Hewlett Packard Enterprise

iLO Amplifier Pack 2.22 User Guide

Abstract

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

Part Number: 30-93845920-009
Published: March 2024
Edition: 1

© Copyright 2020–2024 Hewlett Packard Enterprise Development LP

Notices

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

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

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

Acknowledgments

Adobe, the Adobe logo, Acrobat, and the Adobe PDF logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

AMD, the AMD Arrow symbol, ATI, and the ATI logo are trademarks of Advanced Micro Devices, Inc.

Ampere®, Altra®, and the A®, and Ampere® logos are registered trademarks or trademarks of Ampere Computing.

Arm® is a registered trademark of Arm Limited (or its subsidiaries) in the U.S. and/or elsewhere.

Bluetooth is a trademark owned by its proprietor and used by Hewlett Packard Enterprise under license.

DLTtape logo and SDLTtape logo are trademarks of Quantum Corporation in the U.S. and other countries.

Docker and the Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries.

ENERGY STAR® and the ENERGY STAR® mark are registered U.S. marks.

Google™ and the Google Logo are registered trademarks of Google LLC.

Graphcore®, the Graphcore wordmark and Poplar® are registered trademarks of Graphcore Ltd.

Intel Inside®, the Intel Inside logo, Intel®, the Intel logo, Itanium®, Itanium® 2-based, and Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

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

McAfee® and the M-shield logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries.

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

MLCommons™, MLPerf™, and MLCube™ are trademarks and service marks of MLCommons Association in the United States and other countries.

NVIDIA® and NVIDIA logos are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries.

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



Qualcomm® and the Qualcomm logo are trademarks of Qualcomm Incorporated, registered in the United States and other countries, used with permission.

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

SAP®, SAP HANA®, and SAP S/4HANA® are the trademarks or registered trademarks of SAP SE or its affiliates in Germany and in other countries.

sFlow® is a registered trademark of InMon Corp.

TOGAF® is a registered trademark of The Open Group. IT4IT™ is a trademark of The Open Group.

UNIX® is a registered trademark of The Open Group.

VMware®, VMware NSX®, VMware VCenter®, and VMware vSphere® are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.

X/Open® is a registered trademark, and the X device is a trademark of X/Open Company Ltd. in the UK and other countries.

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

Contents

Introduction 9
- Description 9
- iLO Amplifier Pack key features 9
- iLO Amplifier Pack license segmentation 10
- When to use iLO Amplifier Pack 12

Performing first time setup 15
- Verifying prerequisites 15
  - Devices supported 15
  - Operating systems 16
  - Browser requirements 17
  - Languages 17
  - Prerequisites to host iLO Amplifier Pack 17
  - Prerequisites for managed servers 18
  - Prerequisites for performing updates 19
  - Prerequisites for performing recovery 20
- Downloading iLO Amplifier Pack 20
- Validating the authenticity and integrity of the download 21
- Installing iLO Amplifier Pack 21
  - Installing iLO Amplifier Pack using VMware ESXi 21
  - Installing iLO Amplifier Pack using Windows Hyper-V manager 22
  - Installing iLO Amplifier Pack using KVM on Linux 23
- Performing initial setup of iLO Amplifier Pack 24
- Logging in to iLO Amplifier Pack 25
- Verifying the installation 25

Dashboard 26
- Viewing the dashboard 26
- Dashboard details 27

Discovery 29
- Adding a single server from the Discovery page 29
- Adding servers in an IPv4 address range 30
- Adding servers from a CSV file 31

Managing servers 33
- Viewing the server list 33
  - Viewing server details 34
- Adding a single server from the Servers page 35
- Adding servers in an IPv4 address range from the servers page 36
- Managing server UID status 37
- Managing server power status 37
  - Server power options 38
- Updating server firmware from the servers page 38

Configuring remote syslog ... 40
Mounting and ejecting virtual media ... 40
Updating server credentials ... 41
Deleting a server ... 41
Refreshing the server list ... 42
Updating unmanaged servers ... 42

Managing server groups ... 44
Viewing server groups ... 44
Creating a server group ... 45
Joining a server group ... 46
Unjoining servers from a server group ... 46
Deleting a server group ... 47
Managing UID status for server groups ... 48
Managing power status for server groups ... 49
Updating firmware for server groups ... 49
Configuring remote SysLog for server groups ... 50
Mounting and ejecting virtual media for server groups ... 51
Refreshing servers in server groups ... 52

Alerts and Event Logs ... 53
Managed Servers Alerts ... 53
Viewing alerts from managed servers ... 53
Server alert severity ... 54
Server alert details ... 54
Clearing the Server Alert Viewer list ... 54
Exporting server alerts to a .csv file ... 55
Activity Logs and Alerts ... 55
Viewing activity logs ... 55
Clearing activity alerts ... 56
Generating and submitting the Product Entitlement Report ... 56

Baseline Management ... 58
Importing a firmware baseline ... 58
Importing an OS baseline ... 59
Working with configuration baselines ... 60
Create a configuration baseline ... 60
Import a configuration baseline from a server ... 61
Editing a new configuration baseline ... 61
Deleting a configuration baseline ... 62

Server firmware and driver updates ... 64
Performing an online firmware update for Gen8 and Gen9 servers ... 65
Performing an Express Interactive Update ... 66
Performing a Baseline Automatic Update ... 69
Performing an offline firmware update for Gen8 and Gen9 servers ... 72
iLO Repository Updates ... 74
Performing an iLO Repository Online Update ... 75
Performing an iLO Repository Offline Update ... 76
Deploying already staged firmware and driver components ... 78
Update Jobs monitor ... 80

HPE InfoSight 82
Obtaining a claim token 82
Linking iLO Amplifier Pack with HPE InfoSight 83
Prerequisites for midway server connectivity 85
Viewing the InfoSight Status Report and sending AHS data 86
Managing servers for InfoSight 88
Viewing HPE InfoSight Recommendation Alerts 90
Monitoring InfoSight jobs 92
HPE Unified Supportability Pipeline 94
Working with HPE Unified Supportability Pipeline add-on services 94

Baseline Compliance report 96
Creating the Baseline Compliance report 96
Viewing the Baseline Compliance report 97

Recovery Management 99
Recovery operations 100
Recovery policy 101
Create a recovery policy 101
Delete a recovery policy 102
Recovery administration 102
Assign a recovery policy 102
Unassign a recovery policy 104
Performing a manual recovery 104
Performing a quarantine operation 106
Monitoring recovery jobs 106

Reports 108
Viewing the firmware report 108
Firmware report details 109
Viewing the iLO license report 110
Viewing the basic device report 112
Viewing the Hardware Inventory Report 114
Viewing the Software Inventory Report 116
Viewing the Custom Report 117

Server troubleshooting 119
Discovery of servers fail for external multiple storage enclosures that have too many hard drives 119
Downloading the server Active Health System log 119
Logging in to Active Health System Viewer 120
Logging out of AHSV 120
Loading an AHS log file 121

Viewing job status 122

iLO Amplifier Diagnostics 124

Configuring the iLO Amplifier Pack appliance 126
Upgrading the appliance firmware 126
Upgrading the appliance firmware manually 126
Upgrading the appliance firmware automatically 127
Appliance firmware upgrade storage types 129
Configuring Add-on Services 129
Installing, disabling, and uninstalling an add-on service 130
Installing an add-on service using a binary file 131
Updating add-on services 131
Updating an add-on service using a binary file 132
Configuring general settings 132
Server inventory and service account 134
Configuring alert settings 135
Sending a test alert 137
Setting up an IFTTT alert 137
IFTTT alert syntax 138
Configuring network settings 138
Configuring the network ports 139
Configuring general network settings 140
Configuring proxy settings 141
Configuring time and NTP settings 142
Configuring Remote SysLog Settings for iLO Amplifier Pack 142
Configuring security settings 143
Configuring access settings 143
Obtaining and importing an SSL certificate 143
Generating a certificate signing request 144
Configuring LDAP 144
Configuring Directory Server Settings 145
Managing iLO Amplifier Pack user accounts and active sessions 146
Adding a group account 146
Editing a group account 147
Local users 147
Adding a user account 147
Editing a user account 148
Disabling a user account 149
Deleting a user account 149
iLO Amplifier Pack user privileges 149
Directory groups 150
Disabling a group account 150
Deleting a group account 150
iLO Amplifier Pack group privileges 151
Active sessions 151
Backup and Restore 151
Backing up the iLO Amplifier Pack configuration 151
Restoring the iLO Amplifier Pack configuration 152

iLO Amplifier Pack Redfish API Implementation 154

iLO Amplifier Pack troubleshooting 155
Discovery of servers fail for external multiple storage enclosures that have too many hard drives 155
SSH session does not close 155

Alert notification not visible ... 155
SUT components not downgraded during online update ... 156
Failure message appears when a job is created ... 156
Loading and exporting activity alerts and logs to CSV causes unresponsive GUI ... 156
Firmware configuration settings may not be recovered for S100i Smart Array controller ... 157
Importing a custom SPP Firmware Baseline to iLO Amplifier Pack fails ... 157
Online Express Interactive Update fails on certain servers with "Activate Failed" message ... 157
Online Express Interactive Update on certain servers gets stuck at "Staged" state ... 158
Servers cannot be selected for performing Online Update even though AMS is running ... 158
Duplicate entries created when iLO uses a shared network port and the server is discovered using IP and FQDN ... 158
iLO Repository offline update on servers with High Security modes configured fails when force downgrade option is selected ... 159

InfoSight and appliance update connectivity troubleshooting ... 160

Invalid midway or DNS address. Check the network settings and retry ... 160
Failed to establish connection to midway server. Check the network settings (Proxy/DNS) and retry ... 160
Invalid proxy address ... 161
Failed to establish connection to proxy server. Verify the proxy settings ... 161
Service not running. Enable/Re-submit the InfoSight Settings ... 161
Not Registered ... 162

AHS download error troubleshooting ... 163

AHS file size exceeds max size. Recommended to update the iLO firmware to the latest version ... 163
AHS download not enabled in iLO ... 163
Connection to iLO failed ... 163
AHS file location invalid in iLO ... 164
Connection to iLO failed. Could not get the Authentication Token ... 164
Server Serial Number/Product ID is Blank ... 164
AHS download failed due to NAND failures. Verify the NAND health ... 165

Websites ... 166

Support and other resources ... 167

Accessing Hewlett Packard Enterprise Support ... 167
Accessing updates ... 167
Remote support ... 168
Warranty information ... 168
Regulatory information ... 168
Documentation feedback ... 168

Introduction

Description

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. iLO Amplifier Pack performs rapid server discovery and inventory for thousands of supported servers for the purpose of updating firmware and drivers at scale.

