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to update.
3. Click **Actions**, and then select **Firmware Update**.
4. Enter the URL of the firmware binary image in the **HTTP/HTTPS URL** field.
5. If TPM is present in any of the selected servers, the **TPM Override** option appears. Select the check box if you want TPM-enabled servers to be updated.
6. Click **Apply** to begin the update or click **Close** to return to the **Servers** page.

Configuring remote syslog

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager
- Configure User
- Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to configure.
3. Click **Actions**, and then select **Remote SysLog**.
4. Select one of the following:
   - **Use iLO Amplifier Pack SysLog Settings**—Select to use the SysLog configuration set for iLO Amplifier Pack. For more information, see **Configuring Remote SysLog Settings for iLO Amplifier Pack**.
   - **Use Manual Settings**—Select if you want to use the manual settings for SysLog:
     - **SysLog Enabled**—Select to enable remote SysLog.
     - **SysLog Port**—Enter the port to use for remote SysLog reporting.
     - **SysLog Server**—Enter the IPv4 or IPv6 Address or FQDN of the server hosting the remote SysLog.
5. Click **Apply** to apply the setting or click **Close** to return to the **Servers** page.

Mounting and ejecting virtual media

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to manage.
3. Click **Actions**, and then select **Virtual Media**.
4. Enter the url for the location of the ISO file in the **ISO URL** text box.
5. Click **Mount** to mount the virtual media.

NOTE: You can also eject the virtual media by clicking **Eject**.

Deleting a server

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check box for the server you want to delete.
3. Click **Actions**, and then select **Delete**.
4. Click **Apply** to delete the server or click **Close** to return to the **Servers** page.

Refreshing the server list

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Servers**.
2. Select the check boxes for the servers you want to refresh.
3. Click **Actions**, and then select **Refresh**.
4. On the **Refresh servers** screen, click **Apply**.

Managing iLO Federation groups

Use the **iLO Federation Groups** page to create new iLO Federation groups and to select servers to add to existing groups.

For more information about iLO Federation network requirements and multicast options, see the relevant sections of the *iLO Federation User Guide* available at **http://www.hpe.com/support/ilo4_federation_ug_en**.

NOTE: When creating or joining iLO federation groups, iLO Amplifier Pack does not support the new BIOS, Storage, and Network configuration group privileges that are available for HPE ProLiant Gen10 servers.

iLO Amplifier pack does not support managing iLO Federation Groups using IPv6. This feature will be added in a future release. For more details, see the *iLO Amplifier Pack v1.30 Release Notes*.

Viewing iLO Federation groups

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.
3. Optional: Use the **Show entries** menu to choose the number of groups to display.
4. Optional: Type a value in the **Search** box and hit the enter key to search for a specific group.
5. The following information is displayed for each iLO Federation group.

   - Status
   - Group Name
   - #Servers
   - Last Task
   - Gateway iLO
   - Details
   - Actions
     - Refresh group
     - Delete group

Creating an iLO Federation group

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure Users
- Configure Devices

- Managed servers with iLO Dedicated Port and iLO Advanced license.

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Click **+ Create Group** and a dialog box appears displaying the status of the servers.
3. Select the servers that you want to include in a new iLO Federation Group and then click **Preview**.
4. In the **Common iLO Credentials** section, enter a username and password.
5. In the **Group Details** section, add a group name and key.
6. In the **Group Privileges** section, select from the following options:
   - **Administer User Accounts**—Group members can add, edit, and delete iLO user accounts.
   - **Remote Console Access**—Group members can remotely access the managed server Remote Console, including video, keyboard, and mouse control.
   - **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 scripted Virtual Media with the managed server.
   - **Configure iLO Settings**—Group members can configure most iLO settings, including security settings, and can remotely update firmware.
   - **Login Privilege**—Group members can log in to iLO. Selected by default.
7. Click **Create Group**.

Adding an iLO Federation Group from the Groups page

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** in the left navigation menu, and then click **iLO Federation Groups**.
2. Click **+ Add iLO Federation Group**.
3. Enter the IPv4 address of a member of an iLO Federation group, and then click **Add** to discover the servers that are part of the group.

4. Enter the user name and password of the iLO account.
5. Click **Add**.

Joining an iLO Federation group

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices
- iLO managed servers with federation grouping enabled

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Click **+ Join Group** and a dialog box appears displaying the status of the servers.

   Select the servers that you want to add to an existing iLO Federation group, and then click **Join Group**.
3. In the **Common iLO Credentials** section, enter the username and password for the group you want to join.
4. In the **Group Details** section, select a group from the **Group Name** menu and enter the group key.
5. In the **Group Privileges** section, select from the following options:
   - **Administer User Accounts**—Group members can add, edit, and delete iLO user accounts.
   - **Remote Console Access**—Group members can remotely access the managed server Remote Console, including video, keyboard, and mouse control.
   - **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 scripted Virtual Media with the managed server.
   - **Configure iLO Settings**—Group members can configure most iLO settings, including security settings, and can remotely update firmware.
   - **Login Privilege**—Group members can log in to iLO. Selected by default.

     NOTE: In iLO 5 for Gen10 servers, the new privileges (Host BIOS, Host NIC, Host Storage, and Recovery Set) are not applicable for joining groups from iLO Amplifier Pack.
6. Click **Join Group**.

Deleting an iLO Federation group

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Select the check boxes for the iLO Federation groups you want to delete.
3. Click **Actions**, and then select **Delete**.
4. In the the **Group Delete Confirmation** dialog box, click **Yes** to delete the group, or click **No** to return to the **iLO Federation Groups** page.

Managing UID status for grouped servers

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.

   Use the **Show entries** menu to choose the number of groups to display.

   Type a value in the **Search** box and hit the enter key to search for a specific group.
3. On the **List of iLO Federation Groups** page, select the check boxes for the groups you want to manage.
4. Click **Actions**, and then select **UID Control**.
5. Select the UID setting in the **Set UID** menu.

   NOTE: The setting you select here will be applied to all servers in the group.

- **Off**—UID button is disabled
- **Lit**—UID button is lit

6. Click **Apply** to apply the setting or click **Close** to return to the **List of iLO Federation Groups** page.

Managing power status for grouped servers

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.

   Use the **Show entries** menu to choose the number of groups to display.

   Type a value in the **Search** box and hit the enter key to search for a specific group.
3. On the **List of iLO Federation Groups** page, select the check boxes for the groups you want to manage.
4. Click **Actions**, and then select **Power Options**.
5. Select the power setting in the **Set Power** menu.

   NOTE: The setting you select here will be applied to all servers in the group.

   - **On**—Turn on the system (default).
   - **Force Off**—Perform an immediate (non-graceful) shutdown.
   - **Force Restart**—Perform an immediate (non-graceful) shutdown, followed by a restart of the system.
   - **Push Power Button**—Simulate the pressing of the physical power button on this system.
6. Click **Apply** to apply the setting or click **Close** to return to the **List of iLO Federation Groups** page.

Updating firmware for grouped servers

Use the **Firmware Update** option from the iLO Federation groups page when you want to update the following firmware types:

- iLO firmware
- HPE System ROM
- System Programmable Logic Device
- SL/XL Chassis firmware
- Language Packs

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- A core platform firmware binary image.

  The binary image can be extracted from a core platform component in SPP, or obtained from HPE support portal.

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Select the check boxes for the groups you want to update.
3. Click **Actions**, and then select **Firmware Update**.
4. Enter the URL of the firmware binary image in the **HTTP/HTTPS URL** field.
5. Click **Apply** to begin the update or click **Close** to return to the **iLO Federation Groups** page.

Configuring remote SysLog for grouped servers

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Select the check box for the group you want to configure.
3. Click **Actions**, and then select **Remote SysLog**.

4. Select one of the following:
   - **Use iLO Amplifier Pack SysLog Settings**—Select to use the SysLog configuration set on the iLO Amplifier Pack. For more information, see **Configuring Remote SysLog Settings for iLO Amplifier Pack**.
   - **Use Manual Settings**—Select if you want to use the manual settings for SysLog:
     - **SysLog Enabled**—Select to enable remote SysLog.
     - **SysLog Port**—Enter the port to use for remote SysLog reporting.
     - **SysLog Server**—Enter the IPv4 or IPv6 Address or FQDN of the server hosting the remote SysLog.
5. Click **Configure** to apply the setting or click **Close** to return to the **iLO Federation Groups** page.

Mounting and ejecting virtual media for grouped servers

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Select the check box for the group you want to manage.
3. Click **Actions**, and then select **Mount Virtual Media**.
4. Enter the url for the location of the ISO file in the **ISO URL** text box.
5. Click **Mount** to mount the virtual media.

   NOTE: You can also eject the virtual media by clicking **Eject**.

Refreshing the list of iLO Federation Groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

Procedure

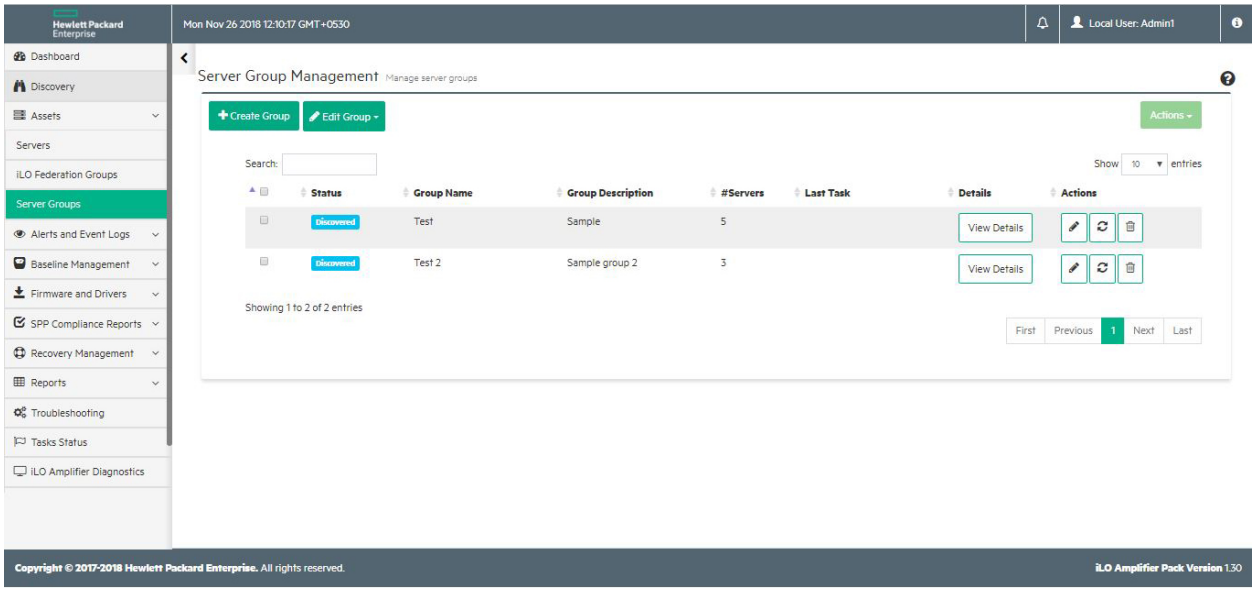
1. Click **Assets** from the left navigation menu, and then click **iLO Federation Groups**.
2. Select the check box for the group you want to refresh.
3. Click **Actions**, and then select **Refresh**.

   The Group Refresh task starts. To see details about the task, click the **task status** link in the message banner at the top of the page.

   When the refresh task finishes, a **Groups Refreshed Successfully** message appears.

Managing server groups

Viewing server groups

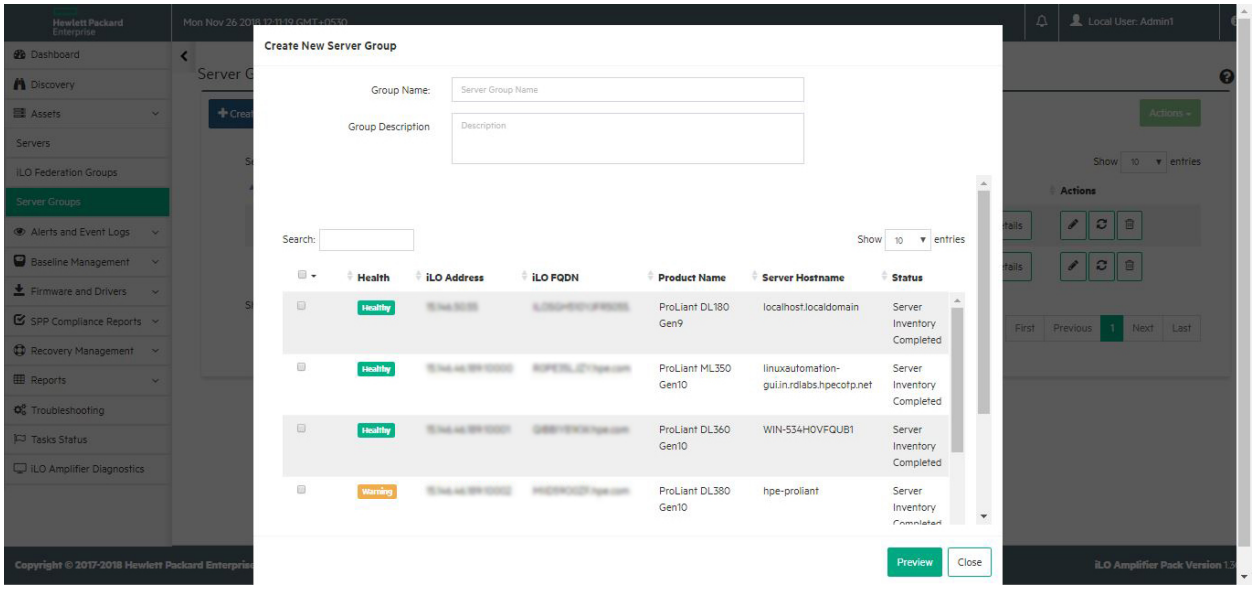


Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.
3. Optional: Use the **Show entries** menu to choose the number of groups to display.
4. Optional: Type a value in the **Search** box and hit the enter key to search for a specific group.
5. The following information is displayed for each server group.

    - Status
    - Group Name
    - Group description
    - #Servers
    - Last Task
    - Details
    - Actions
        - Edit group description
        - Refresh group
        - Delete group

Creating a server group



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Click **+ Create Group** and a dialog box appears displaying the status of the servers.
3. Enter a **Group Name** and the **Group Description**.
4. Select the servers that you want to include in the new server group and then click **Preview**.
5. Review the list of servers added and click **Create Group** to create a server group, or click **Back** to return to the list of servers.

   You can also click **Close** to cancel the operation and return to the **Server Groups** page.

   NOTE: iLO Amplifier Pack supports a maximum of 500 server groups. The group creation task will fail if the user attempts to create more than 500 server groups.

Joining a server group

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager
- Configure User
- Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Click **Edit Group** and then **Join Group**. A dialog box appears displaying the status of the servers.
3. Select the server group to add the servers to.
4. Select the servers that you want to include in the server group and then click **Preview**.
5. Review the list of servers added and click **Join Group** to add the servers to the specified server group, or click **Back** to return to the list of servers.

   You can also click **Close** to cancel the operation and return to the **Server Groups** page.

Unjoining servers from a server group

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Click **Edit Group** and then **Unjoin Group**. A dialog box appears displaying the status of the servers.
3. Select the server group to unjoin the servers from.
4. Select the servers that you want to unjoin from the server group and then click **Preview**.
5. Review the list of servers and click **Unjoin Group** to remove the servers from the specified server group, or click **Back** to return to the list of servers.

   You can also click **Close** to cancel the operation and return to the **Server Groups** page.

   NOTE: This operation only removes the server from the server group and does not delete the server from iLO Amplifier Pack.

Deleting a server group

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager
- Configure User
- Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Select the check box for the group you want to delete.
3. Do one of the following:

   - To remove the servers from the server group and also delete them from iLO Amplifier Pack:

     a. Click **Actions**, and then select **Delete**.

     b. Optional: Click  to delete the group.

     c. In the **Delete Group Confirmation** dialog box, select **Delete servers part of the group from iLO Amplifier Pack**.

     d. Click **Yes** to delete the group, or click **No** to return to the **Server Groups** page.

     NOTE: This action will delete all the servers from iLO Amplifier Pack.

   - To remove the servers from the group but not from iLO Amplifier Pack:

     a. Click **Actions**, and then select **Delete**.

     b. Optional: Click  to delete the group.

     c. In the **Delete Group Confirmation** dialog box, click **Yes** to remove the group, or click **No** to return to the **Server Groups** page.

Managing UID status for server groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.

   Use the **Show entries** menu to choose the number of groups to display.

   Type a value in the **Search** box and hit the enter key to search for a specific group.
3. On the **Server Group Management** page, select the check boxes for the groups you want to manage.
4. Click **Actions**, and then select **UID Control**.
5. Select the UID setting in the **Set UID** menu.

   NOTE: The setting you select here will be applied to all servers in the group.

   - **Off**—UID button is disabled
   - **Lit**—UID button is lit
6. Click **Apply** to apply the setting or click **Close** to return to the **Server Group Management** page.

Managing power status for server groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Optional: Use the navigation buttons to view the first, previous, next, or last page of the groups list. You can also click a specific page number to jump to that page.

   Use the **Show entries** menu to choose the number of groups to display.

   Type a value in the **Search** box and hit the enter key to search for a specific group.
3. On the **Server Group Management** page, select the check boxes for the groups you want to manage.
4. Click **Actions**, and then select **Power Options**.
5. Select the power setting in the **Set Power** menu.

NOTE: The setting you select here will be applied to all servers in the group.

- **On**—Turn on the system (default).
- **Force Off**—Perform an immediate (non-graceful) shutdown.
- **Force Restart**—Perform an immediate (non-graceful) shutdown, followed by a restart of the system.
- **Push Power Button**—Simulate the pressing of the physical power button on this system.

6. Click **Apply** to apply the setting or click **Close** to return to the **Server Group Management** page.

Updating firmware for server groups

Use the **Firmware Update** option from the server groups page when you want to update the following firmware types:

- iLO firmware
- HPE System ROM
- System Programmable Logic Device
- SL/XL Chassis firmware
- Language Packs

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- A core platform firmware binary image.

  The binary image can be extracted from a core platform component in SPP, or obtained from HPE support portal.

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Select the check boxes for the groups you want to update.
3. Click **Actions**, and then select **Firmware Update**.
4. Enter the URL of the firmware binary image in the **HTTP/HTTPS URL** field.
5. Select the **TPM Override** check box to update TPM-enabled servers.
6. Click **Apply** to begin the update or click **Close** to return to the **Server Group Management** page.

Configuring remote SysLog for server groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Select the check box for the group you want to configure.
3. Click **Actions**, and then select **Remote SysLog**.
4. Select one of the following:
   - **Use iLO Amplifier Pack SysLog Settings**—Select to use the SysLog configuration set on the iLO Amplifier Pack. For more information, see **Configuring Remote SysLog Settings for iLO Amplifier Pack**.
   - **Use Manual Settings**—Select if you want to use the manual settings for SysLog:
     - **SysLog Enabled**—Select to enable remote SysLog.
     - **SysLog Port**—Enter the port to use for remote SysLog reporting.
     - **SysLog Server**—Enter the IPv4 or IPv6 Address, or FQDN of the server hosting the remote SysLog.
5. Click **Configure** to apply the setting or click **Close** to return to the **Server Group Management** page.

Mounting and ejecting virtual media for server groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Select the check box for the group you want to manage.

3. Click **Actions**, and then select **Mount Virtual Media**.
4. Enter the url for the location of the ISO file in the **ISO URL** text box.
5. Click **Mount** to mount the virtual media.

NOTE: You can also eject the virtual media by clicking **Eject**.

Refreshing servers in server groups

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Assets** from the left navigation menu, and then click **Server Groups**.
2. Select the check box for the group you want to refresh.
3. Click **Actions**, and then select **Refresh**.

   The Group Refresh task starts. To see details about the task, click the **task status** link in the message banner at the top of the page.

   When the refresh task finishes, a **Groups Refreshed Successfully** message appears.

Alerts and Event Logs

The pages in this section allow you to view and use event and alert information for managed servers and for the iLO Amplifier Pack appliance.

For information about configuring alerts, see **Configuring alert settings**.

Managed Servers Alerts

As part of the inventory process, iLO Amplifier Pack subscribes to iLO for server alerts. When certain conditions occur, iLO Amplifier Pack sends out email or IFTTT alerts when an event is received from iLO.