IMPORTANT: The iLO Federation groups functionality to be discontinued from iLO Amplifier Pack 2.20 release.

iLO Amplifier Pack key features

- **Server System Restore**—iLO Amplifier Pack works with iLO 5 v2.30 or later for Gen10 servers and Gen10 Plus servers to initiate and manage system recovery processes for servers.
- **Gen10 Plus server support**—iLO Amplifier Pack supports HPE ProLiant Gen8, Gen9, and Gen10 servers. As of version 1.60, iLO Amplifier Pack also offers support for certain Gen10 Plus servers in addition to certain Edgeline and Moonshot server blades.
- **Gen11 server support**—iLO Amplifier Pack supports HPE ProLiant Gen11 servers. As of version 2.20, iLO Amplifier Pack supports Gen11 servers.
- **Baseline importing**—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, Gen10 servers and above, and Gen11 servers, including firmware, hardware, and iLO licenses in a matter of minutes.
- **Baseline compliance report**— iLO Amplifier Pack allows users to generate Baseline 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**—iLO Amplifier Pack is IPv6 compliant. Users can use IPv6 addresses when adding servers or configuring various iLO Amplifier Pack network settings.
- **Simplified updates**—iLO Amplifier Pack simplifies update management jobs making it easier and faster with a user interface that is similar to iLO. Users can update multiple servers on server groups reducing downtime and personnel requirements.
- **Group management**—iLO Amplifier Pack can create new groups, add servers to existing groups, and manage server groups.
- **InfoSight integration**—iLO Amplifier Pack version 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.
- **Hyper-V and KVM support**—iLO Amplifier Pack supports Microsoft Hyper-V and KVM. Users can deploy iLO Amplifier Pack using Microsoft Hyper-V on Windows Server, and using KVM on **supported operating systems**.

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 v2.78 and v2.81 or later for Gen8 and Gen9 servers • iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • iLO 6 v1.10, v1.20, and v1.30 or later for Gen11 servers
Inventory	✓	✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • iLO 6 v1.10, v1.20, and v1.30 or later for Gen11 servers
Reports	✓	✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • iLO 6 v1.10, v1.20, and v1.30 or later for Gen11 servers
Core platform firmware update	✓	✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • iLO 6 v1.10, v1.20, and v1.30 or later for Gen11 servers
Core platform firmware update		✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers

Table Continued

Feature	iLO Standard iLO Essentials iLO Scale-Out	iLO Advanced	Dependencies
Online update for firmware, drivers, and HPE software		✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • AMS (iLO Agentless Management Service) v10.99.0 or later for Windows or AMS v2.10.5 or later for Linux on Gen8 and Gen9 servers • SPP v2022.0822.4 or later • iSUT v2.9.1.0 and v4.1.0.0 or later for Gen8, Gen9 servers
iLO Repository Online Update		✓	• iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • AMS v2.51.2.0 and v2.51.3.0 or later for Windows, AMS v2.7.0 and v3.3.0 or later for Linux, and AMS v2022.09.01 and, v2023.04.01 or later for ESXi on Gen10 and Gen10 plus servers • iSUT v2.9.1.0 and v4.1.0.0 or later • HPE SUT v2.9.1.0 and v4.1.0.0 or later for Gen10 Plus servers • SPP v2023.03.00.00 or later
Baseline compliance report	✓	✓	• AMS (iLO Agentless Management Service) v10.99.0 or later for Windows or AMS v2.10.5 or later for Linux on Gen8 and Gen9 servers • AMS v2.51.2.0 and v2.51.3.0 or later for Windows, AMS v2.7.0 and v3.3.0 or later for Linux, and AMS v2022.09.01 and, v2023.04.01 or later for ESXi on Gen10 and Gen10 plus servers
Offline update for firmware and drivers		✓	• iLO 4 v2.78 and v2.81 or later for Gen8 and Gen9 servers • Service Pack for ProLiant
iLO Repository Offline Update		✓	• iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • SPP v2023.03.00.00 or later

Table Continued

Feature	iLO Standard iLO Essentials iLO Scale-Out	iLO Advanced	Dependencies
Server System Restore		✓	• iLO 5 2.72, 2.78, and 2.81 or later for Gen10 servers and Gen10 Plus servers • AMS v2.51.2.0 and v2.51.3.0 or later for Windows, AMS v2.7.0 and v3.3.0 or later for Linux, and AMS v2022.09.01 and , 2023.04.01 or later for ESXi on Gen10 and Gen10 plus servers • iSUT v2.9.1.0 and v4.1.0.0or later • SPP v2023.03.00.00 or later
Alerts	• UI • iLO Amplifier Pack Redfish API Implementation	• UI • Email • IFTTT • iLO Amplifier Pack Redfish API Implementation	
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 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 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 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 v2.30 or later for Gen10 servers and Gen10 Plus servers 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

About this task

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

Procedure

1. **Verifying prerequisites**
2. **Downloading iLO Amplifier Pack**
3. **Installing iLO Amplifier Pack**
4. **Performing initial setup of iLO Amplifier Pack**
5. **Logging in to iLO Amplifier Pack**
6. **Verifying the installation**

Verifying prerequisites

Devices supported

iLO Amplifier Pack supports the following HPE ProLiant servers:

- HPE ProLiant Gen8 (Rack and Tower) servers
- HPE ProLiant Gen9 (Rack and Tower) servers
- HPE ProLiant Gen10 and Gen10 Plus (Rack and Tower) servers
- HPE ProLiant Gen11 servers
- HPE ProLiant MicroServer Gen10 Plus Server
- Edgeline and Moonshot server with iLO 5
  - HPE ProLiant m750 Server
  - HPE ProLiant e910 Server
  - HPE ProLiant e910t Server
- HPE Apollo 4000 Systems (Gen10 Plus, Gen10 and Gen9 with iLO5 or iLO4)
- HPE Alletra 4K Gen 11 server with iLO6

NOTE:

- SPP-based online/offline updates are not available for Edgeline and Moonshot devices. Use the Edgeline/Moonshot firmware and software component packs to update these devices from the **Servers** page in iLO Amplifier Pack. You can find information regarding device updates in the system firmware and software release notes at **http://www.hpe.com/info/edgeline-docs** and **http://www.hpe.com/info/moonshot/docs**.
- Moonshot and Edgeline chassis information is not supported in iLO Amplifier Pack.
- HPE ProLiant m750 Server Blades are not supported if HPE Moonshot iLO Chassis Management Firmware 2.0 has iLO Direct Access disabled. For more information on configuring iLO Direct Access, see the **HPE Moonshot Chassis Manager 2.0 User Guide**.
- If HPE OneView manages HPE ProLiant, Apollo, or Synergy servers, iLO Amplifier Pack does not support any firmware and driver updates.

Operating systems

NOTE: The following operating systems are supported for online updates.

Operating System [1]	Gen8 and Gen9	Gen10 and Gen10 Plus	Gen11
Microsoft Windows 10 x64 [2]		✓	
Microsoft Windows Server 2022	Supports only Gen9	✓	✓
Microsoft Windows Server 2019	✓	✓	✓
Microsoft Windows Server 2016	✓	✓	
Microsoft Windows Server 2012 R2	✓	✓	
Microsoft Windows Server 2012 Essentials	✓	✓	
Red Hat Enterprise Linux 8 Server and above (x86-64)	✓	✓	
Red Hat Enterprise Linux 7 Server (x86-64)	✓	✓	
Red Hat Enterprise Linux 6 Server (x86-64)	✓	✓	
Red Hat Enterprise Linux 8.6 Server and 9.0 Server (x86-64)			✓
SUSE Linux Enterprise Server 15 SP1 and SP2 (x86-64)	✓	✓	
SUSE Linux Enterprise Server 12 SP4 and SP5 (x86-64)	✓	✓	

Table Continued

Operating System [1]	Gen8 and Gen9	Gen10 and Gen10 Plus	Gen11
SUSE Linux Enterprise Server 12 SP5 and 15 SP4	Supports only Gen9	✓	
SUSE Linux Enterprise Server 11 (x86-64)	✓	✓	
SUSE Linux Enterprise Server 15 SP4			✓
VMware ESXi Server 7.0, 7.0 U1, and 7.0 U2		✓	
VMware ESXi Server 6.7 U3		✓	
VMware ESXi Server 7.0 U3 (without vSAN) and 7.0 U2 (with vSAN)		✓	✓

1 For more information, see HPE Service Pack for Proliant Release Notes.

2 Only for inventory on the HPE ProLiant m750 Server Blade.

To know more about the supported Operating Systems for Edgeline, Moonshot and IoT Systems, see **www.hpe.com/support/edgeline-moonshot-IoT-OS**.

Browser requirements

NOTE: Internet Explorer is not a recommended browser.

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

- Chrome v100.0 or later
- Firefox v99.0 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 any of the following:

- A host server configured with VMware ESXi 6.5 or later.
- Windows hypervisor for Windows Server 2016, Windows Server 2019, or Windows Server 2022 DC.
- KVM on any of the following operating systems:
  - Red Hat Enterprise Linux 8 and above.
  - Red Hat Enterprise Linux 7.7 and above.
  - SUSE Linux Enterprise Server 15 SP1 or SP2
  - SUSE Linux Enterprise Server 12 SP4 or SP5

The iLO Amplifier Pack guest VM requires the following minimum resources to be available on the ESXi server, Windows Hyper-V, or KVM:

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

Prerequisites for managed servers

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

Server	Recommended component versions
Gen8 and Gen9 servers	• iLO 4 v2.78 and iLO4 v2.81 • AMS (iLO Agentless Management Service) For Windows - iLO4 10.99, 10.100 For Linux - iLO4: 2.10.5 For Esxi - 2022.09.01, 2023.04.01
Gen10 servers and Gen10 Plus servers	• iLO 5 v2.72, v2.78, and v2.81 • AMS (iLO Agentless Management Service) For Esxi - 2022.09.01 and 2023.04.01 • iSUT Windows/Linux - 2.9.1.0, 4.1.0.0 • iSUT - ESXi 7.0U3, 8.0 - 2021.12.00 and 2023.03.00

Table Continued

Server	Recommended component versions
Gen11 servers	• iLO 6 v1.10, v1.20, and v1.30 • AMS (iLO Agentless Management Service) For Windows - v3.10.0.0, v3.20.0.0, and v3.30.0.0 For Linux - iLO6: v3.1.0, v3.2.0, and v3.3.0 For Esxi - v2022.11.01, v2023.02.01, and v2023.04.01 • iSUT Windows/Linux - 4.0.0.0/4.1.0.0 • iSUT ESXi - 2022.11.00
Edgeline/Moonshot servers	• iLO 5 v2.55, v2.65, v2.70 , and v2.72 • AMS (iLO Agentless Management Service) For Windows - iLO4 10.99, 10.100; iLO5: 2.50.1.0, 2.51.0.0 , 2.51.2.0. For Linux - iLO4: 2.10.3, 2.10.5; iLO5: 2.50, 2.6.0 , 2.7.0 For Esxi - 2021.10.01 and 2022.09.01

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: https://www.hpe.com/servers/sut**

Prerequisites for performing updates

- The recommended SPP versions for Gen11 servers are 2022.12.00.00, 2023.02.00.00, 2023.04.00.00.
- For all generation of servers - SPP (Service Pack for ProLiant) Versions 2022.12.00.00, 2022.03.01, 2022.09.01.00 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
    - .fwpkg
    - .hex
    - .vme
    - .flash

- Bootable baseline ISO image of the firmware update imported into iLO Amplifier Pack. For more information, see "Importing a baseline" in the **iLO Amplifier Pack User Guide**.

  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.

- SPP-based online/offline updates are not available for Edgeline and Moonshot devices. Use the Edgeline/Moonshot firmware and software component packs to update these devices from the **Servers** page in iLO Amplifier Pack. You can find information regarding device updates in the system firmware and software release notes at **http://www.hpe.com/info/edgeline-docs** and **http://www.hpe.com/info/moonshot/docs**.

NOTE:

- iLO Amplifier Pack does not support firmware or driver updates on HPE ProLiant Blade/Synergy servers if they are managed by HPE OneView or VMware vCenter.
- Gen 10 servers and above does not support SPP hosted on an external web server.

IMPORTANT:

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

Use the command `sut -set ilousername=<username> ilopassword=<password>` as when the BIOS password is set, iSUT requires iLO credentials to communicate with iLO.

Prerequisites for performing recovery

Recovery can be performed only on Gen10 and Gen10 plus servers with:

- iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
- SPP v2020.09.0 or later
- SPP consisting of iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
- 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.

Downloading iLO Amplifier Pack

Prerequisites

HPE Passport Login credentials

Procedure

1. Go to the **My HPE Software Center webpage** and login with your HPE Passport Login credentials.
2. Navigate to **Free Software** > **Family: iLO Amplifier Pack** from the Free Software list. Click the **iLO Amplifier Pack** title for displaying the product description.

3. Click the **Download** button and a new page with the list of available binaries will be displayed.
4. Download the appropriate file based on your method of installation to a local directory.

Validating the authenticity and integrity of the download

Prerequisites

- The latest version of the iLO Amplifier Pack appliance file (`ova`, `zip` or `qcow2`) is downloaded.
- The corresponding `.sig` file for iLO Amplifier Pack is downloaded. The `.sig` file is available from the same location as the iLO Amplifier Pack appliance file.

About this task

When you download the iLO Amplifier Pack appliance file from **My HPE Software Center**, you can trust that the virtual appliance image is from HPE because your browser HTTPS connection uses trusted security certificates.

Procedure

1. To further validate the authenticity and integrity of the file, use the free GNU Privacy Guard (GPG) tools:
   - `gpg --verify <filename>.ova.sig <filename>.ova`
   - `gpg --verify <filename>.zip.sig <filename>.zip`
   - `gpg --verify <filename>.gz.sig <filename>.gz`

   NOTE: This digital signature verification step is not required for upgrade installations. The upgrade file (the `*.bin` file) is already digitally signed. The digital signature is automatically validated during the upgrade procedure.
2. See the **HPE GPG or RPM Signature Verification webpage** for detailed verification instructions.

Installing iLO Amplifier Pack

Installing iLO Amplifier Pack using VMware ESXi

Prerequisites

- A host server configured with VMware ESXi 6.5 or later
- A laptop or desktop system with 8GB of minimum available RAM and VMware vSphere Client installed or a supported web browser

Procedure

1. Click the download link on the My HPE Software Center page to download the ova file for VMware ESXi.
2. Check the integrity of the downloaded **`iLOAmpPack_X.XX_vmware.ova`** by comparing the checksum of the file with the checksum value listed on the download page by using an appropriate checksum verification tool.

NOTE: The OVA file is digitally signed. To validate the authenticity and integrity of the download, follow the instructions at the **HPE GPG or RPM Signature Verification webpage**. See **Validating the authenticity and integrity of the download** for more information.

3. Use the VMware vSphere Client or a supported web browser to connect to any VMware ESXi server (6.7U3 or later).
4. 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.
5. 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 restarts, the first-time setup screen is displayed on the console.

Installing iLO Amplifier Pack using Windows Hyper-V manager

Prerequisites

A laptop or desktop system with 8GB of minimum available RAM and Hyper-V manager installed

Procedure

1. Click the download link on the My HPE Software Center page to download the zip for Hyper-V Manager.
2. Check the integrity of the downloaded **`iLOAmpPack_X.XX_HyperV.zip`** by comparing the checksum of the zip file with the checksum value listed on the download page by using an appropriate checksum verification tool.

   NOTE: The ZIP file is digitally signed. To validate the authenticity and integrity of the download, follow the instructions at the **HPE GPG or RPM Signature Verification webpage**. See **Validating the authenticity and integrity of the download** for more information.
3. Extract the **`iLOAmplifierPack`** folder from the zip file.
4. In Hyper-V manager, go to **Actions** > **New** > **Virtual Machine**.

   IMPORTANT: Do not use the **New** action to create a new virtual machine.
5. Select a name and location for the **VM**.
6. Select the generation as **Generation 1**.
7. Specify the of memory to allocate as 8192 MB.
8. Select the networking switch.
9. Connect the existing Virtual Hard Disk from the previously downloaded path `iLOAmplifierPack\Virtual Hard Disks\iLOAmplifierPack.vhdx` and click **Finish**.
10. Navigate to the **Settings** page of the newly deployed VM.

11. Add **Hardware** and select **Network Adapter**.
12. Specify the **Virtual Switch** from the menu and click **Ok**.

    Power on the new VM after the VM gets created.

Installing iLO Amplifier Pack using KVM on Linux

Procedure

1. Click the download link on the My HPE Software Center page to download the qcow2 image file for KVM.
2. Check the integrity of the downloaded qcow2 image file by comparing the checksum of the file with the checksum value listed on the download page by using an appropriate checksum verification tool.

   NOTE: The QCOW2 file is digitally signed. To validate the authenticity and integrity of the download, follow the instructions at the **HPE GPG or RPM Signature Verification webpage**. See **Validating the authenticity and integrity of the download** for more information.
3. Launch Virtual Machine Manager.

   IMPORTANT: The virtual machine storage must have a minimum of 100GB of free space available at all times.
4. From the menu of Virtual Machine Manager, select **File** > **New Virtual Machine** to launch the New VM wizard.
5. From the available options, select **Import existing disk image** and browse to the location where you extracted the qcow2 image file.
6. Follow the onscreen instructions to set up the VM.
   a. Use the default options for **OS type** and **Version**.

      NOTE: For Red Hat Enterprise Linux 8.0 and SUSE Linux Enterprise Server, choose the **OS type** as **Debian Stretch** (Debian 9).
   b. Set the minimum value for Memory as 8192MB and the minimum number of CPU cores as 4 and then click **Forward**.
   c. Specify a name for the virtual machine.
   d. Under **Network selection**, select a network device that has connectivity to your management LAN.
   e. Select the **Source mode** as **Bridge**.
   f. Select the option to **Customize configuration before install**.
   g. Click **Finish**.
   h. iLO Amplifier Pack must be configured with two network interfaces. Click **Add Hardware** > **Network** and then select a network device that has connectivity to your management LAN. Select the **Source mode** as **Bridge**.