Viewing alerts from managed servers

Use the **Managed Servers Alerts** page to see detailed information about alerts that have been received from managed servers.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login

Procedure

1. On the left navigation menu, click **Alerts and Event Logs**.
2. Click **Managed Servers Alerts**.

   The event list appears displaying the following information for each event:

   - **Severity**—Severity of the event
   - **iLO IP Address**—The IPv4 or IPv6 address for the iLO
   - **Alert Category**—Type of event
   - **Alert Name**—Name of event
   - **TimeStamp**—Date and time stamp for each event

3. More options on this page:

   - Enter a value in the **Search** box and hit the enter key to search for specific information.
   - Use the **Show entries** menu and hit the enter key to choose the number of events to display per page.
   - Click the angle bracket icon to see a summary and description of the event, and whether any further action is required.

- Use the navigation buttons to view the first, previous, next, or last page of the alerts list. You can also click a specific page number to jump to that page.
- Click **Export to CSV** to download the server alerts list.
- Click **Clear All** to delete all alerts from the server alerts list.

Server alert severity

The following icons indicate event severity:

- **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.
- **Warning**—The event is significant but does not indicate performance degradation.
- **Ok**—The event falls within normal operation parameters.

Server alert details

The following information is listed for each managed server alert.

- **Severity**—The alert severity level
- **iLO IP Address**—The IPv4 or IPv6 address of the iLO processor on the managed server
- **Alert Category**—The alert type
- **Alert Name**—The alert name
- **TimeStamp**—The date and time that the alert was recorded

Clearing the Server Alert Viewer list

NOTE: A maximum of 10,000 alerts can be displayed in the server alert viewer.

Procedure

1. Select **Alerts and Event Logs** in the navigation tree, and then click **Managed Servers Alerts**.
2. Click **Clear All**.
3. When prompted to confirm the request, click **YES**.

Exporting server alerts to a .csv file

Procedure

1. Click **Alerts and Event Logs** from the left navigation menu, and then click **Managed Servers Alerts**.
2. Click **Export to CSV**.
3. Select a location to save the .csv file, and then click **Save**.

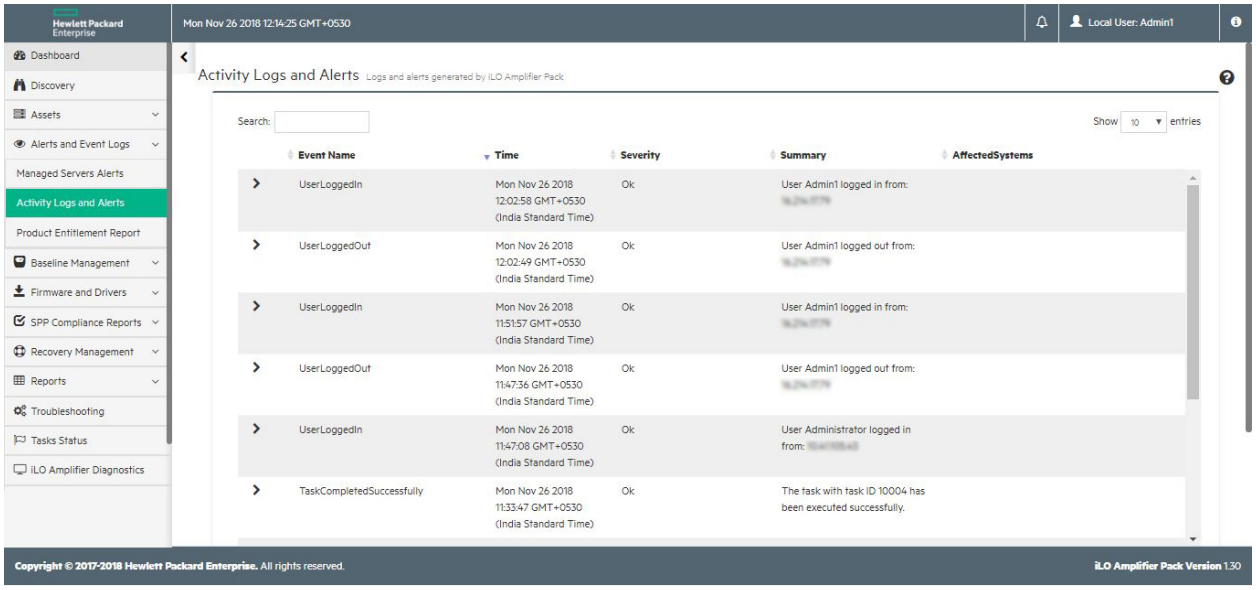
Activity Logs and Alerts

iLO Amplifier Pack records all activity that occurs in the system, whether generated by a user or by the appliance itself.

Activity Logs are sent as email or IFTTT alerts if configured by the user.

Viewing activity logs

Use this page to view logs and alerts generated by iLO Amplifier Pack.



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login

Procedure

1. Click **Alerts and Event Logs**.
2. Click **Activity Logs and Alerts**.

   The event list appears displaying the following information for each event:

   - **Event Name**—Name of event
   - **Time**—Date and time stamp for each event
   - **Severity**—Severity of the event

- **Event Summary**—Description of the event
- **Affected Systems**—Systems that are affected by the task

3. More options on this page:
   - Use the **Search** field to find a specific event.
   - Use the **Show entries** menu to choose the number of events to display per page.
   - Click the angle bracket next to an event to see a description of the event and whether any further action is required.
   - Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
   - Click **Export to CSV** to download the information in CSV format.
   - Click **Clear All** to clear the event list.

Clearing activity alerts

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Select **Activity Logs and Alerts** from the left navigation menu, and then click the **Activity Alerts** tab.
2. Click **Clear All**.
3. When prompted to confirm the request, click **YES**.

Generating and submitting the Product Entitlement Report

This page allows you to generate a product entitlement report. This report can be sent to HPE Support to verify warranty contract compliance for support issues.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

Procedure

1. Click **Alerts and Event Logs** from the left navigation menu.
2. Click **Product Entitlement Report**.
3. Enter a valid **HPE Passport User ID**.
4. Select the **Country**.
5. Click **Generate Request** to download the entitlement report. The report will be saved with the file name "**`iLOAmplifierPack_ProductEntitlementReport.csv`**".
6. Click the **Submit Request** button to open the **iLO Amplifier Pack Product Entitlement Report** webpage on HPE Support Center. Login using your HPE Passport account and upload the **`iLOAmplifierPack_ProductEntitlementReport.csv`** file on this page to submit the entitlement report.

   You will receive an email notification on the email id linked to your HPE Passport account when processing has completed. Switch to the **Product Entitlement Report History** tab to view or download previously processed entitlement reports.

Baseline Management

Importing a firmware baseline

Use the **Import Baseline** feature to make the SPP or custom SPP ISO image easily accessible for firmware updates. iLO Amplifier Pack supports baseline storage up to 80 GB (which includes both firmware and OS baseline files). The percentage of space used is displayed at the top of the **Firmware Baseline** page.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Firmware Baseline**.
2. Click **Import Baseline**.
3. Click to select **Network Share (NFS)** or **HTTP/HTTPS** from the **Import Type** menu.
4. Perform one of the following:
   - For NFS, enter the IPv4 or IPv6 address, mount path, and storage path.
   - Enter the HTTP or HTTPS url to the ISO image. This URL can be an IPv4 or IPv6 address.
5. Click **Import** to import the ISO image or click **Cancel** to return to the **Firmware Baseline** page.
6. Once the import completes, the baseline is listed on the **Firmware Baseline** page, along with the following information:
   - Filename of the .iso file
   - Name of the baseline
   - Version
   - Status of the import
   - File size in MB
7. Optional: Click  to delete the baseline.

   NOTE: You cannot delete a baseline if it is a part of a recovery policy or if it is being used by a task.
8. Optional: Click **View Details** for more information about the component, such as the component name, available version, filename, and recommendation.

The **Recommendation** field provides HPE recommendations for baseline components based on how critical each is for the update. The following values can help you select the baseline components you want to use:

- Recommended
- Critical
- Optional

Importing an OS baseline

OS baselines are user-created, bootable .iso images that are used in the server system restore process to recover the OS, layered applications, and data restore from backups.

Use the **Import Baseline** feature to import operating system .iso images for server system restore. iLO Amplifier Pack supports baseline storage up to 80 GB (which includes both firmware and OS baseline files). The percentage of space used is displayed at the top of the **OS Baseline** page.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **OS Baseline**.
2. Click **Import Baseline**.
3. Click to select **Network Share (NFS)** or **HTTP/HTTPS** from the **Import Type** menu.
4. Perform one of the following:
   - For NFS, enter the IPv4 or IPv6 address, mount path, and storage path.
   - Enter the HTTP or HTTPS url to the iso image.
5. Click **Import** to import the `.iso` image or click **Cancel** to return to the **OS Baseline** page.
6. Once the import completes, the baseline is listed on the **OS Baseline** page, along with the following information:
   - Filename of the `.iso` file
   - Name of the baseline
   - Status of the import
   - File size in MB
7. Click  to delete the baseline.

NOTE: You cannot delete a baseline if it is a part of a recovery policy or if it is being used by a task.

Working with configuration baselines

Configuration baselines are used to create or import the server configuration settings (like BIOS, iLO, and Smart Storage settings) and to restore it back on the servers during the server system restore process.

The **Configuration Baseline** page provides the following information in the **List of Configuration Baselines**:

- Status
- Configuration baseline name
- Configuration baseline type
- Created by

Use the **Configuration Baseline** page to create, import, edit, and delete configuration settings.

Create a configuration baseline

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click **New Configuration Baseline**.
3. Enter a name in the **Configuration Baseline Name** field.
4. Select properties from the following categories:
   - **BIOS Advanced, Generic, and Platform Settings**—For more information, see the UEFI documentation available from **http://www.hpe.com/info/ProLiantUEFI/docs**.

     NOTE: For recovery administration of Gen10 servers, HPE recommends configuring the BIOS boot mode to UEFI mode.
   - **Boot Settings**
   - **Smart Storage Settings**—For more information, see the smart storage and logical drive documentation available from **http://www.hpe.com/info/storage/docs**.
   - **iLO Settings**—For more information, see the iLO documentation available from **http://www.hpe.com/support/ilo-docs**.

5. Scroll through the list of parameters and click the check box to select the parameters you want to include in the baseline.
6. In the **Value** column, specify a value for each selected parameter.
7. Click **Create**.

   The new configuration baseline appears in the list on the **Configuration Baseline** page.

Import a configuration baseline from a server

Prerequisites

- User privileges
  - Configure Devices
  - Configure User
  - Configure Manager
  - Configure Manager with Security
- The server must be powered ON for import configuration to work. If the server is powered OFF the import configuration task fails.

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click **Import Configuration From Server**.
3. Enter a name in the **Configuration Baseline Name** field.
4. Click the check box to select a server, and then click **Import**.

   The new configuration baseline appears in the list of server configuration baselines on the **Configuration Baseline** page.

Editing a new configuration baseline

Use these instructions to edit customizable server configuration baselines.

NOTE: Snapshot server configuration baselines cannot be edited.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click the right arrow next to the baseline you want to edit from the **List of Server Configuration Baselines**.

   The baseline settings appear.
3. Select properties from the following categories:

   - **BIOS Advanced, Generic, and Platform Settings**—For more information, see the UEFI documentation available from **http://www.hpe.com/info/ProLiantUEFI/docs**.
   - **Boot Settings**
   - **Smart Storage Settings**—For more information, see the smart storage and logical drive documentation available from **http://www.hpe.com/info/storage/docs**.
   - **iLO Settings**—For more information, see the iLO documentation available from **http://www.hpe.com/support/ilo-docs**.
4. Scroll through the list of parameters and click the check box to select the parameters you want to change in the baseline.
5. In the **Value** column, specify a value for each selected parameter.
6. Click **Update** to save your changes.

Deleting a configuration baseline

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Baseline Management** from the left navigation menu, and then click **Configuration Baseline**.
2. Click the right arrow next to the baseline you want to delete, and then click **Delete**.

   NOTE: You cannot delete a baseline if it is a part of a recovery policy or if it is being used by a task.

Server firmware and driver updates

- To perform server firmware and driver updates on Gen8 and Gen9 servers, refer to **Online updates for Gen8 and Gen9 servers** and **Performing an offline firmware update**.
- To perform server firmware and driver updates on Gen10 servers and above, refer to **iLO repository updates**.

NOTE: Servers that are managed by HPE OneView are identified in the **Status** field. Servers managed by HPE OneView appear on the server list for inventory purposes, but cannot be updated by iLO Amplifier Pack.

IMPORTANT: Before commencing online updates, ensure that AMS is running and SUT Mode is set to **AutoDeployReboot** or **AutoDeploy**.

Performing an online firmware update for Gen8 and Gen9 servers

iLO Amplifier Pack offers two options for performing an online firmware update for Gen8 and Gen9 servers.

- **Express Interactive Update**

  The Express Interactive Update option gives you the ability to select the specific components you want to deploy on the servers from a baseline image that you select.

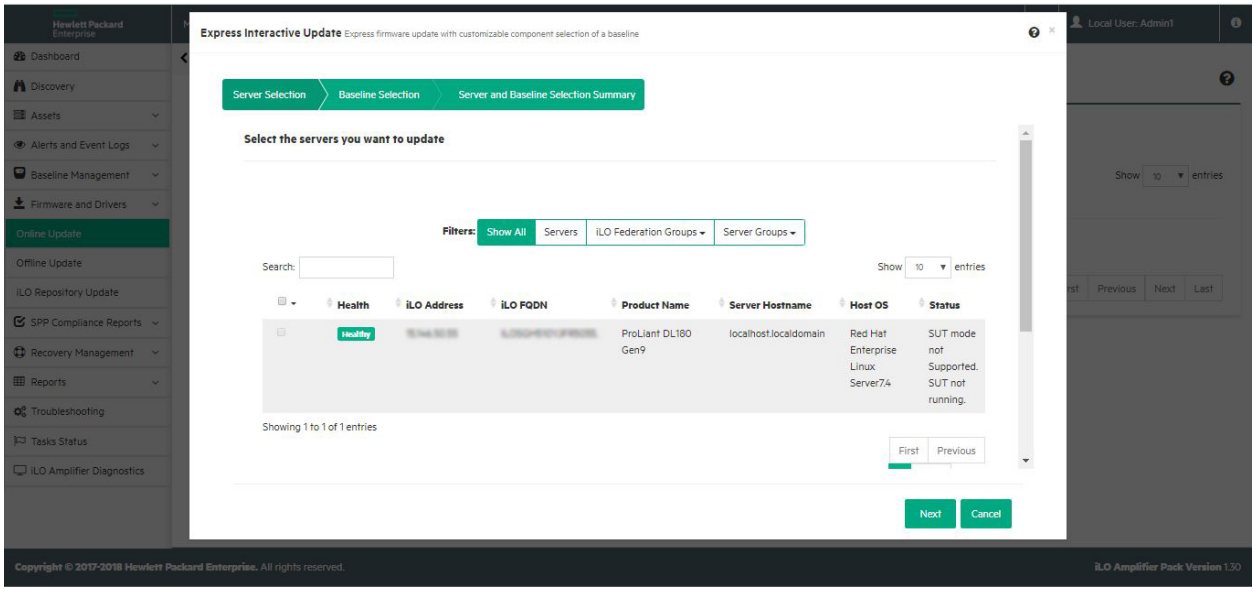
- **Baseline Automatic Update**

  The Baseline Automatic Update option allows you to update the servers with minimal interaction from a baseline image that you select. All applicable components are installed without waiting for approval.

  This option ensures that the target server is compliant with the selected baseline before the update begins.

NOTE: HPE recommends unmounting virtual media in servers before triggering the SPP update using iLO Amplifier Pack.

Performing an Express Interactive Update



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE SUT (Smart Update Tools) v1.8.0 or later installed on Gen8 and Gen9 servers (Recommended to update to SUT v2.0.0)
- AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux
- Bootable baseline ISO image of the firmware update imported into iLO Amplifier Pack (for more information, see **Importing a baseline**.

  Or

  Bootable baseline ISO image of the firmware update extracted to a shared HTTP/HTTPS location on the network and a dedicated web server for hosting SPP (HPE Support Pack for ProLiant) ISO images and files.

  NOTE: If you use an external web server to perform the online update, make sure that the following file extensions are added to the MIME Types settings in the external web server to ensure correct downloading:
  - .bin
  - .iso
  - .xml
  - .pdb

Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Online Update**.
2. Check the task status list to ensure that no tasks are running on the servers you want to update. Updates cannot be performed on servers while tasks are running. For more information about the task status list, see **Running and completed tasks**.
3. Click **Express Interactive Update**.
4. Select the servers that you want to update.

   NOTE: The iLO Amplifier Pack gets inventory details from the iLO and automatically batches servers while doing updates in case the number of servers is too large to be managed simultaneously.

5. Enter a common iLO username and password for the servers you want to update, and then click **Next**.

   The credentials will be used only for systems that are part of a federated group.

6. Select the baseline to use for the update by clicking one of the following options:

   - **Use imported baseline**

     If you have previously imported a baseline ISO image on the **Baseline Management** tab, the baseline name appears in the **Select the Baseline to set firmware** section.

     If you have not imported a baseline ISO image, a message appears directing you to import a baseline on the **Baseline Management** tab. For more information, see **Importing a firmware baseline**.

   - **Use external web server**

     a. Enter a valid URI for a bootable baseline ISO image of the firmware update that is available on the network through HTTP/HTTPS.

     NOTE: The ISO image must have been created by the SPP or a custom SPP. iLO Amplifier Pack calculates the install set from the SPP.

     b. Enter a valid URI for the extracted ISO image of the firmware update that is available on the network through HTTP/HTTPS.

     NOTE: The HTTP URL can be an IPv4 or an IPv6 address.

7. Specify the number of parallel updates you want to perform in the **Batch Size** field and then click **Next**. Up to 50 parallel updates are supported if you are using an external webserver.
8. Click **Begin Task**.

   NOTE: During an update, actions performed on the selected servers are set to a pending state. However, you can perform actions on clear servers using the other pages of the iLO Amplifier Pack.

9. When the status changes to **Waiting**, click **Analyze and Deploy** to switch between two views.

a. **Default View**—The **Component Selection** screen appears, displaying the component information for each server.

b. **Grid View**—The **Component selection** screen appears, displaying the component information for multiple servers in a single screen. The view can be filtered by selecting the Host OS Type filter.

10. Review each server component to designate which of them will receive the update.

- **Select**—Component will not receive the update. Click to select the component for update.
- **Selected**—Components with a status of **Update required** are marked as **Selected** by default to receive the update. Click to clear the selection.
- **Force**—Components with a status of **Already up-to-date** are not selected for the update by default. Click to force the update in cases where you want to reinstall the update or downgrade the firmware on a component.
- **Forced**—Component will be forced to receive the update. Click to clear the selection.

NOTE: iLO Amplifier Pack provides the install set to iSUT for the update; however, you must check the suggested install set before deploying the update.

---

11. Click **Apply All**.

iLO Amplifier Pack analyzes the server components to detect failed dependencies that will cause the update to fail. Clear these issues before proceeding with the update.

For more information, see the iSUT documentation at **http://www.hpe.com/info/isut-docs**.

The update process begins. The following messages appear in succession:

- Online Update Task in progress.
- **Pending**—iSUT is waiting to read the selected components for update.
- **Staging**—Analysis of selected components.
- **Staged**—Analysis of selected components completed and are waiting to be deployed.
- **Installing**—Selected components are being deployed on the server.
- **Installed**—Selected components are deployed.