      IMPORTANT: Unless two network interfaces are added, the iLO Amplifier Pack welcome screen will display the localhost IP address instead of the appliance IP address, and **you will not be able to access the appliance interface**.

i. For SUSE Linux Enterprise Server 15 SP2 only, select the **Device model** as **rtl8139** for both network interfaces and click **Apply**.

j. Select the Virtual Disk Device type as SCSI Disk by changing the disk bus to `SCSI` instead of `VirtIO`. Make any additional changes to the configuration if required in the window that appears, and then click **Begin Installation**.

7. The appliance will now start from the virtual machine console.

   After the VM has started, the first-time setup screen is displayed on the console.

Performing initial setup of 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 Preferred Network Port which will be used to manage servers. NIC 1 is selected by default.

   NOTE: Access to two NICs are provided intentionally to enable iLO Amplifier Pack to connect to two separate networks; one network to connect to iLO over https connections and another to connect to the Internet to access email or IFTTT services. If Internet access is available through the management network, then the second NIC can be disabled.

   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 a welcome screen displays the IP address of the iLO Amplifier Pack management appliance.

Logging in to iLO Amplifier Pack

Prerequisites

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. Read the **iLO Amplifier Pack Acceptable Use Policy** displayed in the pop-up. Click **OK** to continue.

   The iLO Amplifier Pack management dashboard appears.

Verifying the installation

Prerequisites

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

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**.

Dashboard

The Dashboard page displays the server health summary and various other widgets. These widgets provide information about the active sessions, server groups, server models, HPE InfoSight status and AHS transmission details, various alerts, and the baseline compliance jobs.

Viewing the dashboard

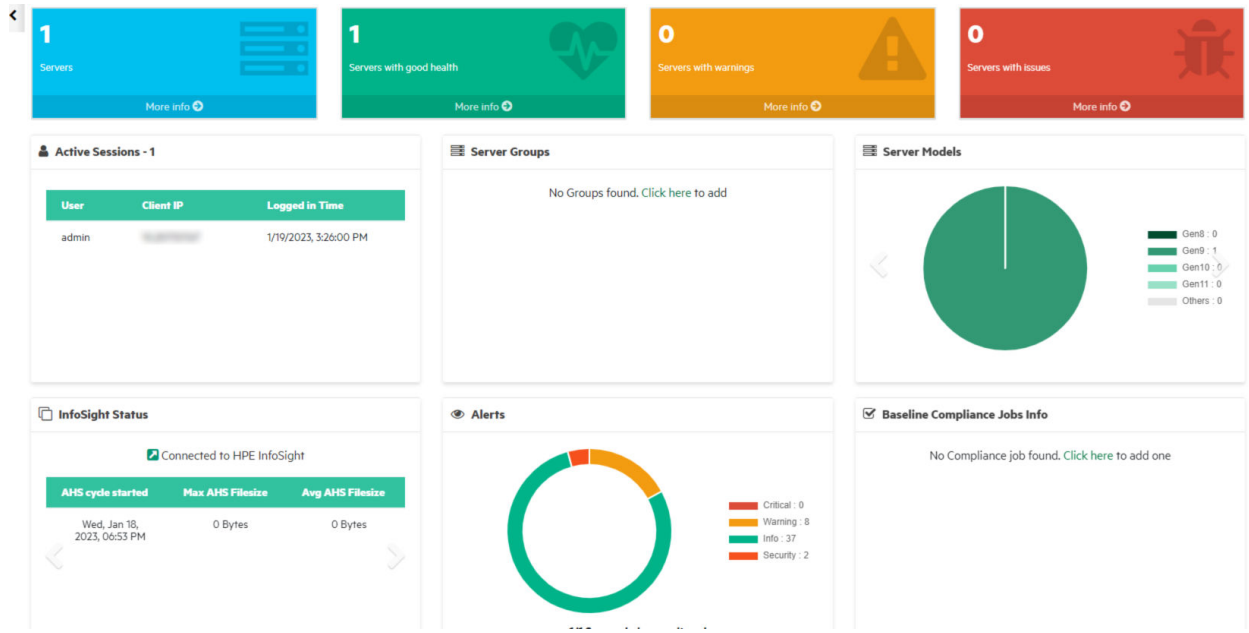
Prerequisites

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

Procedure

1. Click **Dashboard** from the left navigation menu.
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 graph or pie chart to jump to the corresponding page in iLO Amplifier Pack.
   - Click a legend in the graph or pie chart to apply a corresponding filter.

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—This tile also updates to show the servers in critical and unknown states.
- **Active Sessions**—The count of the active sessions is displayed at the top of the widget. The maximum number of active sessions allowed is 20. 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.

  For more information, see **Active sessions**.
- **Server Groups**—Graph showing server groups and the count of servers in each server group separated by the health status.
- **Server Models**—Shows a pie chart to represent the number of servers the customer is managing in each of the different server generation. Also shows a bar graph with the number of servers in each server generation on a per server model basis. Click the arrows to cycle through the views.
- **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 can be viewed by clicking the arrow keys.

- **Alerts**—Donut chart representation of the different alerts that are either critical, warning, informational, or relating to security. The bottom of the widget shows the number of servers being monitored out of the total servers being managed in iLO Amplifier Pack.
- **Baseline Compliance Job Info**—Graph which represents the various baseline compliance jobs that have been run and whether the servers are compliant or not. The bottom of the widget shows the count of servers on which the compliance job is not run out of the total servers being managed in iLO Amplifier Pack.
- **Notification bell**—Provides the count of the alerts received from the managed systems and alerts recommended by InfoSight. Clicking the alert takes you to the **Managed Server Alerts** or the **InfoSight Recommendation Alerts** page depending on the type of the alert.

Discovery

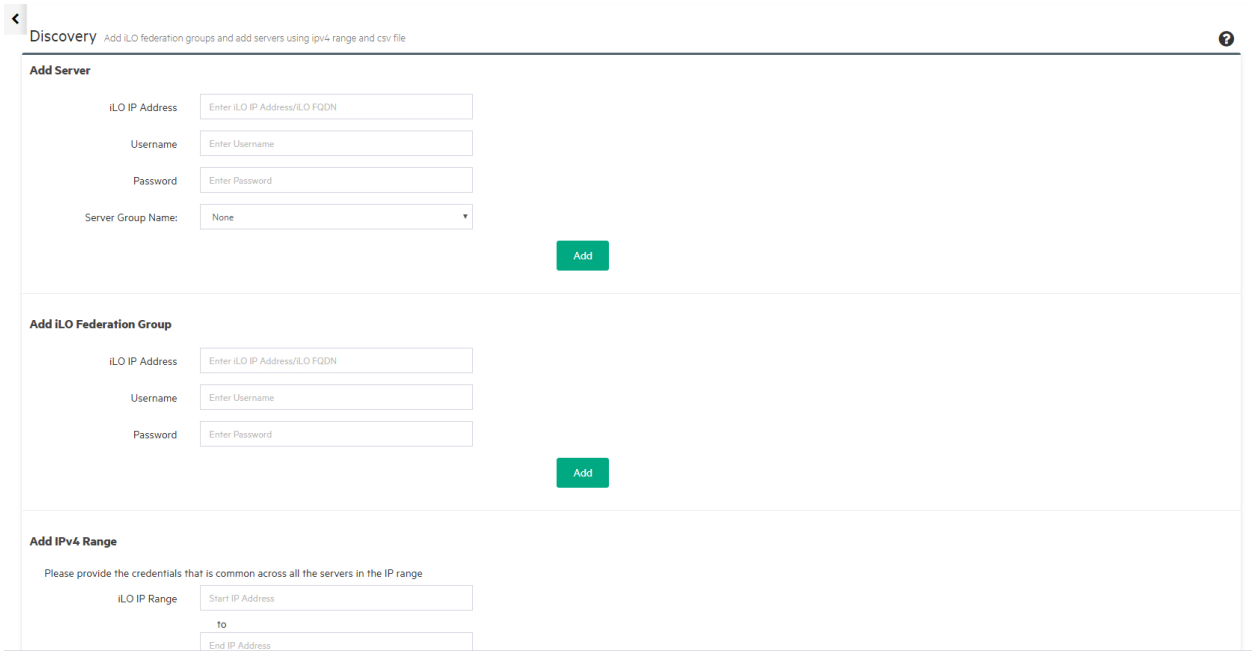
The Discovery page allows you to add assets to manage with iLO Amplifier Pack. Use the Discovery page to discover individual servers, servers within an IPv4 address range, and servers listed in a CSV file.

Adding a single server from the Discovery page

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE Gen8 or Gen9 server with iLO 4 v2.76 or later
- HPE Gen10 server and Gen10 Plus server with iLO 5 v2.30 or later
- HPE Gen11 server with iLO 6 v1.10
- HPE Alletra 4K Gen11 server with iLO 6

About this task



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 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 servers in an IPv4 address range

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE Gen8 or Gen9 server with iLO 4 v2.76 or later
- HPE Gen10 server and Gen10 Plus server with iLO 5 v2.30 or later
- HPE Gen11 server with iLO 6 v1.10
- HPE Alletra 4K Gen11 server with iLO 6

About this task

iLO Amplifier Pack accepts a range of IPv4 addresses to be provided for the discovery of servers. Users can also schedule a discovery operation across a range of IPv4 addresses during a specified time.

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 **Run One Time Scan**.

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

   Servers in the IPv4 range that have incorrect credentials will not be added to iLO Amplifier Pack. To add user account credentials for unmanaged servers, see **Updating unmanaged servers**.

   NOTE: If there are one or more monitoring jobs that are already running, the Discovery Monitoring Job might take slightly longer to complete.

Scheduling IPV4 Range Discovery

4. Optional: To schedule a periodic server discovery and inventory job for a specified IPv4 range, do the following:

   a. Click **Save** to save the information entered in the **Add IPv4 Range** section.

      NOTE: You can schedule up to 5 IPv4 ranges to be discovered.

   b. Enter a value in the **Scan Interval** section in 24 hour format to schedule the server discovery job. If you have provided more than one IPv4 range, the server range scans will be performed sequentially.

   c. Expand the **Scheduled IPv4 Ranges** section to view the scheduled IPv4 ranges added.

   d. Each IPv4 range can be edited or deleted as required by selecting the corresponding icon under the **Action** column.

   e. The **Last Scanned Time** fields shows the time when the IPv4 server discovery job was last performed.

5. 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 Gen8 or Gen9 server with iLO 4 v2.76 or later
- HPE Gen10 server and Gen10 Plus server with iLO 5 v2.30 or later
- HPE Gen11 server with iLO 6 v1.10
- HPE Alletra 4K Gen11 server with iLO 6
- 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.

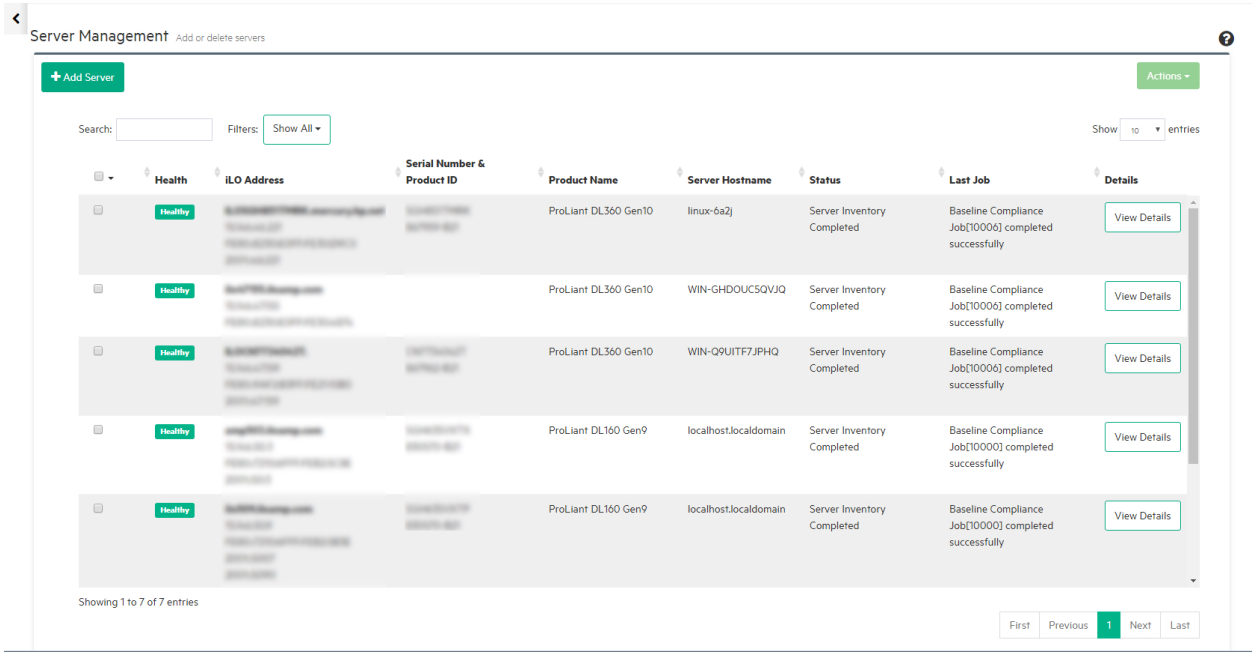
Managing servers

Viewing the server list

Prerequisites

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

About this task



Procedure

1. Click **Assets** on the navigation menu, and then click **Servers**. The **Server Management** page displays 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 FQDN (fully qualified domain name) of the iLO, along with the IPv4 and IPv6 addresses (and port, when applicable) of the iLO subsystem.

- **Serial number and Product ID**—The server serial number, which is assigned when the system is manufactured, and the product ID of the server.
- **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 Job**—The last completed iLO Amplifier Pack job and job 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.

   The **Filters** menu allows you to filter for the following options:

   - **Standalone Managed Servers**—Servers that are not part of any group and are managed individually.
   - **Edgeline Servers**—Servers that are added and managed via HPE Edgeline.
   - **OneView Managed Servers**—Servers that are added and managed via HPE OneView.
   - **Unmanaged Servers**—Servers that have a status of **Unmanaged**. This might be due to unknown health status, incompatible iLO firmware version, invalid or missing credentials, or the server may be unreachable. Also, the servers for which a service account creation fails are listed here.
   - **Server Groups**

3. Optional: Use the following actions to manage servers from this page:

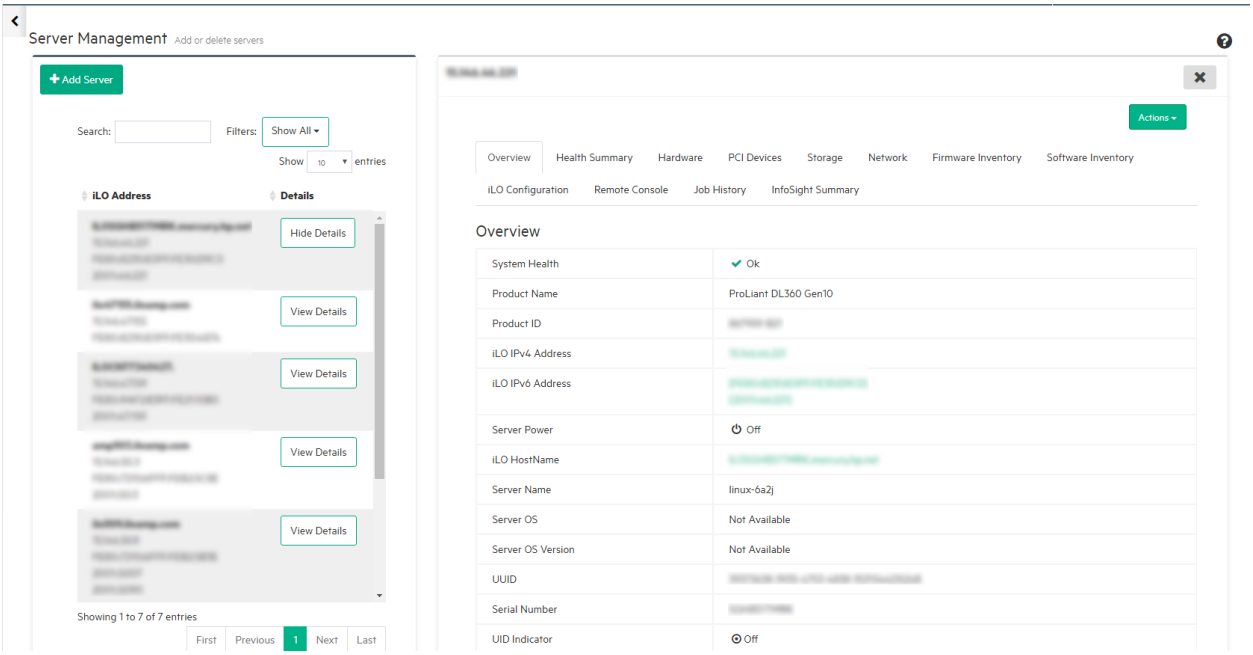
   NOTE: Users with **Login** privileges cannot manage servers.

   - **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**.
     - **Update Credentials**— see **Updating server credentials**
     - **Delete**—see **Deleting a server**.
     - **Refresh**—see **Refreshing the server list**.

Viewing server details

Click **View Details** to view more information about individual servers. 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 Java IRC and provides links for using it.
- **Job History** tab—displays the name, progress percentage, status, and time completed for server jobs.
- **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 and Gen10 Plus server with iLO 5 version 2.30 or later
- HPE ProLiant Gen 11 server with iLO6 version 1.10
- HPE Alletra 4K Gen11 server with iLO 6

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 IP address/iLO FQDN.
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 Gen8 or Gen9 server with iLO 4 v2.76 or later
- HPE Gen10 server and Gen10 Plus server with iLO 5 v2.30 or later
- HPE Gen11 server with iLO 6 v1.10
- HPE Alletra 4K Gen11 server with iLO 6

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 user name 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 that 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 have incorrect credentials will not be added to iLO Amplifier Pack.

   To add user account credentials for unmanaged servers, see **Updating unmanaged servers**.

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

Prerequisites

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

- Configure User.
- Configure Devices.

- A core platform firmware image.

  It is a single component update supported by iLO through Redfish APIs using the firmware image of the component and not the complete SPP. The firmware image can be extracted from a core platform component in SPP, or obtained from HPE support portal.

- Ensure that you are on HPE iLO 5 version 2.30 and above to update the core firmware from the GUI for the `*.fwpkg` file format.

About this task

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
- Innovation Engine (IE) or Server Platform Services (SPS) firmware
- Language Packs

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. Click to select **HTTP/HTTPS Share** or **File Upload** from the **Storage Type** menu.
5. Do one of the following:
   - For **HTTP/HTTPS Share**, enter the HTTP or HTTPS url to the ISO image. This URL can be an IPv4 or IPv6 address.
   - For **File Upload**, click **Choose File** to open the file explorer and choose the baseline stored on your local drive.