12. Reboot the server, if necessary.

When the installation has completed, the task status will change to **Completed** with one of the following messages:

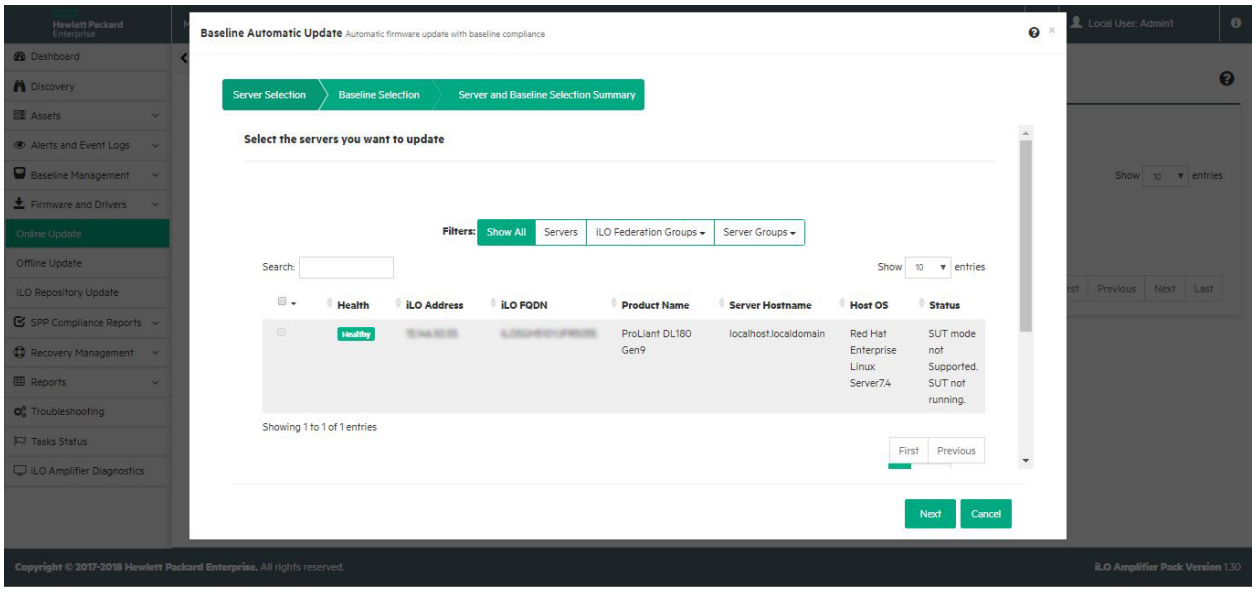
- **Activated**—Selected components are successfully installed (restart is not required).
- **Installed Pending Reboot**—Selected components are successfully installed, but you must restart the server.

NOTE: HPE recommends refreshing the server inventory after the system has restarted.

---

13. Click **Show Results** to see the components that were successfully updated along with any pending user actions.

Performing a Baseline Automatic Update



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE SUT (Smart Update Tools) v1.8.0 or later installed on Gen8 and Gen9 servers (Recommended to update to SUT v2.0.0)
- AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux
- Bootable baseline ISO image of the firmware update imported into iLO Amplifier Pack (for more information, see **Importing a baseline**).

  Or

  Bootable baseline ISO image of the firmware update extracted to a shared HTTP/HTTPS location on the network and a dedicated web server for hosting SPP (HPE Support Pack for ProLiant) ISO images and files.

NOTE: If you use an external web server to perform the online update, make sure that the following file extensions are added to the MIME Types settings in the external web server to ensure correct downloading:

- .bin
- .iso
- .xml
- .pdb

Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Online Update**.
2. Check the task status list to ensure that no tasks are running on the servers you want to update. Updates cannot be performed on servers while tasks are running. For more information about the task status list, see **Running and completed tasks**.
3. Click **Baseline Automatic Update**.
4. Select the servers that you want to update.

   NOTE: The iLO Amplifier Pack gets inventory details from the iLO and automatically batches servers while doing updates in case the number of servers is too large to be managed simultaneously.

5. Enter a common iLO username and password for the servers you want to update and then click **Next**.

   The credentials will be used only for systems that are part of a federated group.

6. Select the baseline to use for the update by clicking one of the following options:

   - **Use imported baseline**

     If you have previously imported a baseline ISO image on the **Baseline Management** tab, the baseline name appears in the **Select the Baseline to set firmware** section.

     If you have not imported a baseline ISO image, a message appears directing you to import a baseline on the **Baseline Management** tab. For more information, see **Importing a baseline**.

   - **Use external web server**

     Enter a valid URI for a bootable baseline ISO image of the firmware update that is available on the network through HTTP/HTTPS.

     NOTE: The ISO image must have been created by the SPP or a custom SPP. iLO Amplifier Pack calculates the install set from the SPP.

7. Specify the number of parallel updates you want to perform in the **Batch Size** field and then click **Next**. Up to 50 parallel updates are supported if the external baseline is used.
8. Click **Begin Task**.

   NOTE: During an update, actions performed on the selected servers are set to a pending state. However, you can perform actions on clear servers using the other pages of the iLO Amplifier Pack.

   The update process begins. The following messages appear in succession:

   - **Baseline Automatic Update Task in progress**
   - **Pending**—iSUT is waiting to read the selected components for update
   - **Staging**—Analysis of selected components
   - **Staged**—Analysis of selected components completed and waiting to be deployed
   - **Installing**—Selected components are being deployed on the server
   - **Installed**—Selected components are deployed

9. Reboot the server, if necessary.

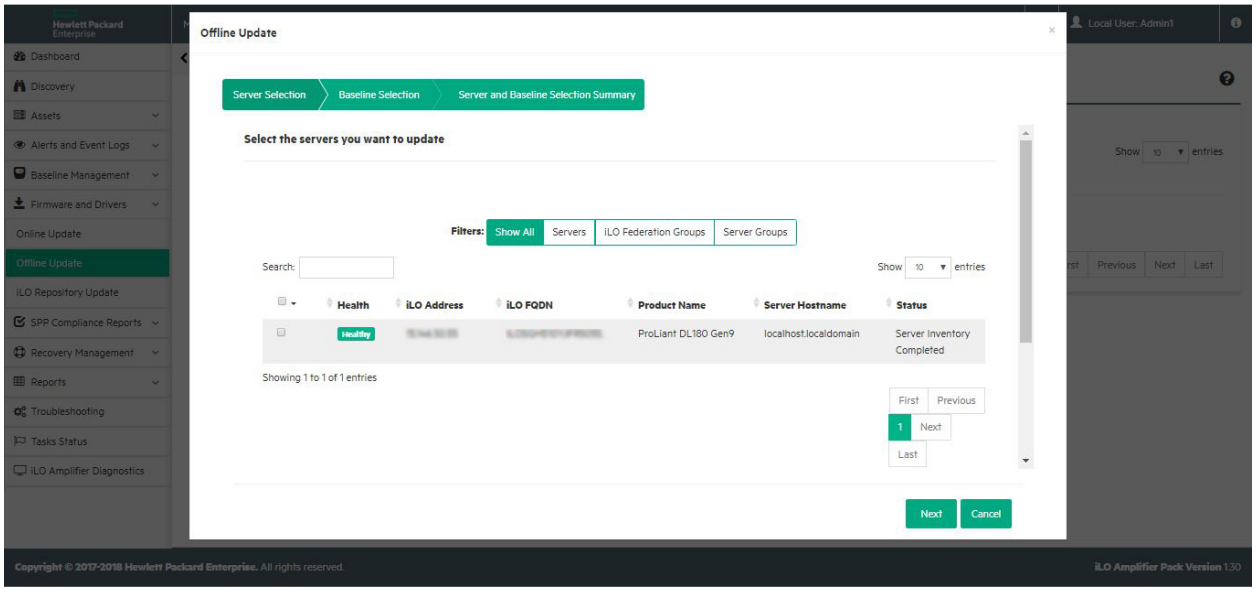
When the installation has completed, the task status will change to **Completed** with one of the following messages:

- **Activated**—Update has been completed (restart is not required).
- **Installed Pending Reboot**—Update has been completed, but you must restart the server.

NOTE: HPE recommends that you refresh the server inventory after the system has restarted.

10. Click **Show Results** to see the components that were successfully updated along with any pending user actions.

Performing an offline firmware update for Gen8 and Gen9 servers



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- Bootable baseline ISO image of the firmware update imported into iLO Amplifier Pack (for more information, see **Importing a baseline**).

  or

  Bootable baseline ISO image of the firmware update extracted to a shared HTTP/HTTPS location on the network and a dedicated web server for hosting SPP (HPE Support Pack for ProLiant) ISO images and files.

NOTE:

- Using a baseline update will alter all applicable components to be compliant with the baseline. iLO Amplifier Pack will downgrade components if necessary to comply with the baseline image.
- HPE recommends unmounting virtual media in servers before triggering the SPP update using iLO Amplifier Pack.

Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Offline Update**.
2. Select the servers, iLO Federation group or server group you want to update.

   NOTE: The iLO Amplifier Pack automatically batches servers while doing updates in case the number of servers is too large to be managed simultaneously.

3. Enter a valid URI for a bootable baseline (SPP) ISO image of the firmware update that is available on the network through HTTP/HTTPS.
4. Enter a common iLO username and password for the servers you want to update.

   The credentials will be used only for systems that are part of a federated group.

5. Click **Begin Task**.

   NOTE: During an update, you cannot perform actions on the selected servers, but you can perform actions on unselected servers using the other pages of the iLO Amplifier Pack.

   The update process begins. The following messages appear in succession:

   - **Pending**—iSUT is waiting to read the selected components for update.
   - **Staging**—Analysis of selected components.
   - **Staged**—Analysis of selected components completed and are waiting to be deployed.
   - **Installing**—Selected components are being deployed on the server.
   - **Installed**—Selected components are deployed.
   - **Installed Pending Reboot**—Selected components are successfully installed.

     NOTE: The system reboots automatically. User interaction is not required.

   - **Activated**—Selected components are successfully installed.

6. Click the **Running Task** tab to view the progression of the update.

   When the installation has completed, the task status will change to **Completed** with the message **Activated**. The system will automatically reboot.

   NOTE: HPE recommends that you refresh the server inventory after the system has restarted.

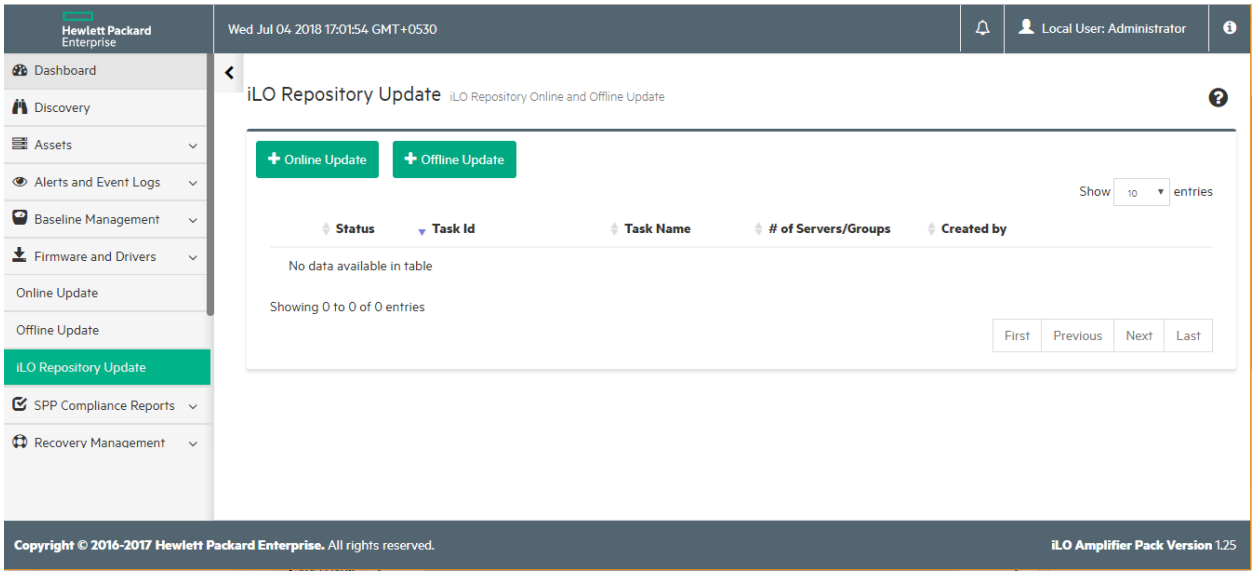
iLO Repository Updates

iLO Repository Updates is a new mechanism of firmware and software update available for Gen10 servers which use the iLO Repository of a server. After proper component selection, sequencing and dependency checking, the necessary components are uploaded to the iLO Repository of a server forming the specific install set. This specific install agent (iLO, BIOS, and SUT) updates the iLO Repository by pulling the component in sequence.

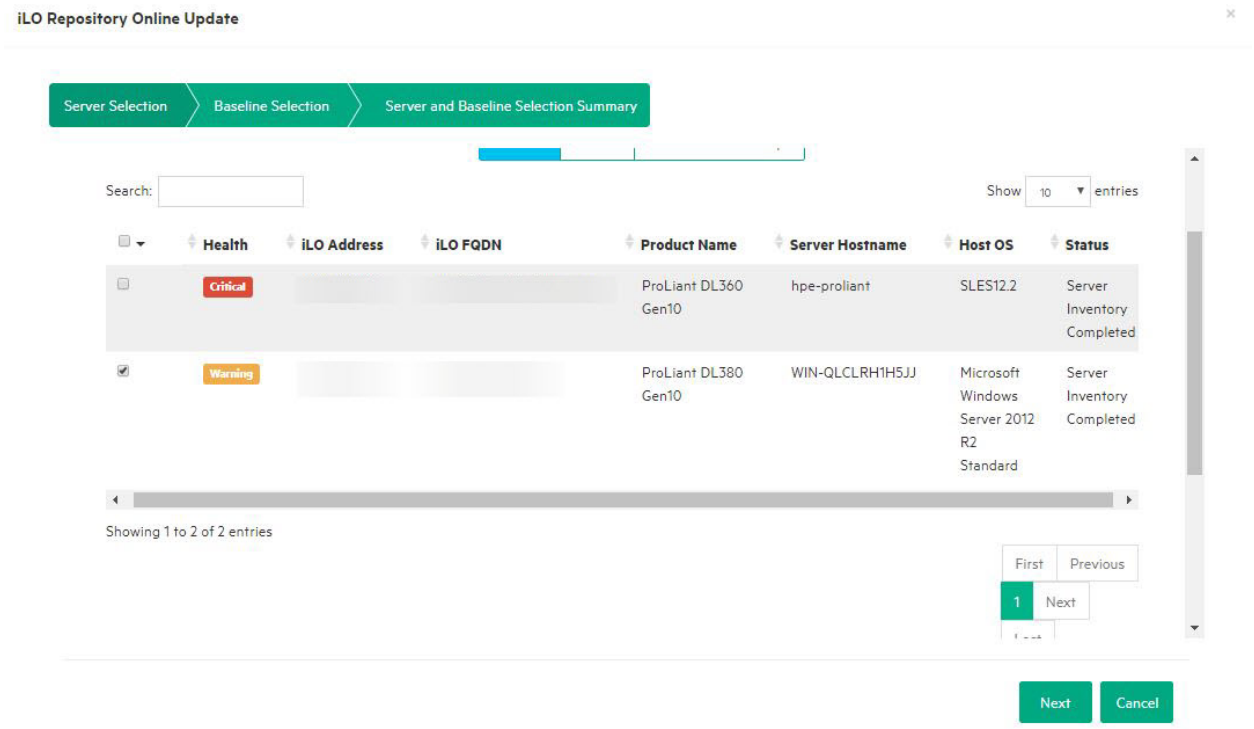
NOTE: iLO Amplifier pack v1.30 onwards supports updates on servers with VMWare ESXi OS version 6.0 and above.

iLO repository updates have two of the following options to perform the firmware updates:

- **Performing an iLO Repository Online Update**
- **Performing an iLO Repository Offline Update**



Performing an iLO Repository Online Update



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Devices
  - Configure User
- For servers set to the HighSecurity/FIPS state
  - Gen10 server with iLO 5 v1.30 or later.
  - SPP version 2018.11.0 or above.
- iSUT (Integrated Smart Update Tools) v2.3.0 and above.
- iSUT 2.3.6 and above for Gen10 servers running VMware ESXi OS.
- AMS must be running and SUT Mode must be set to 'AutoDeployReboot' or 'AutoDeploy'.

Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **iLO Repository Update**.
2. Click **Online Update**.
3. Select the servers that you want to update.

NOTE: The iLO Amplifier Pack gets inventory details from the iLO and automatically batches servers while doing updates in case the number of servers is too large to manage simultaneously.

4. Enter a common iLO username and password for the servers you want to update, and then click **Next**.

   The credentials will be used only for systems that are part of a federated group.

5. If you have previously imported a baseline ISO image on the **Baseline Management** tab, select the baseline name from the **Select the Baseline to set firmware** section.

6. If you have not imported a baseline ISO image, a message appears directing you to import a baseline on the **Baseline Management** tab. For more information, see **Importing a baseline**.

7. Select the **Clear iLO Repository after update** check box in the **iLO Repository Settings** field.

   NOTE: This step is optional.

8. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 20 parallel updates are supported.

9. Click **Begin Task**.

   The update process begins. The task status will be displayed under **Status** column.

10. Reboot the server, if necessary.

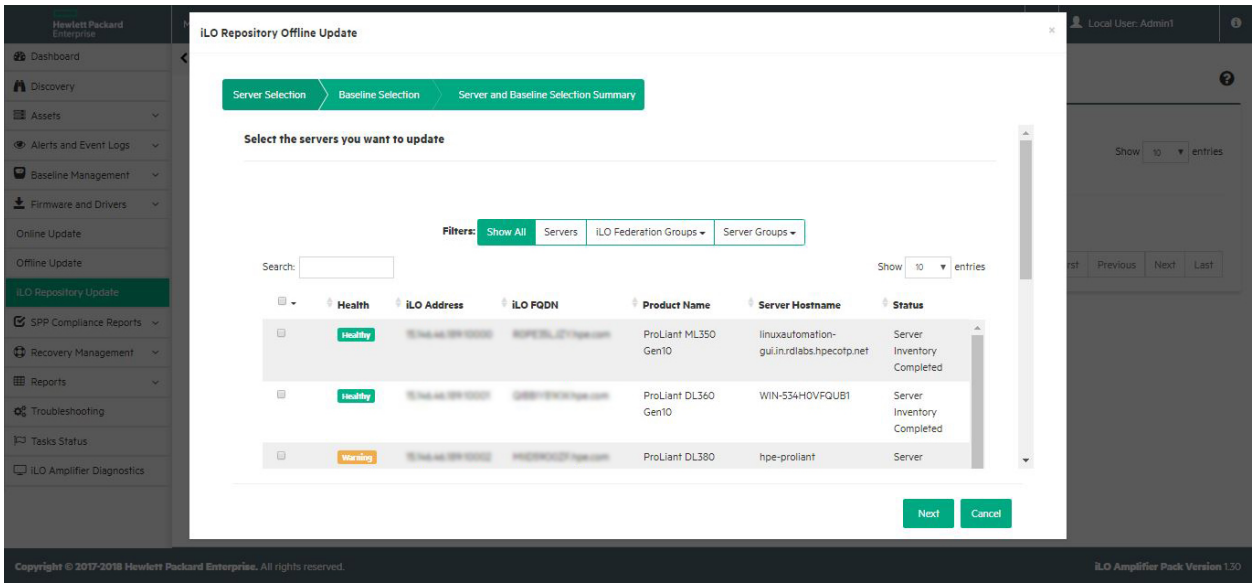
    When the installation has completed, the task status will change to **Completed**.

    For servers set to the HighSecurity/FIPS state, the task status will change to **Completed** with the message **iLO Repository Offline Update Completed. Results of High Security Mode update will be partial/incomplete.**

    NOTE: HPE recommends that you refresh the server inventory after the system has restarted.

11. Click **Show Result** to see the components that were successfully updated along with any pending user actions.

Performing an iLO Repository Offline Update



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Devices
  - Configure User
- For servers set to the HighSecurity/FIPS state
  - Gen10 server with iLO 5 v1.30 or later.
  - SPP version 2018.11.0 or above.

Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **iLO Repository Update**.
2. Click **Offline Update**.
3. Select the servers that you want to update.

   NOTE: The iLO Amplifier Pack gets inventory details from the iLO and automatically batches servers while doing updates in case the number of servers is too large to manage simultaneously.
4. Enter a common iLO username and password for the servers you want to update, and then click **Next**.

   The credentials will be used only for systems that are part of a federated group.
5. If you have previously imported a baseline ISO image on the **Baseline Management** tab, select the baseline name from the **Select the Baseline to set firmware** section.
6. If you have not imported a baseline ISO image, a message appears directing you to import a baseline on the **Baseline Management** tab. For more information, see **Importing a baseline**.
7. Select the **Clear iLO Repository after update** check box in the **iLO Repository Settings** field.

   NOTE: This step is optional.
8. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 50 parallel updates are supported.
9. Click **Begin Task**.

   The update process begins. The task status will be displayed under **Status** column.
10. Reboot the server, if necessary.

    When the installation has completed, the task status will change to **Completed**.

    For servers set to the HighSecurity/FIPS state, the task status will change to **Completed** with the message **iLO Repository Offline Update Completed. Results of High Security Mode update will be partial/incomplete.**

    NOTE: iLO Repository Offline Update is not supported in CNSA Mode.