     NOTE: You can update the core firmware from the GUI for the `*.fwpkg`, `*.bin`, `*.vme`, `*.hex` and `*.flash` file formats for both **HTTP/HTTPS** and **File Upload** storage methods.[1]
6. 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.
7. Click **Apply** to begin the update or click **Close** to return to the **Servers** page.

[1] Power Management Controller, chassis firmware, and NVMe backplane files use the file extension `*.hex` . System Programmable Logic Device (CPLD) firmware file uses the file extension `*.vme`.

Configuring remote syslog

Prerequisites

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

About this task

The remote syslog feature allows you to configure a remote syslog server in iLO Amplifier Pack to send the server system logs and events from iLO Amplifier Pack to a central log collector.

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**.

Updating server 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. Select the check boxes for the servers you want to manage.
3. To update the credentials of servers with invalid credential, click **Actions**, and then select **Update Credentials**.
4. Enter the **Username** and **Password** for the selected server.
5. Click **Apply** to update the valid username and password.

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**.

Updating unmanaged servers

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

About this task

If the iLO credentials for a managed server are modified after it has already been discovered in iLO Amplifier Pack, its status will change to **Unmanaged** on the next refresh of server inventory. To change an unmanaged server to a managed server, provide valid credentials.

Procedure

1. Do one of the following:

   - To manage individual servers:

     a. Click **Assets** from the left navigation menu, and then click **Servers**.

     b. Locate a server with a status of **Unmanaged**. You can also use the **Filters** menu to display all **Unmanaged Servers**.

     c. Click **Manage**.

     d. Enter the iLO username and password.

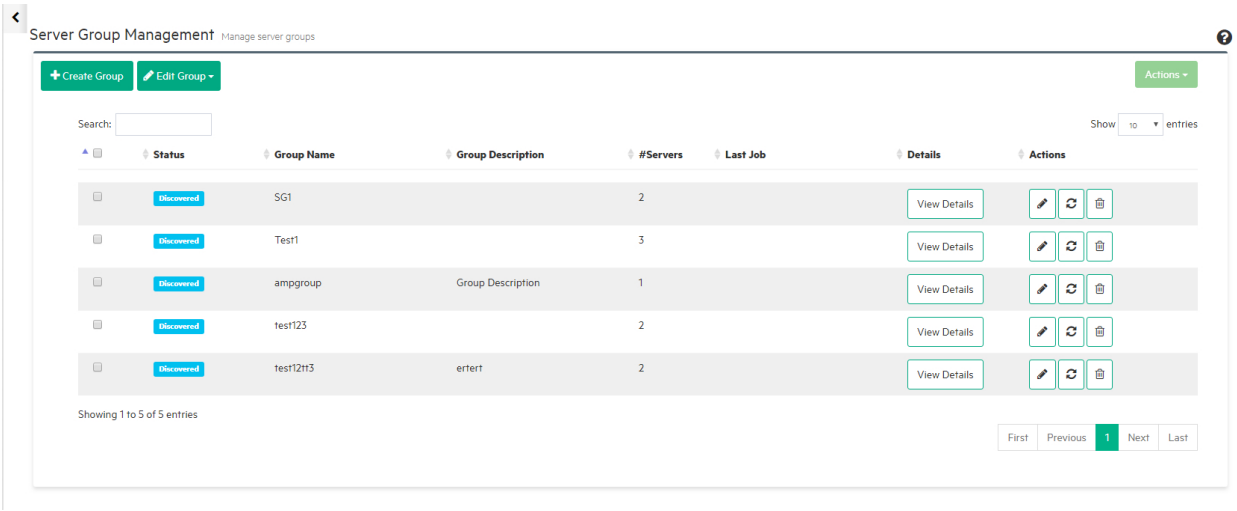
     e. Click **Apply**.

   - To manage multiple servers in an **Unmanaged**, rediscover the servers using one of the following methods:
     - Using IPv4 discovery from the **Discovery** page.
     - Using IPv4 discovery from the **Servers** page.
     - Using **CSV file upload** with the updated or valid credentials.
     - Selecting **Updating server credentials** and providing valid credentials on the Assets page.

Managing server groups

Viewing server groups

About this task



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. The following information is displayed for each server group.

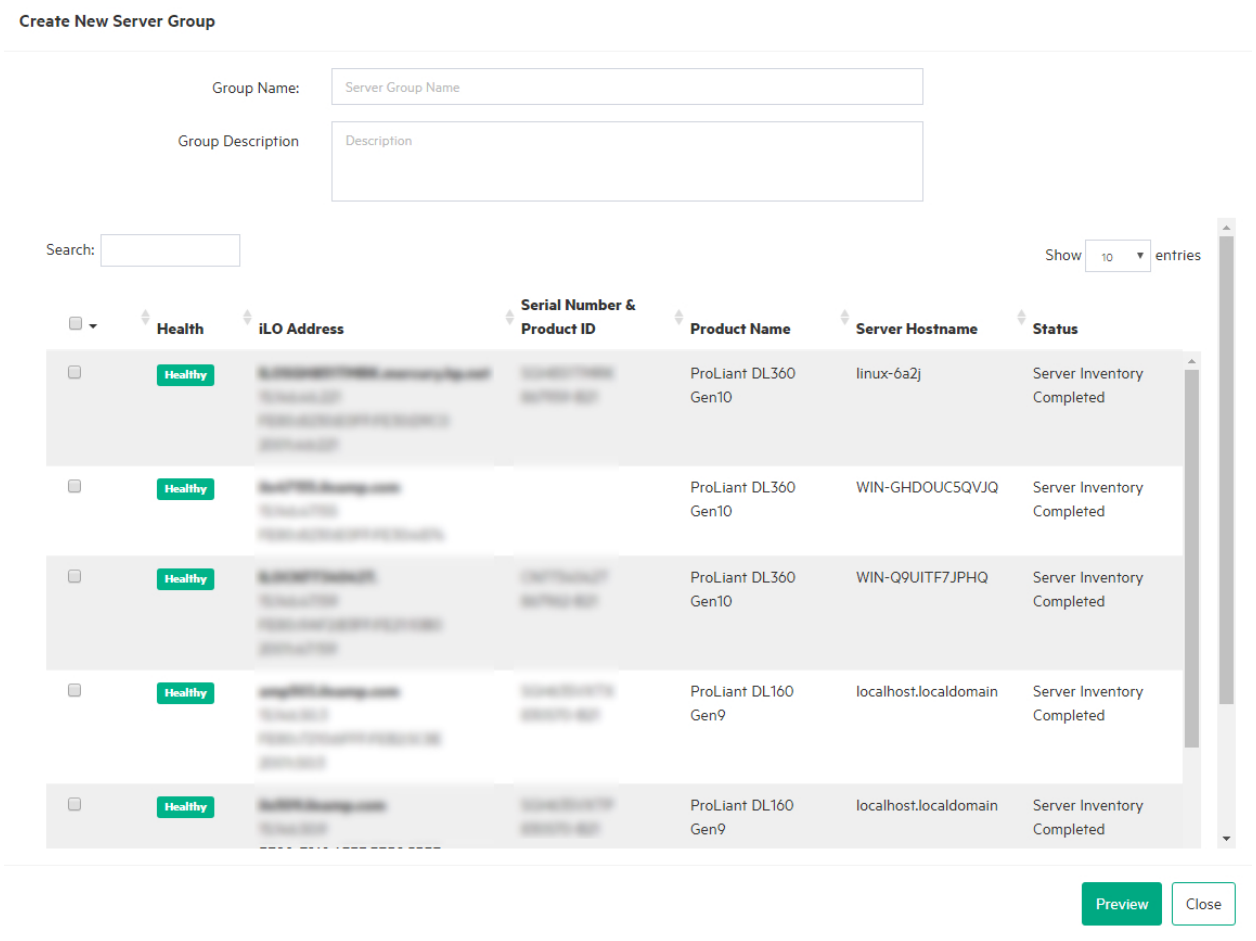
   - Status
   - Group Name
   - Group description
   - #Servers
   - Last Job
   - Details
   - Actions
     - Edit group description
     - Refresh group
     - Delete group

Creating a server group

Prerequisites

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

About this task



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 job 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 servers that are part of this group 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

Prerequisites

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

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

- Ensure that you are on HPE iLO 5 version 2.30 and above to update the core firmware from the GUI for the `*.fwpkg` file format.

About this task

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

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. Click to select **HTTP/HTTPS Share** or **File Upload** from the **Storage Type** menu.
5. Do one of the following:
   - For **HTTP/HTTPS Share**, enter the HTTP or HTTPS url to the ISO image. This URL can be an IPv4 or IPv6 address.
   - For **File Upload**, click **Choose File** to open the file explorer and choose the baseline stored on your local drive.

   NOTE: You can update the core firmware from the GUI for the `*.fwpkg`, `*.bin`, `*.vme`, `*.hex` and `*.flash` file formats for both **HTTP/HTTPS** and **File Upload** storage methods.[2]
6. Select the **TPM Override** check box to update TPM-enabled servers.
7. 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

[2] Power Management Controller, chassis firmware, and NVMe backplane files use the file extension `*.hex` . System Programmable Logic Device (CPLD) firmware file uses the file extension `*.vme`.

- 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 job starts. To see details about the job, click the **Job status** link in the message banner at the top of the page.

   When the refresh job 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

Prerequisites

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

About this task

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

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

About this task

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.

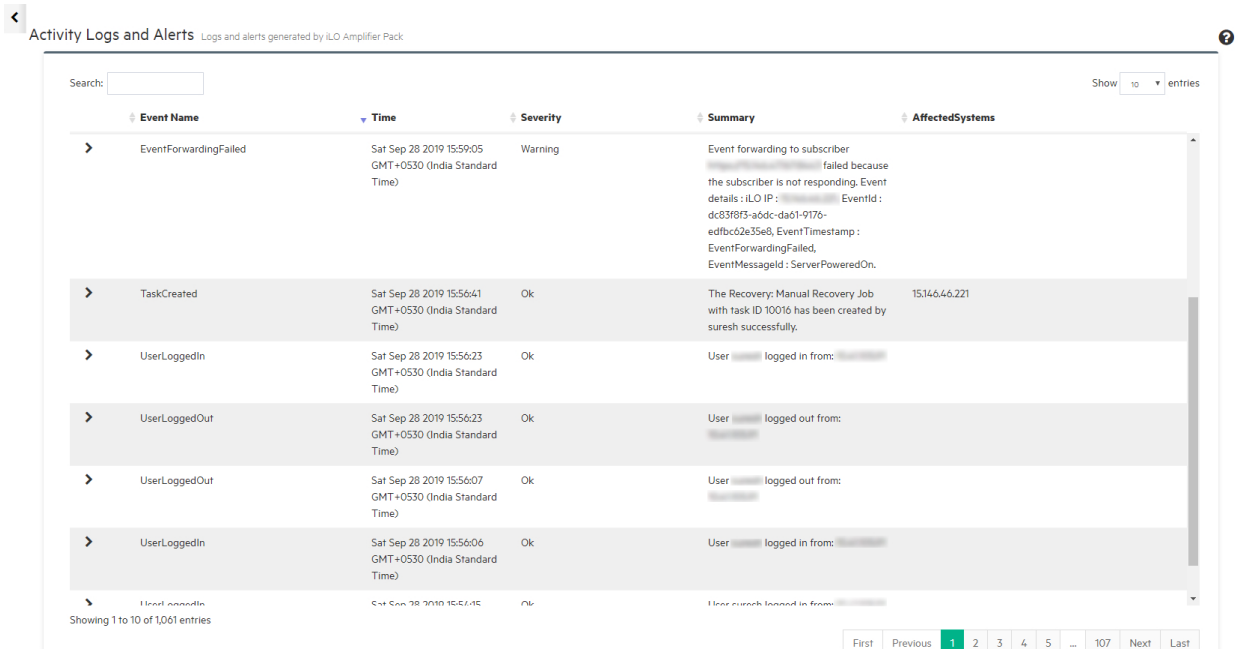
Viewing activity logs

Prerequisites

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

About this task

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



Procedure

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

   The event list displays 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 job

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

Prerequisites

- User privileges

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

About this task

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.

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.

Importing a firmware baseline

Prerequisites

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

About this task

Use the **Import Baseline** feature to make the baseline or custom SPP ISO image easily accessible for firmware updates. iLO Amplifier Pack supports up to 80 GB of baseline storage, which includes firmware, OS baseline files and downloaded components from HPE InfoSight. The percentage of space used is displayed at the top of the **Firmware Baseline** page. Additionally, you can delete the automatically downloaded components (from InfoSight) by clicking **Clear Component Repository**.

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)**, **HTTP/HTTPS**, or **File Upload** from the **Import Type** menu.
4. Do one of the following:
   - For **Network Share (NFS)**, enter the IPv4 or IPv6 address, mount path, and storage path.
   - For **HTTP/HTTPS**, enter the HTTP or HTTPS url to the ISO image. This URL can be an IPv4 or IPv6 address.
   - For **File Upload**, click **Choose File** to open the file explorer and choose the baseline stored on your local drive.
5. Click **Import** to import the ISO image or click **Cancel** to return to the **Firmware Baseline** page.

   The import progress can be seen on the **Jobs Status** 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 job.

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

Prerequisites

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

About this task

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.

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)**, **HTTP/HTTPS**, or **File Upload** from the **Import Type** menu.
4. Do one of the following:
   - For **Network Share (NFS)**, enter the IPv4 or IPv6 address, mount path, and storage path.
   - For **HTTP/HTTPS**, enter the HTTP or HTTPS url to the ISO image. This URL can be an IPv4 or IPv6 address.
   - For **File Upload**, click **Choose File** to open the file explorer and choose the baseline stored on your local drive.
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 job.

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**:

- 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 **https://www.hpe.com/info/ProLiantUEFI/docs**.

NOTE: For recovery administration of Gen10 servers and above, 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 **https://www.hpe.com/info/storage/docs**.
- **iLO Settings**—For more information, see the iLO documentation available from **https://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 job 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

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

- Configure User
- Configure Devices

About this task

Use these instructions to edit customizable server configuration baselines.

NOTE: Snapshot server configuration baselines cannot be edited.

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 **https://www.hpe.com/info/ProLiantUEFI/docs**.
   - **Boot Settings**
   - **Smart Storage Settings**—For more information, see the smart storage and logical drive documentation available from **https://www.hpe.com/info/storage/docs**.
   - **iLO Settings**—For more information, see the iLO documentation available from **https://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 job.

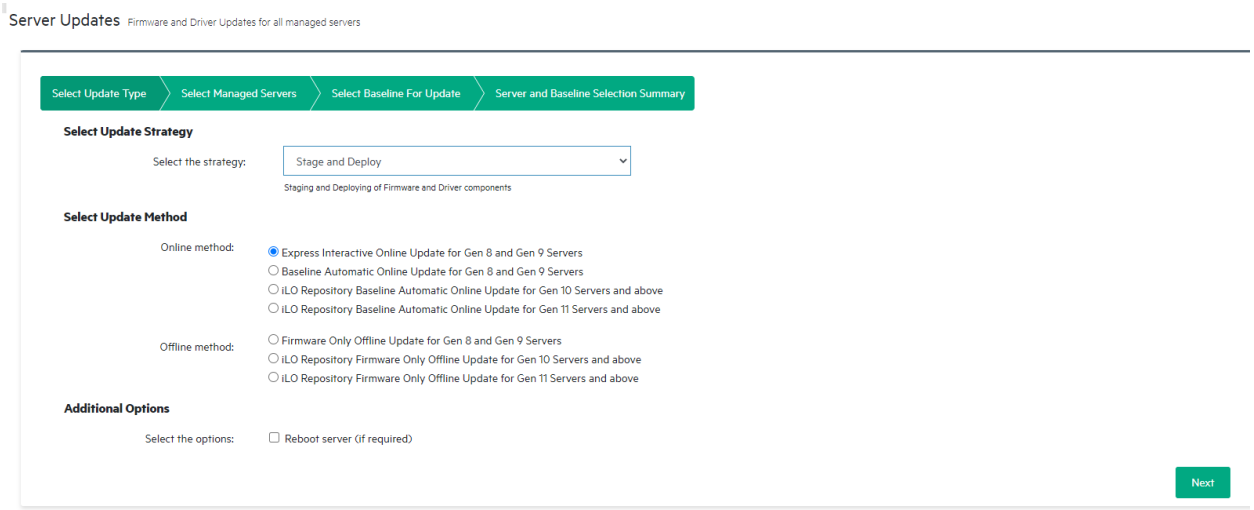
Server firmware and driver updates

iLO Amplifier Pack allows users to perform online and offline firmware updates for servers.

- **Online updates**: Online updates are performed when the server is in a powered on state. Updates are carried out for the operating system as well as firmware and driver components.
- **Offline updates**: Offline updates are performed when the server is in a powered off state. The server boots to the mounted media or SPP and the SUT performs the firmware updates. Once the update is complete, the server will continue to be in an offline state and must be rebooted by using an offline utility.

iLO Amplifier Pack version 1.40 and above offers users different update strategies to independently allow staging, staging and deploying, or only deploying previously staged firmware updates. Update components are staged during the non-maintenance window and then activated or deployed during the maintenance window. This reduces the overall time needed to perform the updates and helps increase scalability for deploying updates.

Users who need to perform firmware updates within a small maintenance window can now save time by staging the update and then deploying it later to reduce downtime.



iLO Amplifier Pack offers the following update strategies to perform server firmware updates:

- **Stage and Deploy**

  Firmware and driver components are first staged and then deployed immediately. This strategy offers an additional option to **Reboot server (if required)** after the update. The supported update methods are as follows:

  - Performing online firmware updates
    - **Performing an Express Interactive Online Update for Gen8 and Gen9 Servers**
    - **Performing a Baseline Automatic Online Update for Gen8 and Gen9 Servers**
    - **Performing an iLO Repository Baseline Automatic Online Update for Gen10 servers and above**
    - **Performing an iLO Repository Baseline Automatic Online Update for Gen11 servers and above**
  - Performing offline firmware updates

- **Performing a Firmware Only Offline Update for Gen8 and Gen9 servers**
- **Performing an iLO Repository Firmware Only Offline Update for Gen10 servers and above**
- **Performing an iLO Repository Firmware Only Offline Update for Gen11 servers and above**

- **Stage only**

  Firmware and driver components are staged only and not deployed. The staged components will persist even if the iLO Amplifier Pack appliance is rebooted. The supported update methods are as follows:

  - Performing online firmware updates
    - **Performing an Express Interactive Online Update for Gen8 and Gen9 Servers**
    - **Performing a Baseline Automatic Online Update for Gen8 and Gen9 Servers**
    - **Performing an iLO Repository Baseline Automatic Online Update for Gen10 servers and above**
    - **Performing an iLO Repository Baseline Automatic Online Update for Gen 11 Servers and above**

    Only one **Stage only** job can be performed when performing an Express Interactive online update or an iLO Repository Online update. Any additional jobs will be queued with the status **Pending**.