NOTE: HPE recommends that you refresh the server inventory after the system has restarted.

11. Click **Show Result** to see the components that were successfully updated along with any pending user actions.

Running and completed tasks

You can monitor the progress of firmware update tasks and the results of completed tasks from the **Online Update** and **Offline Update** pages. The following information is displayed:

- **Status**—Progress of the selected task.
- **Task ID**—ID assigned to the task.
- **Task Name**—Name of the task.
- **Number of Servers**—Number of servers affected by the task.
- **Created by**—Username of the person who initiated the task.
- **Results**—Displays the following information about completed tasks:
  - **Component Name**—Name of the hardware that was updated.
  - **Previous Installation**—Firmware version that was on the component before the update.
  - **Installed Version**—Firmware version that was installed during the update.
  - **Deployment Result**—Displays success or failure of the update.
- **Abort Task**—Allows you to cancel a running task.

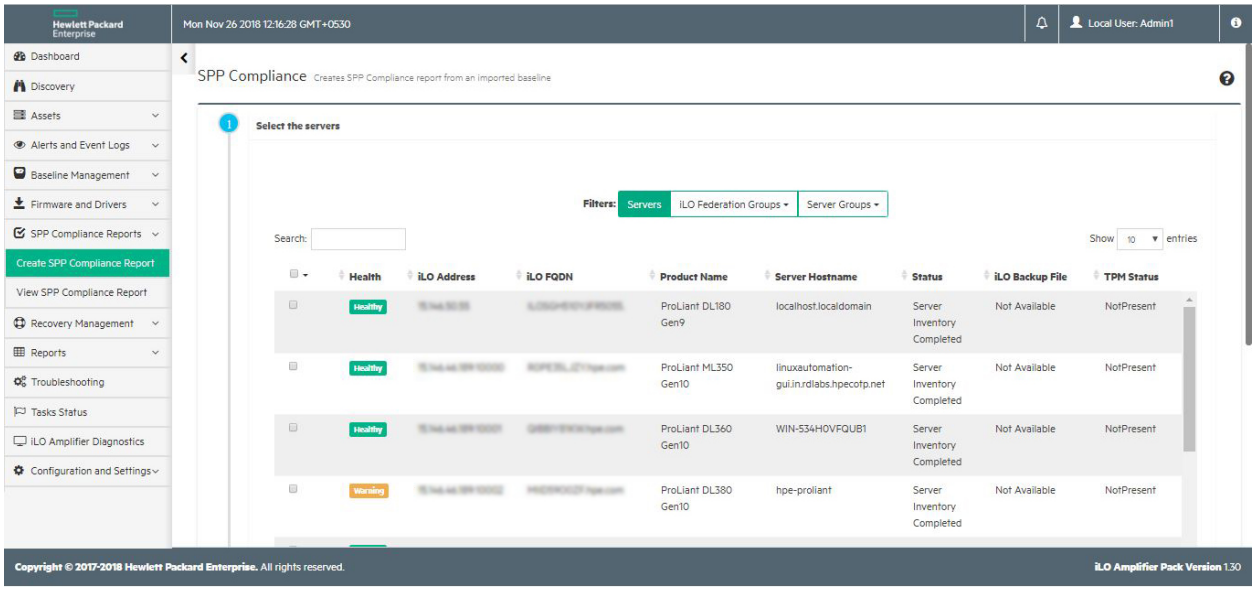
NOTE: Tasks cannot be aborted at later stages of the update procedure.

SPP compliance report

The SPP compliance report provides information about the compliance status of a server. This report displays the server compliance of the firmware and software components for an imported SPP.

iLO Amplifier Pack allows the users to generate SPP compliance reports for multiple servers at a time.

Creating the SPP compliance report



Prerequisites

- iLO Amplifier Pack user with the following privileges:
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices
- Import SPP to create an SPP Compliance report

Procedure

1. From the left navigation menu, select SPP **Compliance Report** > **Create SPP Compliance Report**.
2. Select the server for which you want to generate the report.

   You can select multiple servers at a time to generate the report.

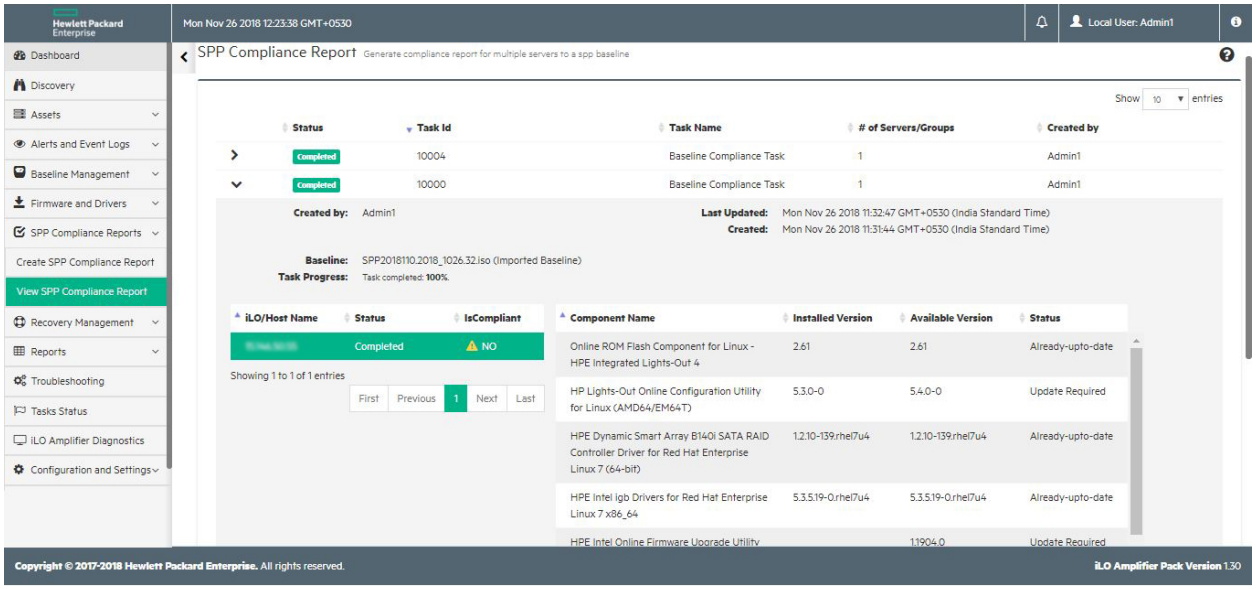
   NOTE: If the selected servers are part of an iLO Federation group, common credentials are required.
3. Select the Baseline for creating SPP Compliance Report.
4. To view **SPP Compliance Summary**, click **Begin Task**.

5. To create the SPP Compliance report, Click **Start**.
6. A task is created, which may show one or all the following states of task:
   - **Pending**
   - **Running**
   - **Complete**
   - **CompletedwithException**
   - **Failed**
7. The SPP compliance report is generated.

   NOTE: It may take a while to generate the report.

Viewing the SPP compliance report

NOTE: If HPE ProLiant Gen8 servers, HPE ProLiant Gen9 servers, and HPE ProLiant Gen10 servers are selected together when creating an SPP Compliance Report, two separate reports are created – one for Gen8 and Gen9 servers and the other for Gen10 servers.



Prerequisites

The SPP compliance report is generated.

For detailed information, see **Creating the SPP compliance report**.

Procedure

1. From the left navigation menu, click **View SPP Compliance Report**.
2. To see the compliance status of the individual components of the server, click and expand the task id listed.

   The table with servers provides the following details:

- **IsCompliant—**Displays whether the server is compliant with the baseline used.
- **Component Name**—Displays the server name.
- **Installed version**—Displays the installed version of the component.
- **Available version**—Displays the latest available version for the component.
- **Status**—Displays if the update is required.

An SPP compliance report contains only firmware component information for certain servers in the following cases:

- Server is in the power off state.
- The OS installed on the server is ESXi. (Only for Gen8 and Gen9 servers.)
- The associated server does not have AMS running.

3. To export the report to CSV file, click **Export to CSV**.

Recovery Management

Introduction

The Server System Restore feature that works with iLO 5 v1.17 or later to recover Gen10 servers according to user-created recovery policies.

When iLO detects system corruption in a server that is monitored by iLO Amplifier Pack, iLO automatically alerts iLO Amplifier Pack to initiate and manage the system recovery process. iLO Amplifier Pack checks the event against user-created recovery policies for the affected system, and then begins the recovery process as outlined in the recovery policy assigned to the server.

Prerequisites

- Gen10 server with iLO 5 v1.17 or later.
- For servers set to the HighSecurity/FIPS state
  - Gen10 server with iLO 5 v1.30 or later.
  - SPP version 2018.11.0 or above.
- An iLO Advanced license is required to use Server System Restore.
- To perform any recovery-related actions, iLO Amplifier Pack user must have Configure Manager with Security privilege.
- The Firmware Baseline to be used for recovery should have iLO 5 v1.17 or later.
- For recovery administration of Gen10 servers, HPE recommends configuring the BIOS boot mode to UEFI mode.
- For Device initiated full auto recovery, the recovery policy must have all three baselines specified: Firmware + Configuration + Operating System
- You must have at least one recovery install set in iLO before triggering a Device Initiated recovery. HPE recommends not deleting the iLO Factory Install set to use the recovery feature in iLO Amplifier Pack.

More information

The following pages in iLO Amplifier Pack provide the tools to define recovery policies, assign them to managed servers, and monitor the recovery process.

- **Recovery Policy**
- **Recovery Administration**
- **Recovery Task Monitor**

Recovery operations

Each recovery operation follows a similar path:

Automatic recovery operations

Follow these steps to perform an Automatic Server Recovery or a Device Initiated Full Recovery.

1. Import firmware and OS baselines. For more information, see **Importing a firmware baseline** and **Importing an OS baseline**.
2. Create a Complete iLO configuration backup on the iLO NAND. This will create a backup of the complete configuration of iLO on the iLO NAND.

   NOTE: This option is only available for Gen10 servers running iLO 5 v1.37 and later.

3. Create or import a configuration baseline from a server. For more information, see **Create a configuration baseline** and **Import a configuration baseline from a server**.
4. Create a recovery policy with the firmware, configuration, and OS baselines. For more information, see **Create a recovery policy**.
5. Assign a recovery policy to the selected servers with **Auto Recovery Action** enabled. For more information, see **Assign a recovery policy**.
6. A recovery task is triggered in iLO Amplifier Pack once it receives a recovery message from iLO when it finds corrupted firmware.

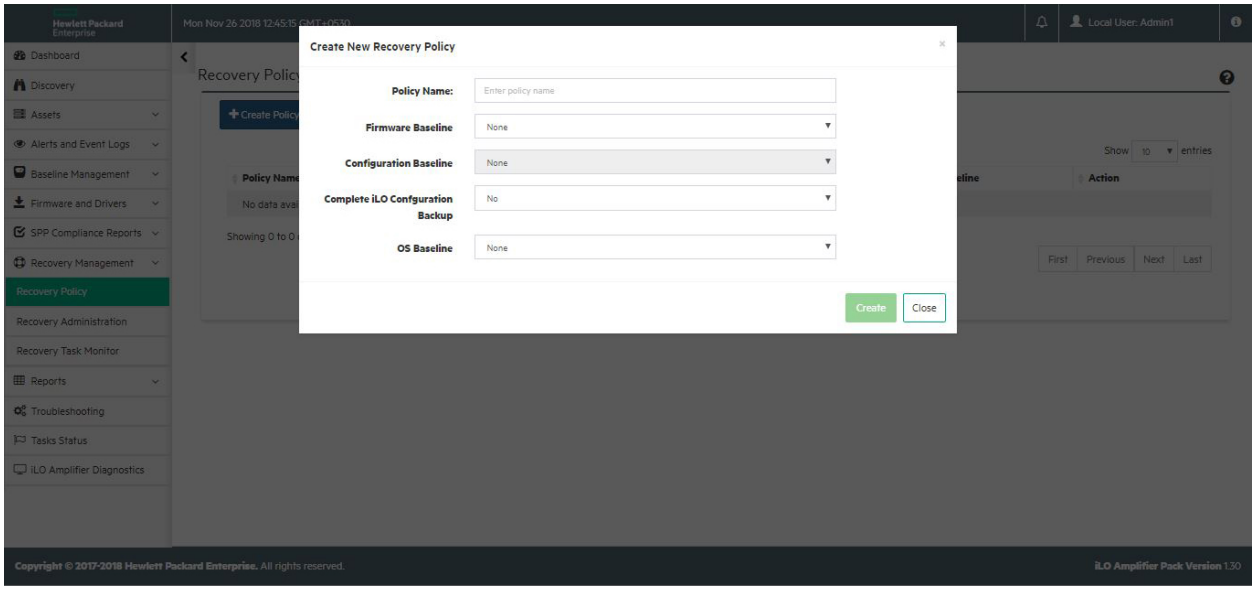
Manual recovery operations

Follow these steps to perform a Manual Recovery:

1. Import firmware and OS baselines. For more information, see **Importing a firmware baseline** and **Importing an OS baseline**.
2. Once iLO Amplifier Pack receives a firmware corruption alert from iLO, the check box becomes enabled for the selected server on the **Administration** page.
3. You can select and perform a Manual Recovery by selecting the required baselines or a recovery policy. For more information, see **Performing a manual recovery**.

Recovery policy

Create a recovery policy



Prerequisites

- User privileges
  - Configure Manager with Security
- To create a recovery policy that includes an OS baseline or a firmware baseline, you must first upload the baselines to iLO Amplifier Pack from the **Baseline Management** page.

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Policy**.
2. Click **Create policy**.
3. Enter a name for the new policy, and then select firmware, configuration, and OS baselines.

   You can also select Complete iLO configuration Backup to backup iLO configuration settings on the iLO NAND. This option is available only for Gen10 servers running iLO 1.37 and later.

   The following combinations are supported:

   - Firmware only
   - Firmware + Configuration
   - Operating System only
   - Firmware + Configuration + Operating System

   NOTE:

   - The list of firmware baselines includes only those that have been successfully uploaded to iLO Amplifier Pack.
   - The list of firmware baselines includes only those containing firmware that supports Gen10 servers and later.
   - The list of configuration baselines does not list the snapshot configuration baselines that are still importing or those that failed to import.
   - Any iLO settings in the configuration baseline will overwrite the settings restored from the iLO NAND.
   - All users upgrading from iLO Amplifier Pack 1.25 to any higher version will need to create a recovery policy and reassign them to the servers before using Complete iLO configuration backup.

4. Click **Create** to save the policy.

   The new policy appears in the list on the **Recovery Policy** page.

Delete a recovery policy

Prerequisites

- User privileges
  - Configure Manager with Security
- Before deleting a recovery policy, unassign the policy from any servers to which it might be assigned.

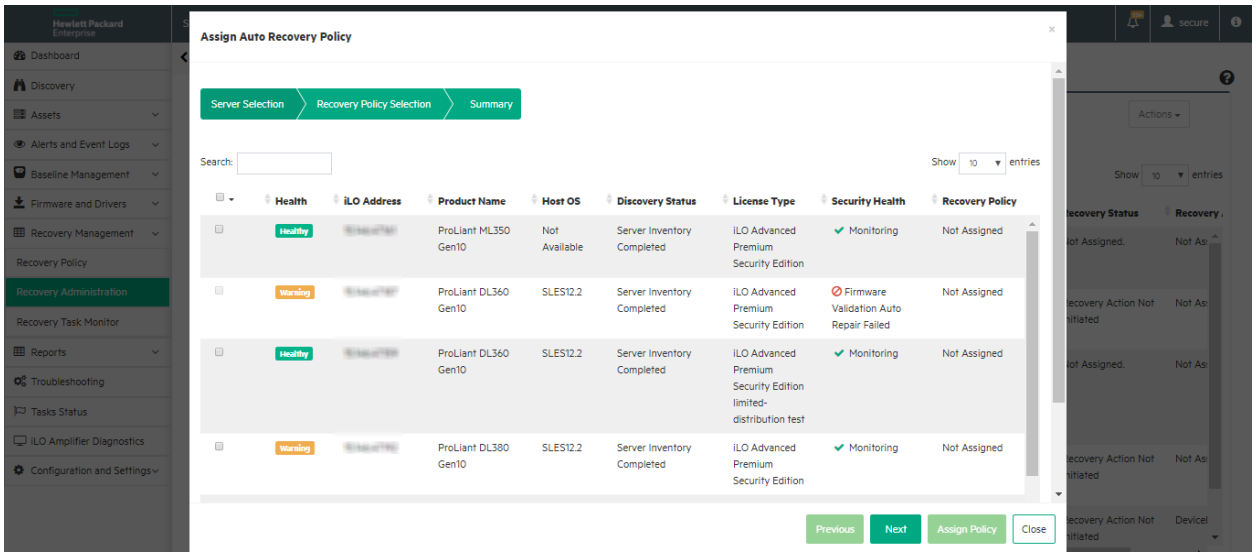
Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Policy**.
2. Click the  icon for the policy that you want to delete.

Recovery administration

The **Recovery Administration** page lists all the Gen10 servers with an iLO Advanced license that are managed by iLO Amplifier Pack. When a firmware corruption occurs on a system, iLO detects this corruption and sends out an event to iLO Amplifier Pack. iLO Amplifier Pack then initiates the recovery process based on the recovery policy that is assigned to the server.

Assign a recovery policy



Prerequisites

- User privileges
  - Configure Manager with Security
- Gen10 server with iLO 5 v1.17 or later
- iLO Advanced license

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Administration**.
2. Click **Assign Auto Recovery Policy**.
3. Click the check box to select one or more servers, and then click **Next**.
4. Select one of the following options from the **Action** drop-down menu:

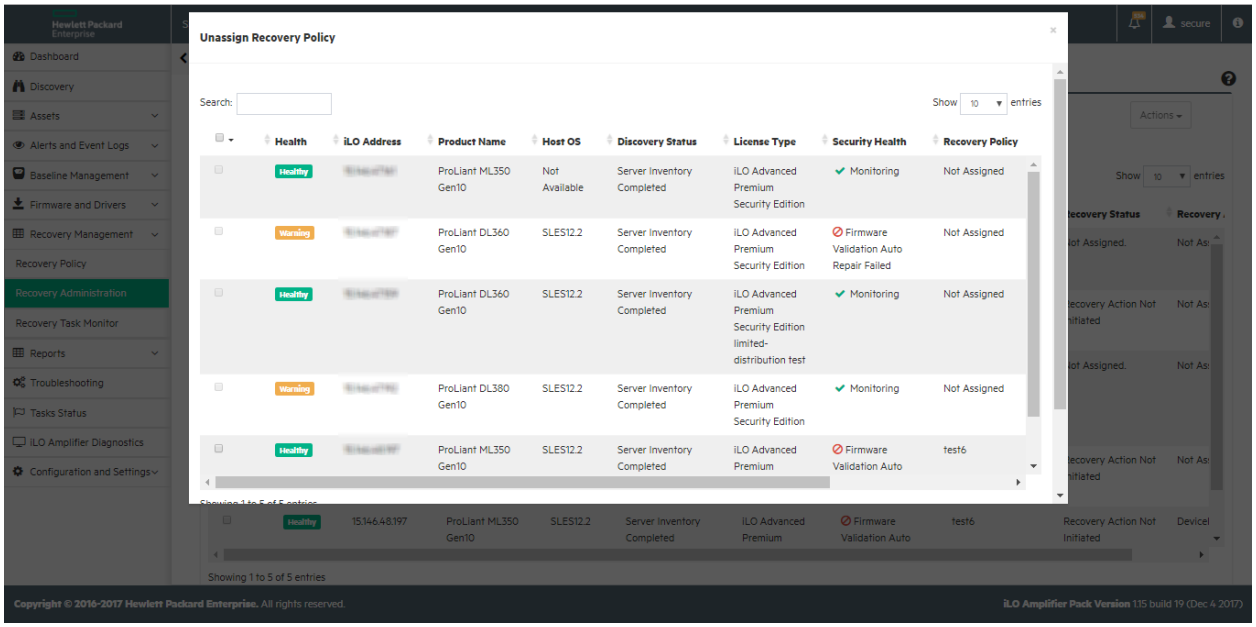
- **Auto Recovery**—Recovery process starts when iLO Amplifier Pack is automatically alerted from iLO.
- **Device Initiated Full Auto Recovery**—Recovery process starts when a user manually initiates a recovery alert from iLO to iLO Amplifier Pack. A user can initiate a recovery alert from iLO by logging in to iLO with a user account that has recovery set privileges. In the iLO interface, navigate to the **Administration** > **Firmware Verification** page, and then click **Send Recovery Event**.
- **Quarantine**—Recovery process is not started, but server is shut down automatically from iLO Amplifier Pack.

5. Select the recovery policy that you want to apply from the **Recovery Policy** drop-down menu, and then click **Next**.
6. Verify your selections as displayed on the **Summary** page, and then click **Assign Policy** or click **Previous** to go back to change selections.

NOTE: For Device initiated full auto recovery, the recovery policy must have all three baselines specified:

Firmware + Configuration + Operating System

Unassign a recovery policy



Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

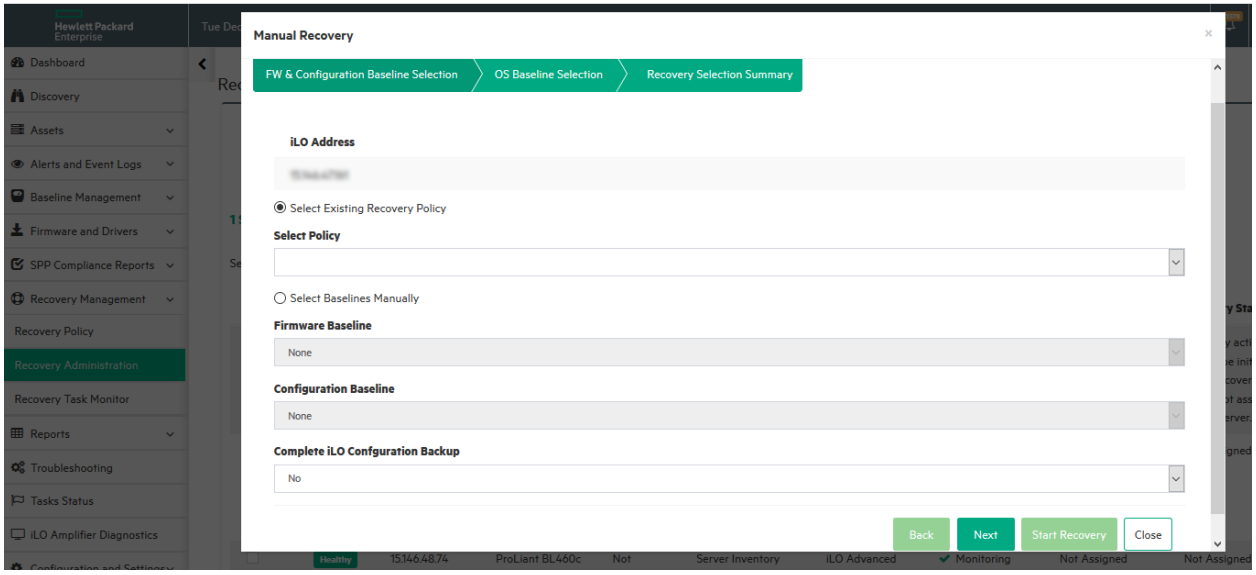
1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Administration**.
2. Click **Unassign Recovery Policy**.

   NOTE: This action will also delete any Complete iLO configuration backup created on the iLO NAND by a recovery policy.

3. Click the check box to select one or more servers, and then click **Unassign**.

Performing a manual recovery

The **Recovery Administration** page lists all the Gen10 servers with an iLO Advanced license that are managed by iLO Amplifier. When a firmware corruption happens on a system, iLO detects this corruption and sends out an event to iLO Amplifier. When this event is received, iLO Amplifier enables the check box on the **Recovery Administration** page. Select the system, and then perform the Manual Recovery.



Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Administration**.
2. Select the servers on which you want to perform a manual recovery.

3. From the **Actions** drop-down menu, click **Manual Recovery**.
4. On the **Manual Recovery** page, select a recovery policy from the drop-down menu.
5. Select a firmware and/or configuration baseline from their respective drop-down menus, and then click **Next**.
6. Optional. If a Complete iLO configuration backup has been created, select **`Yes`** to restore from this backup. If no backup has been created, the task will continue to the next step.
7. Select an OS baseline, and then click **Next**.
8. Review your selections and click **Back** to make changes, if needed.
9. Click **Start Recovery**, and then click **Close**.

   Check the progress of the manual recovery task on the **Recovery Task Monitor** page.

Performing a quarantine operation

Prerequisites

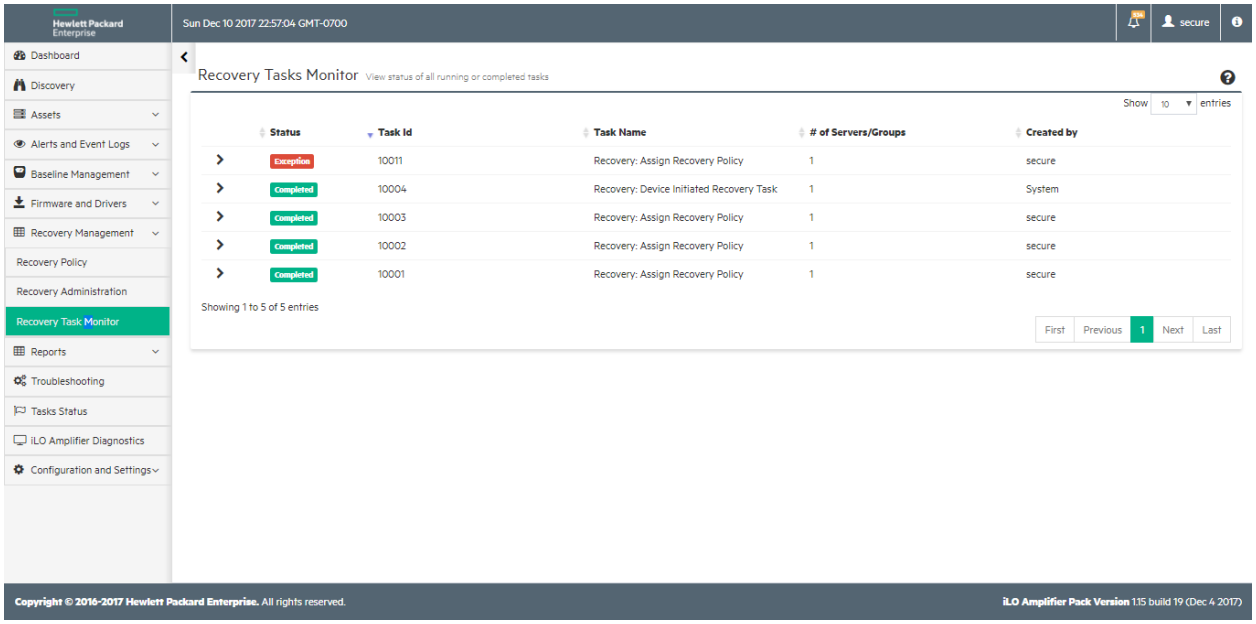
- User privileges
  - Configure Manager with Security

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Administration**.
2. Select the servers on you want to quarantine.
3. From the **Actions** drop-down menu, click **Quarantine**.
4. Click **Yes** on the **Quarantine Confirmation** dialog box to continue or click **No** to cancel the operation.

   Check the progress of the quarantine task on the **Recovery Task Monitor** page.

Monitor recovery tasks



Prerequisites

- User privileges
  - Configure Manager with Security

Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Monitor Recovery Tasks** to view all the status of all running and completed tasks.
2. Click the right arrow to see details and the percentage of the task progress.

   iLO Amplifier Pack applies the recovery policy in the following order:

   a. The server is powered down.

   b. The firmware is updated, if selected.

   c. The Complete iLO configuration backup stored on the iLO NAND will be restored, if selected.

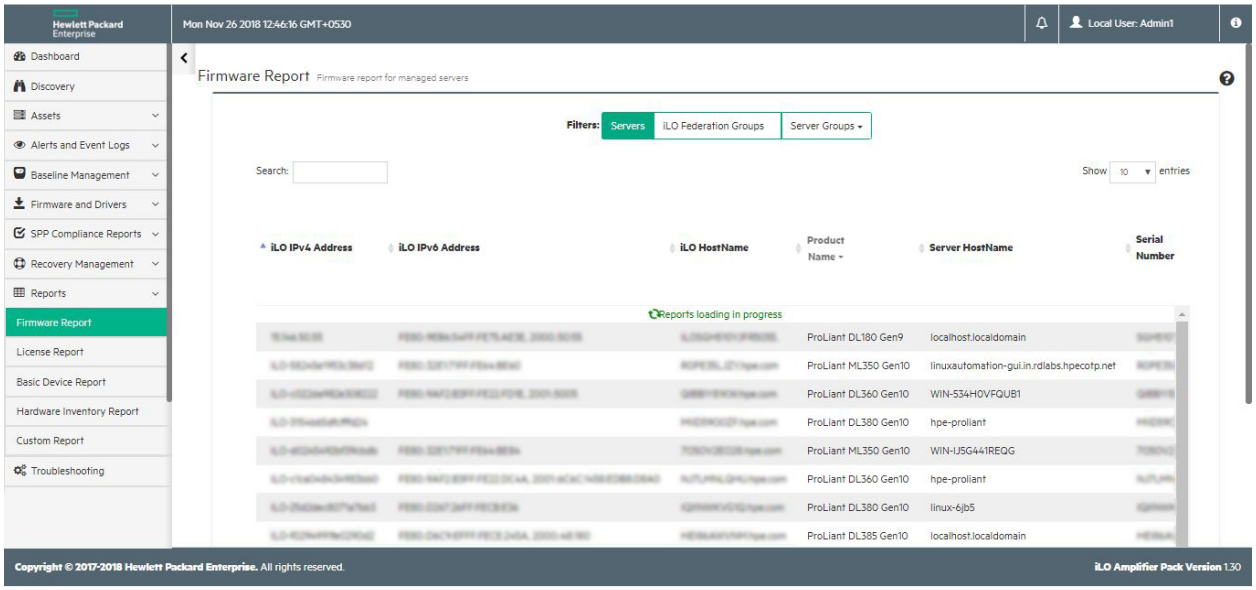
   d. The configuration baseline is applied, if selected.

   e. The server is rebooted to the OS baseline, if selected.

   The recovery process may take a while to complete. See the **Activity Logs and Alerts** page for the status of the recovery process.

Reports

Viewing the firmware report



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- For Gen8 and Gen9 servers: AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on the managed servers
- For Gen10 servers: AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux

Procedure

1. Click **Reports** on the left navigation menu.
2. Click **Firmware Report**.

   The report provides information on the iLO, System, ROM, NIC, and storage devices. For a full list, see **Firmware report details**.
3. Options on this page:

- Enter a value in the **Search** box and hit the enter key to search for specific information.
- Use the **Servers, iLO Federation Groups or Server Groups** filter to customize the display.
- Use the **Show entries** menu to choose the number of entries to display per page.
- Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
- Click **Export to CSV** to download the report in CSV format.

Firmware report details

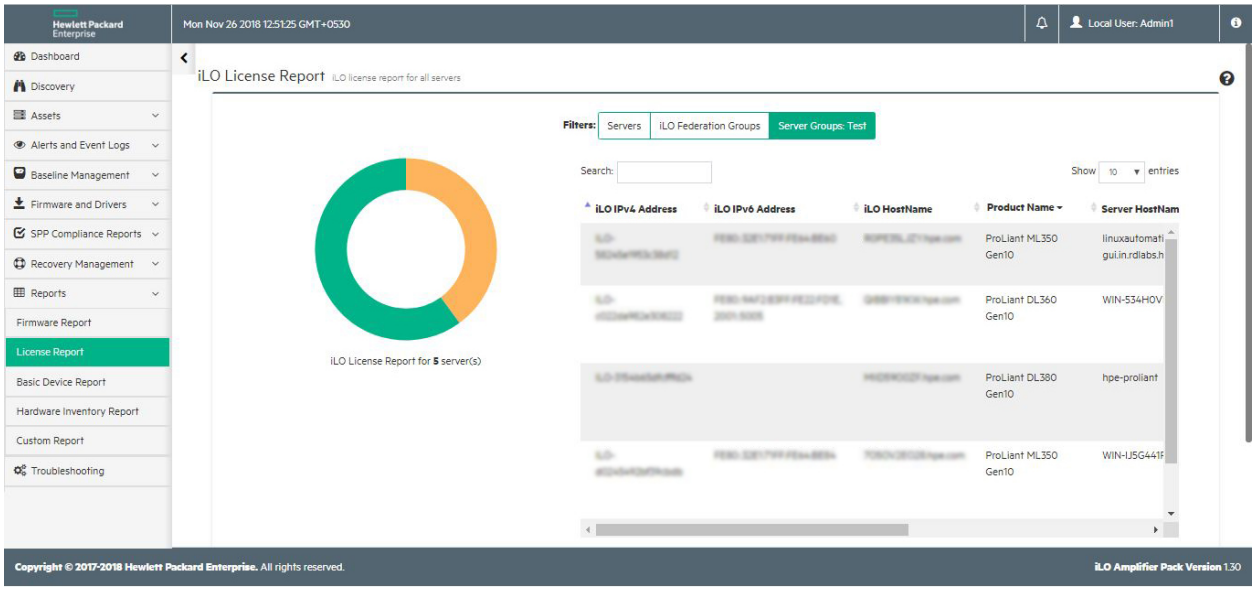
The following information appears in the firmware report details.

- iLO IP Address—The network IP address of the iLO subsystem.
- iLO HostName—The fully qualified network name assigned to the iLO subsystem.
- Product Name—The product with which the iLO processor is integrated.
- Serial number—The server serial number, which is assigned when the system is manufactured.
- Server Hostname—The fully qualified network name assigned to the server.
- iLO Firmware—The version and date of the installed iLO firmware.
- System ROM—The version of the active system ROM.
- System ROM - backup—The version of the backup system ROM. If a system ROM update fails or is rolled back, the backup system ROM is used.
- Intelligent Provisioning—A web interface you can use to perform operating system deployments and review in-depth hardware configuration details.
- Possible firmware options:
  - Intelligent Platform Abstraction Data
  - Power Management Controller Firmware
  - Power Management Controller FW Bootloader
  - System Programmable Logic Device
  - Server Platform (SPS) Firmware
- PCI device information:
  - PCI Devices - Name
  - PCI Devices - Location
  - PCI Devices - Version
- Network device information:
  - Network Devices - Name
  - Network Devices - Version
- Storage device information:

- Storage Devices - Name
- Storage Devices - Version

Viewing the iLO license report

Hover your mouse over the ring chart to see the number and type of licenses for the selected view.



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- For Gen8 and Gen9 servers: AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on the managed servers
- For Gen10 servers: AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux

Procedure

1. Click **Reports** on the left navigation menu.
2. Click **License Report**.

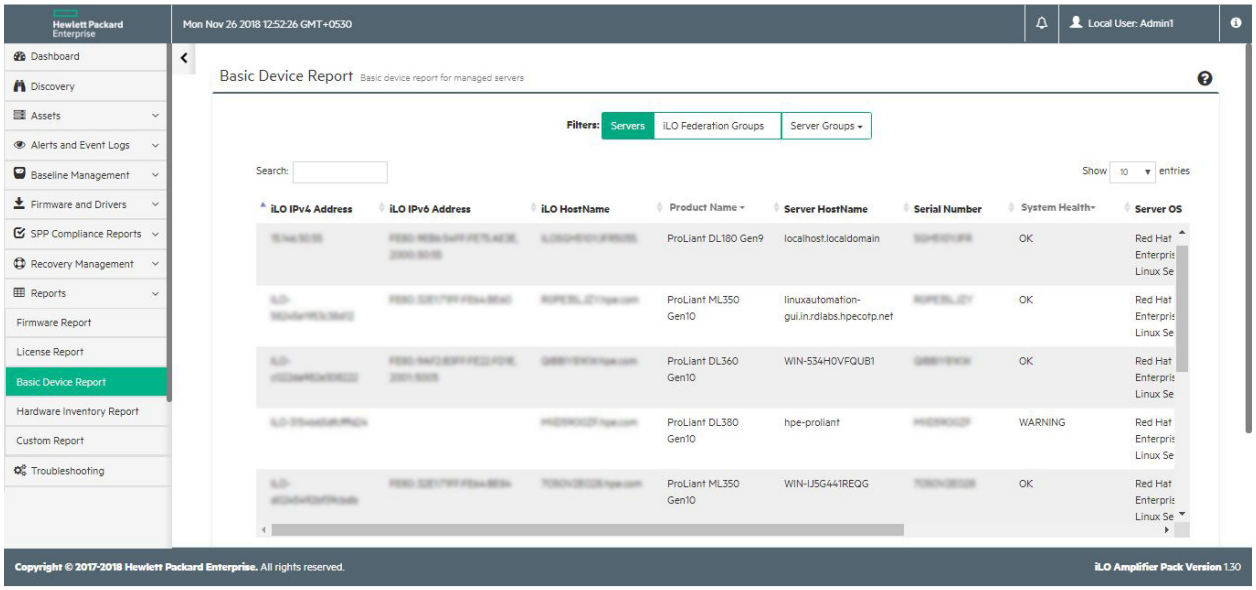
   The following information appears:

   - **iLO IP Address**—The network IP address of the iLO subsystem
   - **iLO HostName**—The fully qualified network name assigned to the iLO subsystem

- **Product Name**—The product with which the iLO processor is integrated
- **Server HostName**—The server name defined by the host operating system
- **Serial number**—The server serial number, which is assigned when the system is manufactured
- **License Key**—Key provided with iLO license
- **License**—The license level purchased with iLO
  - iLO Standard
  - iLO Essentials
  - iLO Scale-Out
  - iLO Advanced
- **License Type**—The level of licensed iLO firmware functionality
  - **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.

3. Options on this page:
   - Enter a value in the **Search** box and hit the enter key to search for specific information.
   - Use the **Servers, iLO Federation Groups or Server Groups** filter to customize the display.
   - Use the **Show entries** menu to choose the number of entries to display per page.
   - Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
   - Click **Export to CSV** to download the report in .csv format.

Viewing the basic device report



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- For Gen8 and Gen9 servers: AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on the managed servers
- For Gen10 servers: AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux

Procedure

1. Click **Reports** on the left navigation menu.
2. Click **Basic Device Report**.

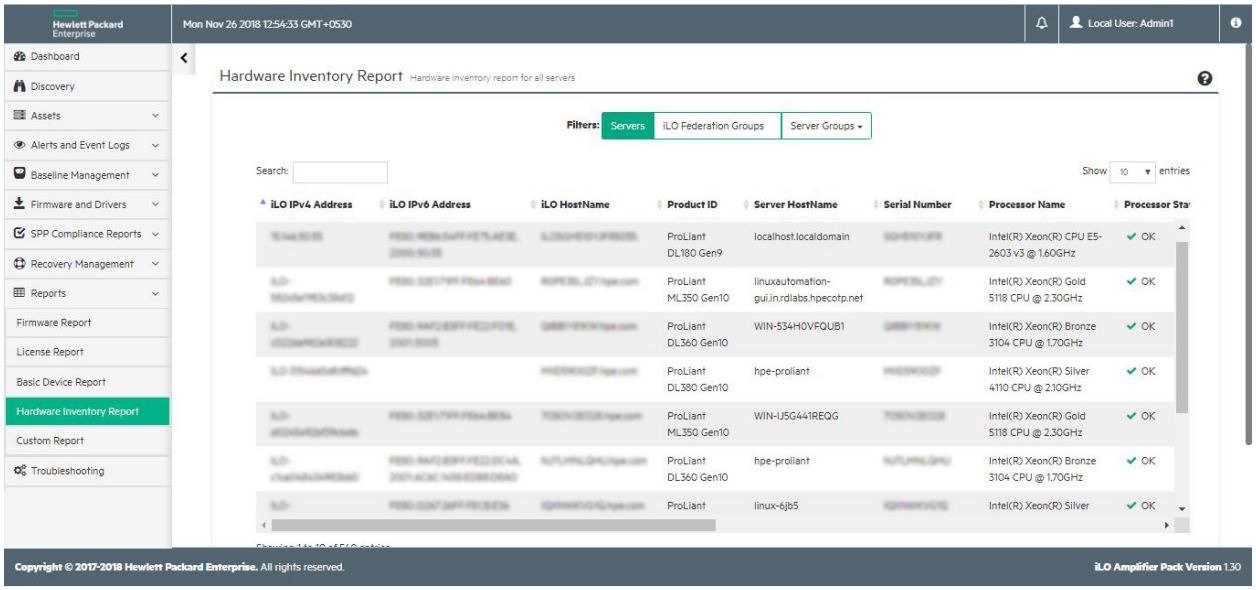
   The following information appears for each managed server:

   - **iLO IP Address**—The network IP address of the iLO subsystem.
   - **iLO HostName**—The fully qualified network name assigned to the iLO subsystem.
   - **Product Name**—The product with which the iLO processor is integrated.
   - **Server HostName**—The server name defined by the host operating system.
   - **Serial number**—The server serial number, which is assigned when the system is manufactured.

- **System Health**—The server health indicator summarizing the condition of the monitored subsystems, including overall status and redundancy (ability to handle a failure).
- **Server OS**—The operating system installed on the server
- **Server OS Version**—The version of the operating system installed on the server
- **iLO Firmware**—The version and date of the installed iLO firmware.
- **System ROM**—The version of the active system ROM.

3. Options on this page:
   - Enter a value in the **Search** box and hit the enter key to search for specific information.
   - Use the **Servers, iLO Federation Groups or Server Groups** filter to customize the display.
   - Use the **Show entries** menu to choose the number of entries to display per page.
   - Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
   - Click **Export to CSV** to download the report in CSV format.

Viewing the Hardware Inventory Report



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User

- Configure Devices
- Login

- For Gen8 and Gen9 servers: AMS (iLO Agentless Management Service) v10.6.0 or later for Windows or AMS v2.5.2 or later for Linux running on the managed servers
- For Gen10 servers: AMS v1.1.0 or later for Windows and AMS v1.0.0 or later for Linux

Procedure

1. Click **Reports** on the left navigation menu.
2. Click **Hardware Inventory Report**.

   The following information for each server appears:

   - iLO IP Address—The network IP address of the iLO subsystem.
   - iLO HostName—The fully qualified network name assigned to the iLO subsystem.
   - Product ID—The product with which the iLO processor is integrated.
   - Server HostName—The server name defined by the host operating system.
   - Serial number—The server serial number, which is assigned when the system is manufactured.
   - Processor inventory
     - Processor Name
     - Processor Status
     - Number of Processors
     - Number of Cores
   - Memory inventory
     - Total Memory
     - Number of DIMMs
     - Memory Status
   - Power inventory
     - Number of Fans
     - Number of Power Supplies

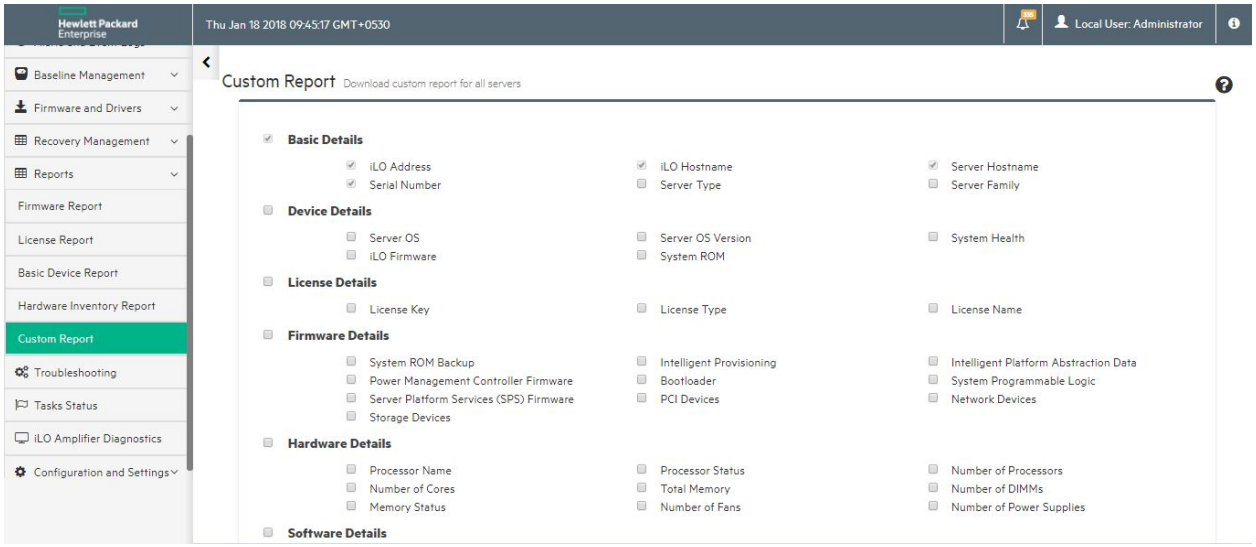
3. Options on this page:

   - Enter a value in the **Search** box and hit the enter key to search for specific information.
   - Use the **Servers, iLO Federation Groups or Server Groups** filter to customize the display.
   - Use the **Show entries** menu to choose the number of entries to display per page.

- Use the navigation buttons to view the first, previous, next, or last page of the list. You can also click a specific page number to jump to that page.
- Click **Export to CSV** to download the report in .csv format.

Viewing the Custom Report

Custom Report allows users to customize the reports and download them. The various fields in the Firmware Report, Basic Device Report, Hardware Inventory Report, and other fields are shown. The user can select which fields will be shown in the report.



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login

Procedure

1. Click **Reports** from the left navigation menu.
2. Click **Custom Report**.

   The following information appears:

   - Basic Details

     Select one or more options from the basic details to download the customized report. For more information, refer **Basic report details**.
   - Device Details

Select one or more options from the device details to download the customized report. For more information, refer **Device report details**.

- License Details

  Select one or more options from the license details to download the customized report. For more information, refer **iLO license report details**.

- Firmware Details

  Select one or more options from the firmware details to download the customized report. For more information, refer **Firmware report details**.

- Hardware Details

  Select one or more options from the hardware details to download the customized report. For more information, refer **Hardware inventory report details**.

- Software Details

  Select the software details check box to download the customized report.

Server troubleshooting

Downloading the server Active Health System log

To assist in troubleshooting server issues, you can download a server's AHS (Active Health System) log and send it to HPE for analysis.

For more information, see the documentation for the AHSV (Active Health System Viewer) at **www.hpe.com/support/ahsv-docs**.

Procedure

1. Click **Troubleshooting** from the left navigational menu.
2. Select the server for which you want to collect AHS data.
3. Click **Support Actions**, and then click **Download AHS logs**.
4. Enter the date range for the data you want to collect.
5. Select **Removable Storage** or **Network Share (NFS)** from the **Storage Type** menu.
6. Select a mounted USB if available.
7. Specify the folder path to use.
8. Click **Apply** to download the log file or click **Close** to cancel.

Logging in to Active Health System Viewer

Procedure

1. To access the AHSV webpage, go to **http://www.hpe.com/servers/ahsv** in a supported browser. Supported browsers include:
   - Internet Explorer 11
   - Chrome v51 or later
   - Firefox v46 or later
2. Enter your **User ID** (email address) and **Password**, and then click **Sign In**.

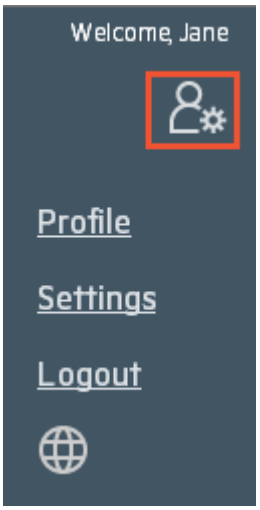
NOTE: To log in using an HPE Passport account, or to create an HPE Passport account, go to **http://www.hpe.com/info/insightonline**. In most cases, your HPE Passport account is the same as the email address you used during the HPE Passport account registration process. If you changed your user ID in the Hewlett Packard Enterprise Support Center, be sure to log in with your user ID and not your email address.

NOTE: To have the system remember your log in credentials, select **Remember Me** before clicking **Sign In**.

Logging out of AHSV

Procedure

1. To log out of AHSV, click the user settings menu.

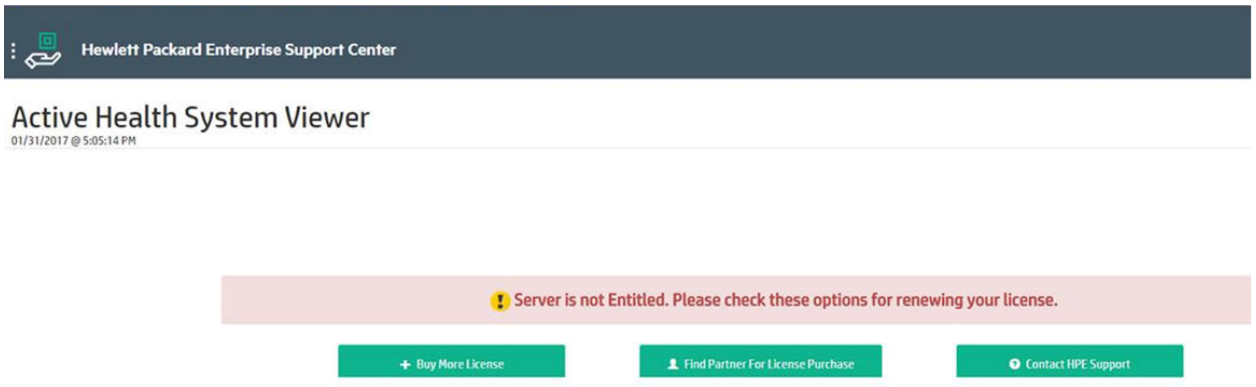


2. Click **Logout**. You will be logged off and the log in page is displayed.

Loading an AHS log file

IMPORTANT: The server that the AHS log was created from, must have a valid warranty. If the server is out of warranty, an error message is displayed, stating "`Server is not Entitled. Please check these options for renewing your license.`" The options include:

- Buy More Licenses
- Find Partner for License Purchase
- Contact HPE Support



- To load an AHS log file through AHSV, select **Upload AHS Log**. Navigate to your log file and click **Open.**

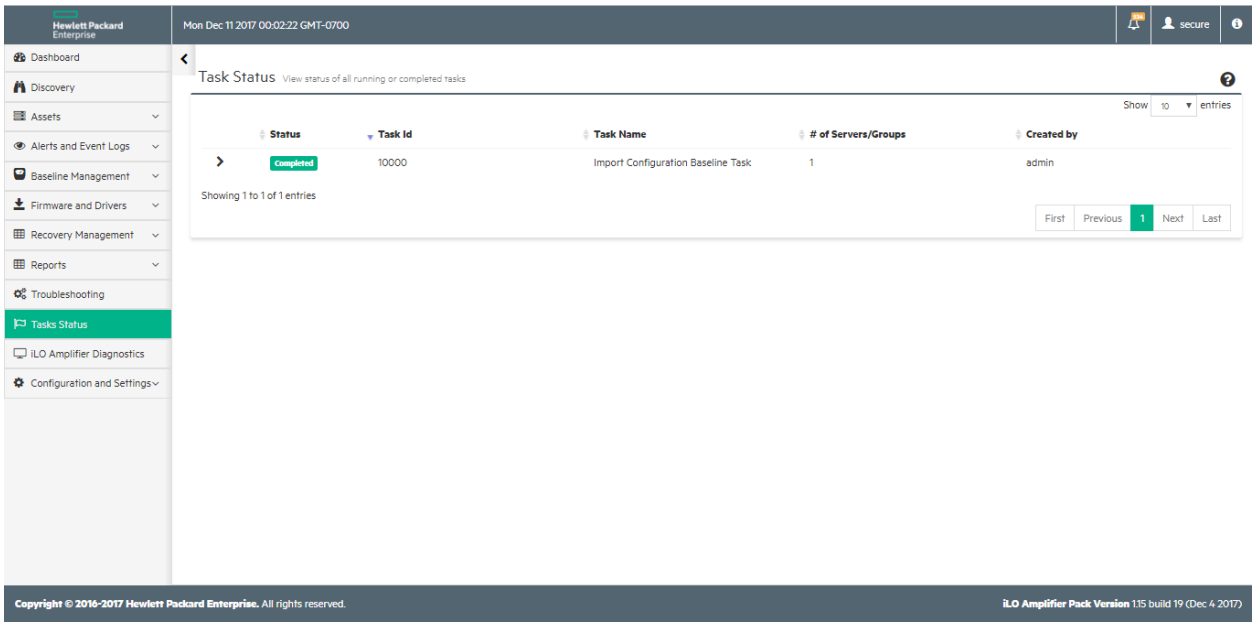
NOTE: Maximum file size limit is 250 MB. For logs greater that 250 MB, contact the HPE Support Center.

- A window is displayed that shows parsing and log loading states. To cancel the load process, click **Cancel**.
- This window also displays videos for different platforms. You can search and play different videos while you are waiting for the log file to load.
- As the AHS log loads, the screen displays the estimated time of completion.
- Search for an existing AHS log.
  - Under **Search AHS viewer for uploaded AHS log**, enter the AHS log name or System Serial Number, and then click the search icon.
  - Click the log file that you want to open.
- To view a previously loaded an AHS log file, select the log file from the table.

Viewing task status

You can view and abort any task from the **Tasks Status** page.

NOTE: Some tasks cannot be aborted after a certain stage.



Procedure

1. Click **Tasks Status** on the left navigation menu.

   The following information appears:

   - **Status**—Any of the following states can appear:
     - **Running**—The task is executing.
     - **Pending**—The task is pending and has not started.

       The **Pending** status can occur for several different reasons, such as too many tasks running at one time. iLO Amplifier Pack allows only a predetermined number of each type of task to run at one time. Another reason could be that some other task is already running on one of the selected servers. In both of these cases, the task will be scheduled automatically once the conflicting task finishes.
     - **Completed with exception**—The task has at least one failed server.
     - **Completed**—The task has completed successfully.
     - **Killed**—The task was aborted by the user.

- **Exception**—The task has stopped due to an exception condition. The reason for the failure appears in the **Message** field.
- **Waiting**—The task is waiting for user action. This status appears only during an online update. The task requires the user to make a choice before it can continue.

- **Task ID**—Task IDs are not always sequential. This is a normal behavior.
- **Task Name**
- **# of servers/groups**
- **Created by**—Logged in user.

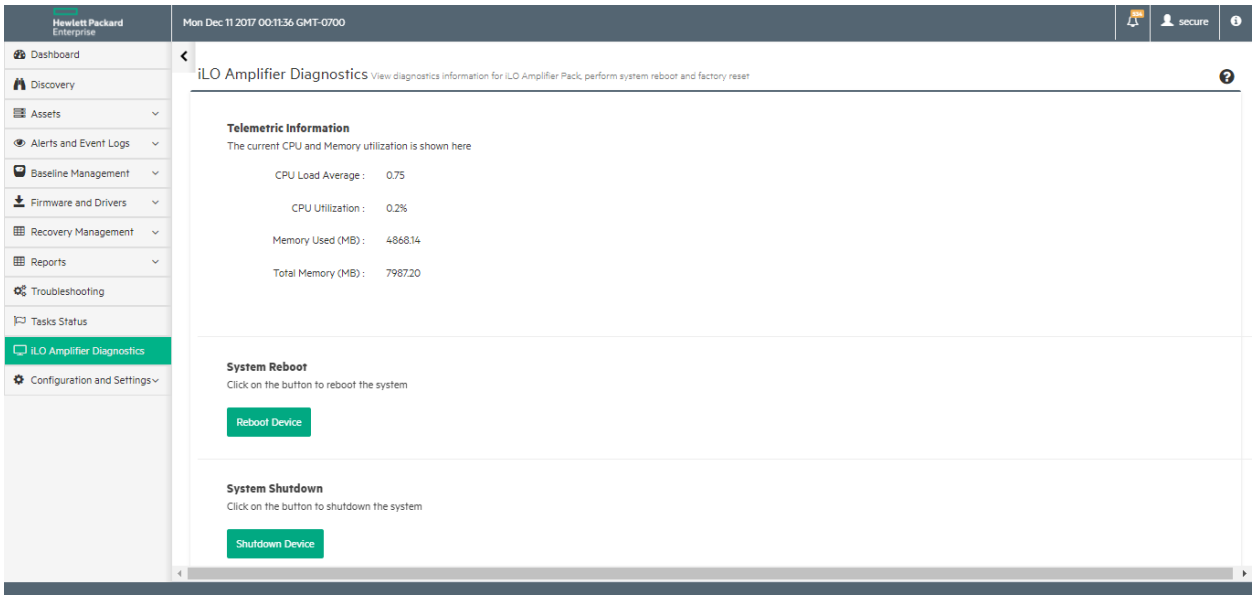
2. Click the right arrow to reveal the task status details.
   - **Task Progress**—Percentage of task completed
   - **Activity**—List of tasks
     - **iLO/Host Name**—iLO, Host Name, or Federation Group Name
     - **Task Name**
     - **Message**—Information about the success or failure of the task
     - **Progress**
   - **Last updated**—Date, time, and time zone of last task update
   - **Created**—Date, time, and time zone of task creation
3. Optional: If a task is in the **Running** state, you can click **Abort** to cancel the task.

   If a task is in the **Completed**, **Exception**, or **Killed** state, you can click **Rerun Task** to run the task again.

   NOTE: Some tasks cannot be rerun, such as the online update task. The tasks that are created using the server **Actions** menu from the server list can be rerun.
4. Click **Close** to close the task details.

iLO Amplifier Diagnostics

Use the **iLO Amplifier Diagnostics** page to view diagnostic information about iLO Amplifier Pack and to perform a system reboot, shutdown, or factory reset. Access to support logs is also available on this page.



- **Telemetric information**—Current CPU and memory utilization information:
  - CPU Load Average
  - CPU Utilization
  - Memory Used
  - Total Memory
- **System Reboot**—Click **Reboot Device** to stop all activities and restart the appliance.
- **System Shutdown**—Click to shut down the appliance.
- **Factory Reset**—Perform a factory reset by selecting one of the following options from the **Factory Reset Type** menu, and then clicking **Factory Reset**.

  NOTE: Factory reset will erase all configuration from iLO Amplifier Pack, based on the factory reset type selected.

  - **Managed Systems Configuration**—Erases only the configuration related to the servers and groups managed in iLO Amplifier Pack.
  - **All Configuration**—Erase both the configuration of the managed servers and the configuration of the iLO Amplifier Pack.

  iLO Amplifier Pack reboots after a factory reset.
- **Support Logs**—Click **Download Support Logs** to download the support logs.

Configuring the iLO Amplifier Pack appliance

System Update

Upgrading the appliance firmware

NOTE: To upgrade iLO Amplifier Pack from version 1.0x to version 1.10 or later, you must redeploy the appliance. The configuration can be restored from version 1.0x to version 1.10 or later.

HPE recommends backing up your current configuration before upgrading so that you can restore the configuration of the earlier version.

Prerequisites

- iLO Amplifier Pack user with either of the following privileges:
  - Configure Manager
  - Configure Manager with Security

Procedure

NOTE: Use the following procedure to upgrade iLO Amplifier Pack from v1.10 to v1.15 or later releases.

1. Download and save **`iLOAmpPack_1.30_Binary.zip`** and its corresponding checksum file.

   NOTE: Use an appropriate checksum verification tool to verify the integrity of the downloaded files.

2. Extract **`iLOAmplifierPack.bin`** from the zip file.
3. Save the firmware upgrade file to a removable storage device, network share, HTTP share, or your client computer.
4. Click **Configuration and Settings** from the left navigation menu, and then click **System Update**.
5. Select the storage type that corresponds to the location where you saved the firmware upgrade file.
6. Depending on the storage type you selected, do one of the following:
   - For removable storage (USB), select the mounted device or enter the file path in the format `/folder/filename`.
   - For a network share, enter a file path in the format `/folder/filename`, an IPv4 or IPv6 address, and the network storage path.
   - For an HTTP file share, enter the URL for the firmware upgrade file.
   - For a file upload, click **Browse**, and then navigate to the firmware upgrade file on the client computer.
7. Click **Update**.

   The system will reboot after the update is finished.

NOTE: The IP address of the appliance might change after reboot if iLO Amplifier Pack is configured with DHCP.

8. Clear the browser cache.

NOTE:

- The update will fail if tasks are still running.
- Keep the initial registration email for use with future updates.

Appliance firmware upgrade storage types

Choose from the following methods when you upgrade the iLO Amplifier Pack firmware:

- **Removable Storage (USB)**—Upgrade the firmware from a file saved on a removable storage device.
- **Network Share (NFS)**—Upgrade the firmware from a file saved on a shared network device.
- **HTTP/HTTPS Share**—Upgrade the firmware from a file saved on an HTTP/HTTPS file share.
- **File Upload**—Upgrade the firmware from a file saved on the client computer.

Performance settings

Modifying the refresh settings

You can set the refresh settings for iLO Amplifier Pack to wait between inventory processes either automatically or manually.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

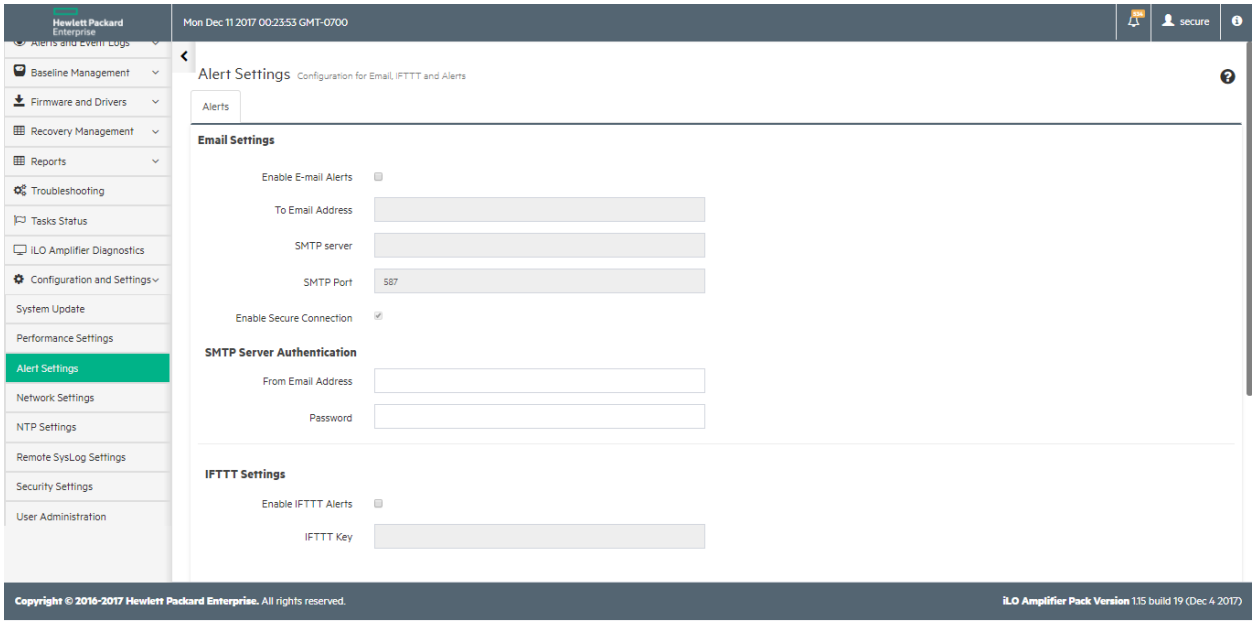
Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **Performance Settings**.
2. Select one of the following:
   a. To have iLO Amplifier Pack automatically refresh server inventory, click to select the **Enable Auto Refresh** check box.
   b. To specify the refresh interval time, select a number from the **Refresh Interval (in hours)** menu.
3. Click **Save**.

When Auto Refresh is selected, iLO Amplifier Pack continuously refreshes the inventory. Servers that have been refreshed within the past hour will not be inventoried again.

iLO Amplifier Pack waits for the selected period of refresh interval time (in hours) and then starts the inventory process for all the added servers.

Configuring alert settings



Prerequisites

- One of the following user privileges:
  - Configure Manager with Security
  - Configure Manager
- iLO Advanced License on the managed server
- An IFTTT account for IFTTT alerts
- Mail server details and an email address for email alerts.
- Proxy set up on the **Network Settings** page if your Internet connection uses a proxy

Procedure

1. Click **Configuration and Settings**, and then click **Alert Settings**.
2. Optional: Configure email alerts.
   a. In the **Email Settings** section, select the **Enable Email Alerts** check box.
   b. Enter the email address to which you want the alerts sent. You can enter multiple email addresses by separating them with a semicolon.
   c. Add the SMTP server information in the following format: **`smtp.gmail.com`**.
   d. Provide the outgoing server port number.
   e. To enable authentication, click the **Enable Secure Connection** check box, and then enter the username and password for the email account that will send the alerts.
3. Optional: Configure IFTTT alerts

a. In the **IFTTT Settings** section, select the **Enable IFTTT Alerts** check box.

b. Enter the **IFTTT** key.

NOTE: For information about setting up an IFTTT account, see **Setting up an IFTTT alert**.

---

4. Select the alert categories and severities for which you want to receive emails.

   Click **All Alerts** to receive emails for all alert categories and severities or click any combination of the following to designate for which alerts the appliance will send an email.

   - **Alert Category**
     - Security
     - Hardware Failure
     - General Failure
     - Storage
     - Maintenance
     - Administration
     - Other
   - **Alert Severity**
     - Critical
     - Warning
     - Info

5. Optional. If you want to receive alerts from the iLO Amplifier Pack appliance, select the **Enable Activity Alerts** check box.
6. Optional. Click **Send Test Alert** to test the alert configuration.
7. Click **Save** to save your settings.

Sending a test alert

Procedure

1. Click **Configuration and Settings**, and then click **Alert Settings**.
2. Click **Send Test Alert.**

   This will send an email or IFTTT event, whichever is configured.

Setting up an IFTTT alert

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager

Procedure

1. Create an account on the **www.ifttt.com** website and sign in.
2. In the search box, search for **`webhooks`**.
3. Click on the **Services** tab and then click the **webhooks** icon
4. Click **Connect**, and then click **Settings**.
5. Copy the URL into another tab in the browser, and then go to that page to get your key.
6. Copy the key and save it in Notepad.
7. Go back to the profile page and click **New Applet** on the top right corner of the page.
8. Click the word **this**, and then search for **`Webhooks`**.
9. Click **Webhooks**, and then click **Receive a web request**.
10. Enter **`HPEServerAlert`** as the event name, and then click **Create Trigger**.
11. Click the word **that**, and then click the **Email** icon.
12. Click **Send me an email** on the **Choose action** page.
13. Review the action fields, and then click **Create action**.
14. Click **Finish** on the **Review and finish** page to complete the alert.
15. Open iLO Amplifier Pack, click **Configuration and Settings**, and then click **Alert Settings**.
16. Enter the key in the **IFTTT** field.

IFTTT alert syntax

Use the following syntax for the types of alerts you want to receive.

Email, Twitter, Facebook, and other social networking sites

Subject line (email only)

```
HPE server alert
```

Body

```
What: {{EventName}}<br>
When: {{OccurredAt}}<br><br><br>
Category: {{Value1}}<br>
Summary: {{Value2}}<br>
Action: {{Value3}}
```

SMS

Body

```
{{EventName}}<br>
When: {{OccurredAt}}<br>
```

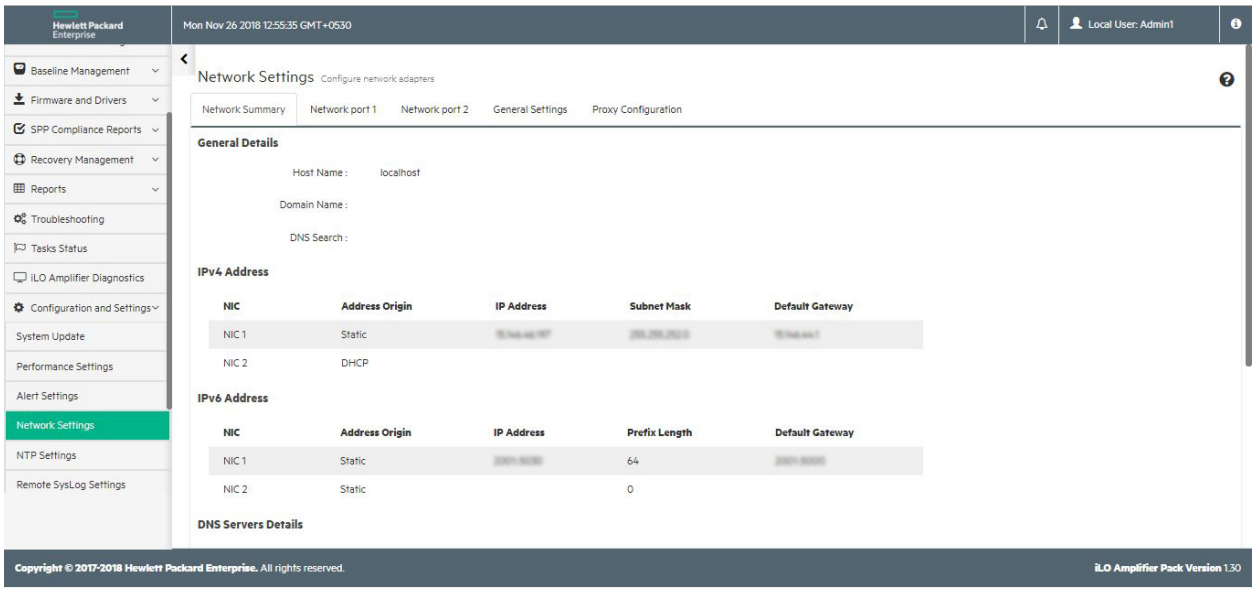
```
Category: {{Value1}}<br>
Action: {{Value3}}
```

Configuring network settings

Use the settings on the following tabs to configure the network settings for the iLO Amplifier Pack.

- Network Summary
- Network port 1
- Network port 2
- General Settings
- Proxy Configuration

The results are displayed on the **Network Summary** tab.



Configuring the network ports

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Network Settings**.
2. Select the **Network Port 1** or **Network Port 2** tab.
3. Click the check boxes to enable NIC, DHCPv4, or DHCPv6 if required.
4. Do one of the following or both if DHCP is not configured:

- Enter information into the **Static IPv4 Address** section:
  - IP address
  - Subnet mask
  - Default gateway
- Enter information into the **Static IPv6 Address** section:
  - IP address
  - Default gateway
  - Prefix Length

5. Click **Save** to save your settings.
6. Click **Reboot** to restart the system.

NOTE: If the appliance is configured with DHCP, the appliance IP address might change after you restart the system.

Configuring general network settings

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Network Settings**.
2. Click the **General Settings** tab and provide the following information in the **General Settings** section:
   - **Host Name**
   - **Domain Name**
   - **DNS Search**
3. Optional: In the **Manually configured IPv4 DNS Servers** or **Manually configured IPv6 DNS Servers** section, enter the DNS IP address for up to two servers.
4. Optional: In the **DHCP Settings** section, click the check boxes to enable the appropriate DHCPv4 or DHCPv6 settings:
   - DHCPv4 settings:

- **Use DHCPv4 Supplied DNS Servers**
- **Use DHCPv4 Supplied Domain Name**
- **Use DHCPv4 Supplied Gateway**

- DHCPv6 settings:
  - **Use DHCPv6 Supplied DNS Servers**
  - **Use DHCPv6 Supplied Domain Name**
  - **Use DHCPv6 Supplied Gateway**

5. In the **Management Network Port** section, select **Network Port 1** or **Network Port 2**.
6. Click **Save** to save your settings. Click **Reboot** to restart the system.

Configuring proxy settings

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Network Settings**.
2. Click the **Proxy Configuration** tab.
3. Click to select the **Enable Proxy** check box.
4. Enter the **Proxy Servername** in the following format: **`<proxy server>`**.
5. Enter the **Port number**.
6. Optional: Click to select the **Enable Secure Proxy Connection** check box.
7. Click **Save** to save your settings. Click **Reboot** to restart the system.

Configuring time and NTP settings

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Time and NTP Settings**.
2. Select a time zone from the menu.
3. To use NTP settings, select the **Use NTP** check box, and then enter the **Primary** and **Secondary Server Address**.
4. Click **Save** to save your settings.

Configuring Remote SysLog Settings for iLO Amplifier Pack

Use this page to configure the SysLog settings for iLO Amplifier Pack. Remote SysLog settings for individual servers can also use the settings on this page or can be configured to send server SysLog files to a different location. For more information, see **Configuring remote syslog** and **Configuring remote SysLog for grouped servers**.

Prerequisites

- User privileges
  - Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Remote SysLog Settings**.
2. Click to select the **SysLog Enabled** check box.
3. Enter the **SysLog Port** number.
4. Enter the IPv4 or IPv6 address and host name for up to two servers in the **SysLog Server1** and **SysLog Server2** fields.
5. Click **Send test SysLog** to validate the server settings.
6. Click **Save**.

Configuring security settings

Configuring access settings

Prerequisites

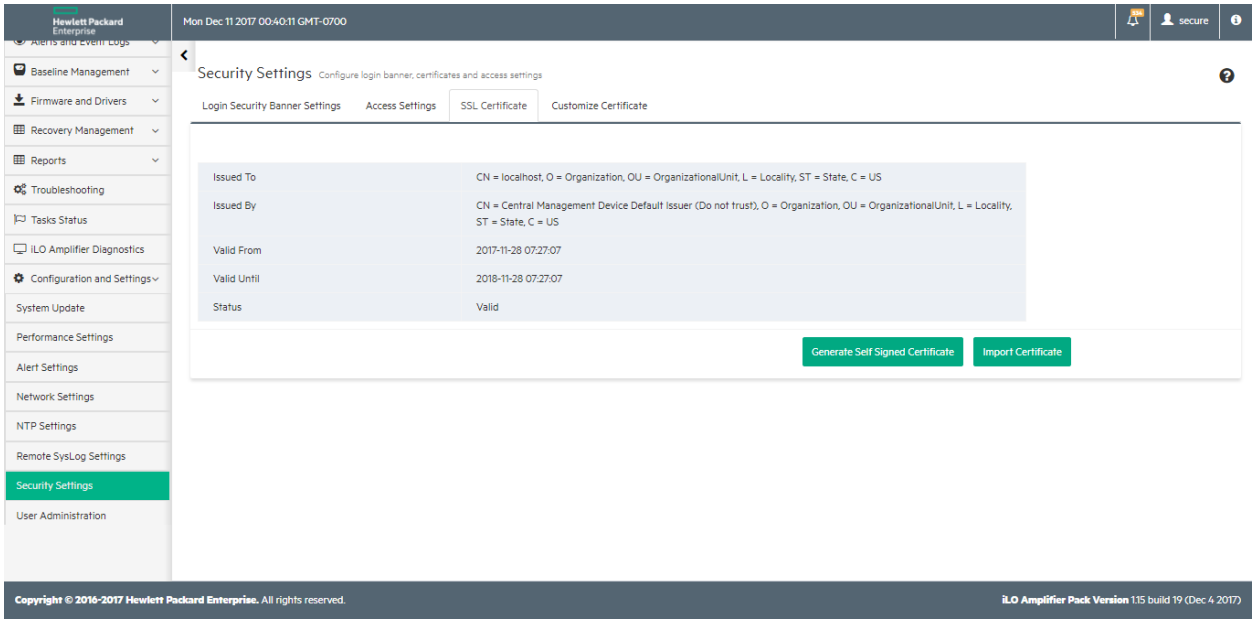
- User privileges

- Configure Manager with Security
- Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigational menu, click **Security Settings**, and then click the **Access Settings** tab.
2. Set the minimum password length in the **Min Password Length** field.
3. Select the time-out period from the **Session Idle Time Out (Min)** menu.
4. Click **Save** to save your settings.

Obtaining and importing an SSL certificate



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** from the left navigation menu, click **Security Settings**, and then click the **SSL Certificate** tab.
2. Perform one of the following:

- Click **Generate Self Signed Certificate**
- Click **Import Certificate**, paste the base64-encoded X.509 Certificate in the field provided, and then click **Import**.

Generating a certificate signing request

Use this page to create a CSR (Certificate Signing Request) that you can send to a Certificate Authority to obtain a trusted SSL certificate.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** from the left navigation menu, click **Security Settings**, and then click the **Customize Certificate** tab.
2. Select **Generate CSR**.
3. Provide the following information:
   - Country
   - State
   - City or Locality
   - Organization Name
   - Organizational Unit
   - Common Name
4. Click **Generate CSR**.

Configuring LDAP

LDAP is a lightweight client/server protocol for accessing directory services that provides information about users, systems, networks, services, and applications in the network. LDAP is used as a centralized repository for authentication purposes. With this version of iLO Amplifier Pack, you can configure iLO Amplifier to authenticate users using the LDAP directory services. iLO Amplifier communicates using secure protocol to the LDAP servers. Users must be part of groups in an LDAP directory. The groups can be configured in iLO Amplifier and privileges can be associated to the groups. A user logged in to iLO Amplifier, will have the privilege associated to the group.

Login LDAP using the following formats:

1. Domain\Log-on name format (for example, asia\testuser).
2. Email ID (for example, Username: **jon.doe@domain.com**).
3. Distinguished name of the user (for example, CN=jon_doe,DC=Domain,DC=com).

NOTE: Although there can be multiple Active Directory servers and domains in the data center, iLO Amplifier can configure only one Active Directory server. However, iLO amplifier allows authentication for groups and users that are part of the same domain in the Active Directory server which is configured in iLO amp. Groups and users configured on different servers will not work.

Example:

Suppose **`Username1`** and **`Username2`** belong to Domain 1 while **`Username3`** belongs to Domain 2. iLO Amplifier will only allow **`Username1`** and **`Username2`** to log in to Domain 1. Unlike Microsoft Active Directory, **`Username3`** will not be able to log in to Domain 1 since **`Username3`** is part of a different server (Domain 2).

Configuring Directory Server Settings

Use this page to configure the Directory Server Settings.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

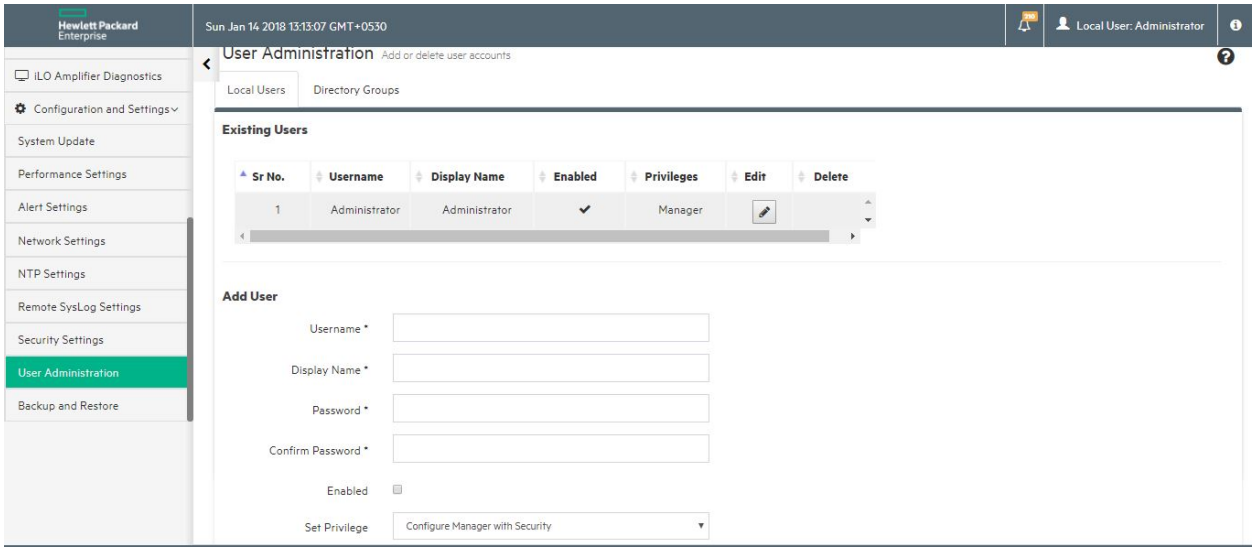
1. Click **Configuration and Settings** from the left navigation menu, click **Security Settings**, and then click the **Directory** tab.
2. To enable the directory server settings, select the **Enabled** check box.
3. Select the **Active Directory** from the **Directory Type** field.
4. Enter the base distinguished name in the **Base DN** field.

   Base DN format (for example, OU=My_OU,DC=Domain,DC=COM).

   NOTE: To avoid LDAP timeout, users are advised to use a more specific base DN value. For example, instead of using "DC=domain,DC=com", use specific values such as "CN=path1,DC=domain,DC=com" or "OU=path2,DC=domain,DC=com" or "CN=path1,OU=path2,DC=domain,DC=com" (assuming the users are present in this specified path).
5. Enter the IPv4 or IPv6 address or FQDN in the **Directory Server Address** field.
6. Select the port number from the **Directory Server Port** field.
7. To enable the iLO Amplifier Pack communication with LDAP server using secure protocols, select the **Use secure communication** check box.
8. Click **Save**.

Managing iLO Amplifier Pack user accounts

Use the options on the **User Administration** tabs to manage user/group privileges.



Local users

Adding a user account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Configuration and Settings** in the left navigation menu, and then click **User Administration**.

   The **Local Users** tab opens by default.

2. Enter the **User Name**.

   This value is the name that you use when logging in to iLO Amplifier Pack. The maximum length for a user name is 32 characters. The **User Name** must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each display name.

3. Enter the **Display Name**.

   This value is the name that is displayed after you log in. The **Display Name** does not have to be the same as the **User Name**. The maximum length for a display name is 32 characters. The display name must use printable characters.

4. Use **Password** and **Password Confirm** to set the password that the user will use to log in to the appliance.

Password minimum length must conform to the setting on the **Access Settings** page. The maximum password length is 39 characters.

5. Select the **Enabled** check box to enable the user login.
6. Set the privilege level for this user.
   - **Configure Manager with Security**—Allows all operations including recovery management.
   - **Configure Manager**—Allows all operations except recovery management.
   - **Configure User**—Allows configuring users with device privileges
   - **Configure Devices**—Allows configuring and performing actions on devices and login privileges.
   - **Login**—Allows report generating and read operations, such as viewing discovered servers and groups.
7. Click **Save**.

Editing a user account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users
  - Configure Devices

Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **User Administration**.

   The **Local Users** tab opens by default.
2. Click  for the user you want to edit.
3. Click **Save**.

Disabling a user account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure Users
- Configure Devices

Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **User Administration**.

   The **Local Users** tab opens by default.
2. Click  for the user you want to disable.
3. Clear the **Enabled** check box, and then click **Save**.

Deleting a user account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices

Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **User Administration**.

   The **Local Users** tab opens by default.
2. Click  for the user you want to delete, and then click **Ok** to confirm the deletion.
3. Click **Save**.

iLO Amplifier Pack user privileges

iLO Amplifier Pack user accounts can have the following privileges:

- **Configure Manager with Security**—Allows a user to perform all iLO Amplifier Tasks, including Recovery Management.
- **Configure Manager**—Allows a user to perform all iLO Amplifier Pack tasks, except for Recovery Management.
- **Configure User**—Allows a user to configure user accounts. This privilege includes the **Configure Devices** and **Login** privileges.
- **Configure Devices**—Allows a user to configure and perform tasks on devices. This privilege includes the **Login** privilege.
- **Login**—Allows a user to log in to iLO Amplifier Pack with read-only access.

Directory groups

Adding a group account

Prerequisites
User privileges

- Configure Manager with Security
- Configure Manager
- Configure User

Procedure

1. Click **Configuration and Settings** from the left navigation menu, click **User Administration**, and then click the **Directory Groups** tab.
2. Enter the group name in the **Group** field.

   The maximum length allowed for a group is 255 characters. The group name must contain a group name and a domain component name. For example, CN=group name, DC=domain, DC=com.
3. Set the privilege level for this group.

   - **Configure Manager with Security**—Allows all operations including recovery management.
   - **Configure Manager**—Allows all operations except recovery management.
   - **Configure User**—Allows a user to configure user accounts. This privilege includes the **Configure Devices** and **Login** privileges.

     Devices and Login privileges:
   - **Configure Devices**—Allows configuring and performing actions on devices and login privileges.
   - **Login**—Allows report generating and read operations, such as viewing discovered servers and groups.
4. Select the **Enabled** check box to enable the group account.
5. Click **Save**.

Editing a group account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users

Only configure user and above privileges is allowed.

Procedure

1. Click **Configuration and Settings** on the left navigational menu, click **User Administration**, and then click the **Directory Groups** tab.
2. Click  for the group you want to edit.
3. Click **Save**.

Disabling a group account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Users Login

Only "Configure User" privileges and above is allowed.

Procedure

1. Click **Configuration and Settings** on the left navigational menu, click **User Administration**, and then click the **Directory Groups** tab.
2. Click  for the group you want to disable.
3. Clear the **Enabled** check box, and then click **Save**.

Deleting a group account

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User Login

Only Configure User and above privileges are allowed.

Procedure

1. Click **Configuration and Settings** from the left navigation menu, click **User Administration**, and then click the **Directory Groups** tab.
2. Click  for the group you want to delete, and then click **Ok** to confirm the deletion.
3. Click **Save**.

iLO Amplifier Pack group privileges

iLO Amplifier Pack user accounts can have the following privileges:

- **Configure Manager with Security**—Allows a group to perform all iLO Amplifier Tasks, including Recovery Management.
- **Configure Manager**—Allows a group to perform all iLO Amplifier Pack tasks, except for Recovery Management.
- **Configure User**—Allows a group to configure user accounts. This privilege includes the **Configure Devices** and **Login** privileges.
- **Configure Devices**—Allows a group to configure and perform tasks on devices. This privilege includes the **Login** privilege.
- **Login**—Allows a user to log in to iLO Amplifier Pack with read-only access.

Backup and Restore

Backing up the iLO Amplifier Pack configuration

NOTE: Imported baseline images will not be backed up and cannot be restored.

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Click **Configuration and Settings** on the left navigation menu, and then click **Backup and restore**.

   The **Backup** tab opens by default.
2. In the **File settings and security** section, enter the following information:
   - **Storage Type**—select **NFS Share** or **USB Share**.
   - **Destination File Path**
   - **Backup File Passphrase**—used to encrypt the configuration data; required to restore from this file
   - **Confirm Passphrase**
3. In the **Network Settings** section for NFS Share option, enter the following information:
   - **IPv4 or IPv6 Address**
   - **Network Storage Path**

     NOTE: For USB, select the connected USB and specify the folder in which to save the backup.
4. Click **Backup Now** to start backup process.

Restoring the iLO Amplifier Pack configuration

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

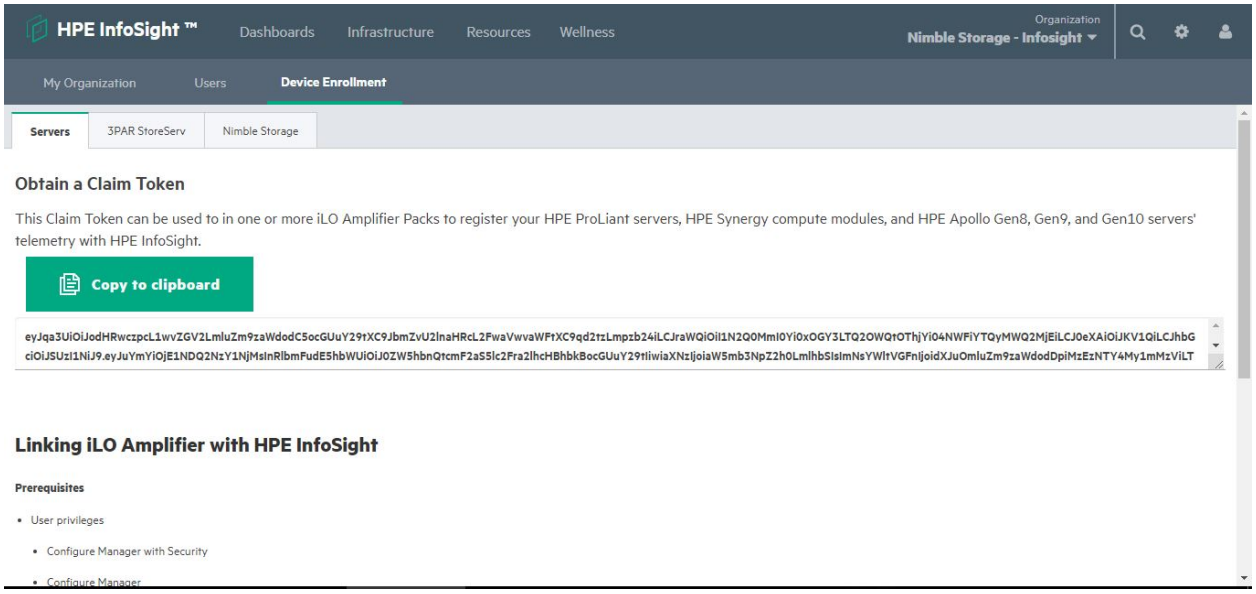
1. Click **Configuration and Settings** on the left navigation menu, and then click **Backup and Restore**.
2. Click the **Restore** tab.
3. In the **File settings and security** section, enter the following information:
   - **Storage Type**—select **NFS Share** or **USB Share**.
   - **File Path**
   - **Backup File Passphrase**
4. For the NFS Share option, enter the following information in the **Network Settings** section:
   - **IPv4 or IPv6 Address**
   - **Network Storage Path**
5. HPE recommends that you turn off the old amplifier during restoration to avoid IP conflicts. You can power the amplifier back on after the Restoration process is completed.
6. Click **Restore** to begin the restoration process.
7. During the restoration, the new amplifier changes its IP address to the same IP address as the old amplifier. To avoid IP conflicts, you must manually change the IP address on the new amplifier.

HPE InfoSight

HPE InfoSight is an artificial intelligence (AI) platform that eliminates the pain of managing infrastructure. HPE InfoSight employs cloud-based machine learning to predict and prevent problems across the infrastructure stack and ensures optimal performance and efficient resource use. For more details, see the *HPE InfoSight for Servers User Guide*.

NOTE: HPE recommends using iLO 5 version 1.37 or above for HPE InfoSight.

Obtaining a claim token



To send AHS and heartbeat information to HPE InfoSight, a claim token must be created in HPE InfoSight and provided to iLO Amplifier Pack. Once the claim token has been entered and validated, data is sent automatically to HPE InfoSight for all monitored servers.

NOTE: Claim tokens are good for a brief time, long enough to copy and paste claim token into iLO Amplifier, but not long enough to save the token to use at a later time.

A new claim token needs to be generated for registration when:

- You need to link iLO Amplifier Pack with HPE InfoSight.
- You have several instances of iLO Amplifier Pack in a single location or at multiple locations.
- You receive an error that your claim token is no longer valid.

Prerequisites

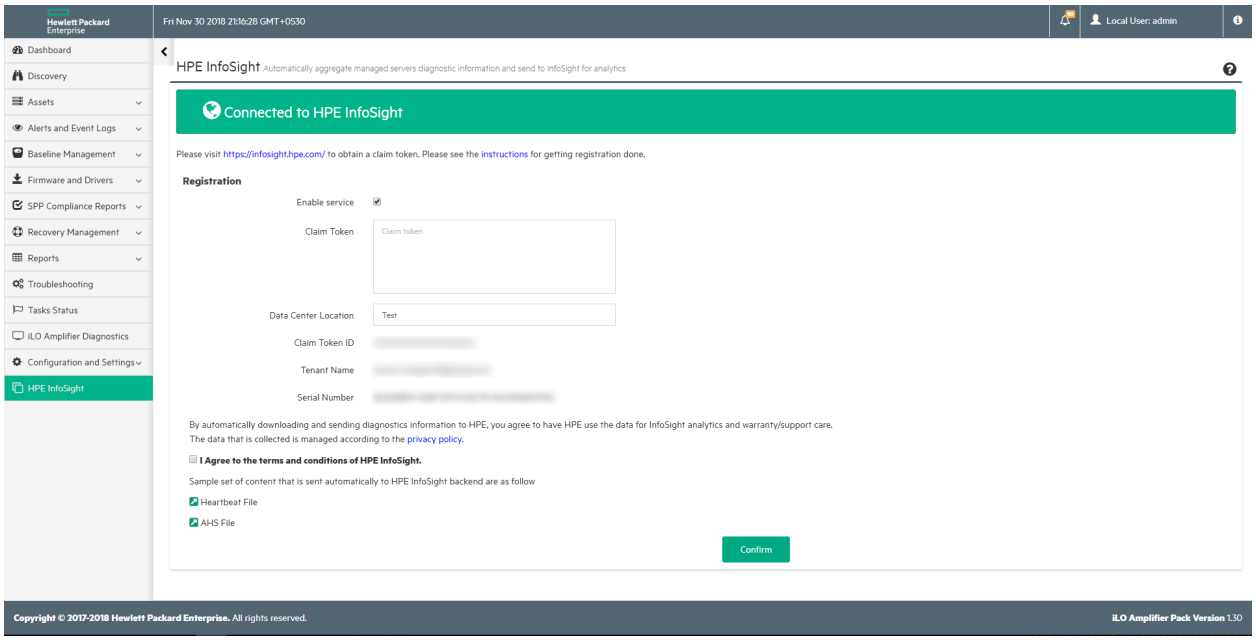
HPE Passport Login credentials

Procedure

1. Go to the HPE InfoSight login webpage at **https://infosight.hpe.com/app/login**.
2. Login with your HPE Passport Login credentials.

3. Acknowledge the message bulletins and terms of use.
4. The dashboard is displayed. Click the gear icon and then select **Device enrollment**.
5. Ensure that you are in the **Servers** tab. The claim token is generated and displayed on the page. To link it successfully with HPE InfoSight, copy this token and enter it in the **HPE InfoSight** settings page in iLO Amplifier Pack.

Linking iLO Amplifier Pack with HPE InfoSight



Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
- DNS configuration
- Proxy settings if required. See **Configuring network settings** for more details.

Procedure

1. Click **HPE InfoSight** on the left navigation menu.
2. Select the **Enable service** check box to activate the **Claim Token** and **Data Center Location** entry fields.
3. Enter the **claim token** generated on the HPE InfoSight website.
4. Enter your data center location.
5. Read and accept the terms of use about the diagnostic information that will be sent back to HPE.
6. Optional: Click the links to know more about the sample **Heartbeat File** and **AHS file** that will be sent to HPE.

NOTE: The maximum file size limit for AHS logs is 250 MB. For logs greater than 250 MB, contact the HPE Support Center.

7. Click the **Confirm** button to link iLO Amplifier Pack with HPE InfoSight.
8. The HPE InfoSight connection status is shown in a message at the top of the page. On successful linking, the following details are displayed on the page:
   - **Claim Token ID**
   - **Tenant Name**
   - **Serial number**
9. If at any time, you would like to unlink iLO Amplifier Pack from HPE InfoSight, clear the **Enable service** check box, and then click **Confirm**.

iLO Amplifier Pack troubleshooting

Report information does not sort

Symptom

Information on the **Reports** page is not sorted.

Cause

Intermittent GUI Issue.

Action

Refresh the page, and then try sorting again.

Discovery fails on CSV file upload

Symptom

The process of server discovery fails when using a CSV file to upload the server information.

Cause

The CSV file contains blank cell in the IP or username field.

Action

Upload the CSV file within the defined format and make sure that no fields are left empty.

SSH session does not close

Symptom

An SSH session does not close when a user account configuration is modified.

Cause

Session timeout does not close the SSH sessions.

Action

Close the SSH session manually, and then log in again.

Alert notification not visible

Symptom

The alert bell notification menu is not seen.

Cause

Intermittent GUI issue.

Action

1. Do either of the following:

   - Refresh the browser.
   - From the left navigation menu, click **Alerts and Events Logs**, and then click **Server Alert Viewer** to see alerts.

SUT components not downgraded during online update

Symptom

SUT does not support a downgrade for version 2.0.1. If the install set contains SUT components for downgrade in iLO Amplifier Pack, SUT ignores the component.

Cause

SUT does not support downgrade for version 2.0.1

Action

Do not use iLO Amplifier Pack to downgrade SUT v2.0.1 components.

Failure message appears when a task is created

Symptom

Failure error message is displayed when task is created by selecting 600+ servers.

Cause

Selecting 600 or more servers during task creation can result in a failure message, even if task creation is successful.

Action

To check that task was created or has failed, see **Task Status** page

Loading and exporting activity alerts and logs to CSV causes unresponsive GUI

Symptom

The GUI might not respond when a user navigates to the **Activity Alerts and Logs** page with more than 70,000 records.

Cause

Loading of large data from the backend might cause GUI to not respond for some time.

Action

Wait until the loading of activity alerts and logs is complete.

Firmware configuration settings may not be recovered for S100i Smart Array controller

Symptom

Firmware configuration settings, including logical drive configuration for the S100i Smart Array controller, may not be recovered during an automatic or manual server system restore.

Cause

S100i Smart Array controller configuration settings are not correctly provided/recovered by the providers.

Action

If applying the firmware configuration fails on the S100i Smart Array controller, configure the settings manually on the controller.

Importing a custom SPP Firmware Baseline to iLO Amplifier Pack fails

Symptom

Importing a custom SPP Firmware Baseline to iLO Amplifier Pack fails with error "ISO validation failed" since the custom SPP created from the SPP Custom Download Portal does not contain the required files.

Cause

Required files are missing in the custom SPP download.

Action

1. Do either of the following:
   - While creating the Custom SPP from the SPP Custom Download Portal, use the SPP (2018.03.0) or later as the Base to create any custom SPP images.
   - Use SUM (Smart Update Manager) v8.20 or later to create the custom SPP images.

Online Express Interactive Update fails on certain servers with "Activate Failed" message

Symptom

Attempting Online Express Interactive Update on servers with SUT version 2.0.x or earlier could fail with the message **`"Activate Failed"`**. The server is updated with the SPP components, but the Result indicates **`"Activate Failed"`** due to a known issue in SUT version SUT v2.0.x and earlier.

Cause

Issue with the System Update Tool (SUT).

Action

1. During the process of Online Express Interactive Update, do not select the SUT component for update.
2. Update the SUT on the system to SUT v2.1.0 or later.

Online Express Interactive Update on certain servers gets stuck at "Staged" state

Symptom

Attempting Online Express Interactive Update on servers having SUT version 2.2.0 or earlier cannot proceed beyond **"Staged"** state if iLO Amplifier is attempting to rewrite SUT to the same version. The update task in iLO Amplifier Pack waits for approximately eight hours until it times out.

Cause

Issue with the System Update Tool (SUT).

Action

During the process of Online Express Interactive Update, do not select the SUT component for update/ rewrite on the same SUT version on the server.

Servers cannot be selected for performing Online Update even though AMS is running

Symptom

iLO does not detect that AMS is installed and running. Thus iLO Amplifier gets the inventory as **"No AMS found"**. Hence servers with this symptom cannot be selected to perform Online Update from iLO Amplifier.

Cause

The AMS state/status is incorrectly reflecting in the iLO Inventory.

Action

Restart/ Reinstall AMS and reboot the server.

Manual Recovery Task fails in iLO Amplifier as host fails to power on

Symptom

After performing a manual firmware recovery, iLO Amplifier tries to power on the server. Intermittently the host fails to power on and hence the task in iLO Amplifier fails.

Cause

Issue with the iLO firmware v1.20.

Action

Retry the operation.

Duplicate entries created when iLO uses a shared network port and the server is discovered using IP and FQDN

Symptom

Duplicate entries are created when iLO uses a shared network port and the server is discovered using IP and FQDN

Cause

When iLO is configured using a shared network port, discovering the server using IP or FQDN creates duplicate entries.

Action

If iLO is configured with a shared network port, discover the server using either IP or FQDN but not both.

Websites

iLO Amplifier Pack

NOTE: For any product feedback, send an email to **iloamplifier@hpe.com**.

For any product queries or issues, refer to our support channels.

Product page
www.hpe.com/servers/iloamplifierpack
Activation portal
www.hpe.com/downloads/iloamplifierpack
iLO Amplifier Pack Information Library
www.hpe.com/support/ilo-ap-docs
User Guide
www.hpe.com/support/ilo-ap-ug-en
Frequently Asked Questions
www.hpe.com/support/ilo-ap-faq
Release Notes
www.hpe.com/support/ilo-ap-rn-en

iLO
iLO 4
http://www.hpe.com/info/ilo/docs
iLO 5
http://www.hpe.com/info/ilo/docs
iLO licensing
http://www.hpe.com/info/ilo/licensing

HPE ProLiant Servers
HPE ProLiant Gen8 servers
http://www.hpe.com/info/proliantgen8/docs
HPE ProLiant Gen9 servers
http://www.hpe.com/support/proliantgen9/docs
HPE ProLiant Gen10 servers
http://www.hpe.com/support/proliantgen10/docs

HPE InfoSight
HPE InfoSight for Servers
http://www.hpe.com/servers/infosight

General
Hewlett Packard Enterprise Information Library
www.hpe.com/info/EIL

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://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

  www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

  www.hpe.com/support/downloads

  Software Depot

  www.hpe.com/support/softwaredepot

- To subscribe to eNewsletters and alerts:

  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:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT: Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty information for your product, see the links provided below:

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

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:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

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, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.