- **Deploy only**

  Firmware and driver components that are already staged using the **Stage only** strategy are deployed. You can choose additional options like **Clear the iLO repository after update** and **Reboot server (if required)**. Multiple **Deploy only** jobs can be performed on different servers in parallel. The supported update method is as follows:

  - **Deploying Firmware and Driver components which are already staged**

IMPORTANT: If an offline firmware update job is performed on a server with staged components, the staged components will be overwritten and the user will not be able to perform the **Deploy only** job.

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.
- SPP-based online/offline updates are not available for Edgeline and Moonshot devices. Use the Edgeline/Moonshot firmware and software component packs to update these devices from the **Servers** page in iLO Amplifier Pack. You can find information regarding device updates in the system firmware and software release notes at **http://www.hpe.com/info/edgeline-docs** and **http://www.hpe.com/info/moonshot/docs**.

IMPORTANT: Before commencing updates using the **Stage and Deploy** or **Stage only** strategies, ensure that AMS is running and SUT Mode is set to **AutoDeployReboot** or **AutoDeploy**. Once the server is staged, the SUT settings should not be modified.

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.

Based on the server inventory, iLO Amplifier Pack calculates and displays the components that require an update. Users can select and update specific components from this list. If there are any dependency failures, the dependency components have to be first resolved or unselected to proceed with the update. The baseline is mounted in the iLO Virtual Media and the list of components to be updated is then passed on to SUT which initiates the update procedure

- **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. Here, iLO Amplifier Pack does not need to calculate and create the list of components to be updated. iLO Amplifier Pack directly submits the request to SUT with the required baseline image, and SUT initiates the update process for all applicable components from the mounted baseline in iLO Virtual Media.

For a list of operating systems supported for performing online updates, see *Operating systems*.

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

Performing an Express Interactive Update

Prerequisites

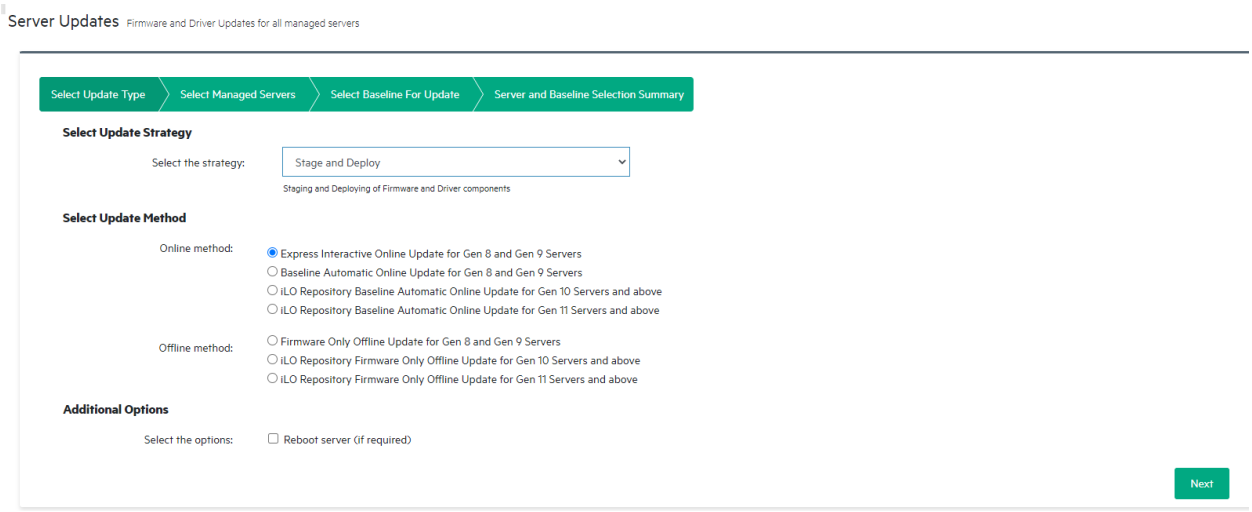
- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
- HPE iSUT (Integrated Smart Update Tools) v2.5.0 or later installed on all generation of servers
- AMS (iLO Agentless Management Service) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux. AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- 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

About this task



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the update strategy as either **Stage and Deploy** or **Stage only** based on your requirement.
3. Select the update method as **Express Interactive Online Update for Gen8 and Gen9 Servers** and then click **Next**.
4. Optional. If you select the update strategy as **Stage and Deploy**, you are presented with an additional option of rebooting the server if required.
5. Check the job status list to ensure that no jobs are running on the servers you want to update. Updates cannot be performed on servers while jobs are running. For more information about the job status list, see **Update Jobs Monitor**.
6. On the next page, 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.
7. 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.
8. 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.

9. Specify the number of parallel updates you want to perform in the **Batch Size** field and then click **Next**. Up to 30 parallel updates are supported if you are using an internal baseline. Up to 50 parallel updates are supported if you are using an external webserver.

10. Review your selections on the **Server and Baseline Selection Summary page** and then click **Begin Job**.

NOTE: During an update, actions performed on the selected servers are set to a pending state. However, you can perform actions on servers that are not being updated using the other pages of iLO Amplifier Pack.

11. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs.

12. When the status changes to **Waiting**, click  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.

13. 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.

14. 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 **https://www.hpe.com/info/sut-docs**.

The update process begins. If the update strategy was selected as **Stage only**, the following messages appear in succession:

- Online Update Job 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.

If the update strategy was selected as **Stage and Deploy**, the following messages are also displayed:

- **Installing**—Selected components are being deployed on the server.
- **Installed**—Selected components are deployed.

15. Reboot the server, if necessary. If you selected the additional option to **Reboot server (if required)** on the **Select update type** page, the server will be rebooted automatically.

    If the update strategy was selected as **Stage only**, when the installation has completed, the job status will change to **Staged**.

    If the update strategy was selected as **Stage and Deploy**, when the installation has completed, the job 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.

16. Click  to view the update parameters and the servers on which the job is run.
17. Click  to **view the job results**, and to see the components that were successfully staged/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 iSUT v2.5.0 or later installed on Gen8 and Gen9 servers
- AMS (iLO Agentless Management Service) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- Bootable baseline ISO image of the firmware update imported into iLO Amplifier Pack (for more information, see **Importing a baseline**).

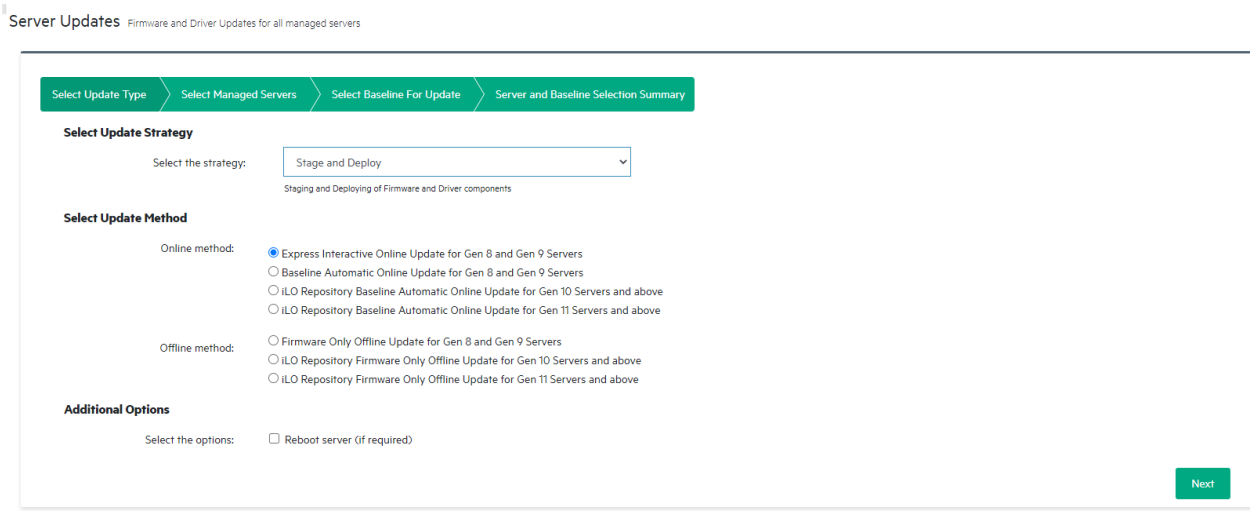
  Or

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

About this task



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the update strategy as either **Stage and Deploy** or **Stage only** based on your requirement.
3. Select the update method as **Baseline Automatic Update for Gen8 and Gen9 Servers** and then click **Next**.
4. Optional. If you select the update strategy as **Stage and Deploy**, you are presented with an additional option of rebooting the server if required.
5. Check the job status list to ensure that no jobs are running on the servers you want to update. Updates cannot be performed on servers while jobs are running. For more information about the job status list, see **Update Jobs monitor**.
6. On the next page, 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.
7. 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.
8. 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.

9. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 30 parallel updates are supported if you are using an internal baseline. Up to 50 parallel updates are supported if you are using an external webserver.
10. Review your selections on the **Server and Baseline Selection Summary page**, and then click **Begin Job**. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs.

    NOTE: During an update, actions performed on the selected servers are set to a pending state. However, you can perform actions on servers that are not being updated using the other pages of iLO Amplifier Pack.

    The update process begins. If the update strategy was selected as **Stage only**, the following messages appear in succession:

    - **Baseline Automatic Update Job 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.

    If the update strategy was selected as **Stage and Deploy**, the following messages are also displayed:

    - **Installing**—Selected components are being deployed on the server.
    - **Installed**—Selected components are deployed.

11. Reboot the server, if necessary. If you selected the additional option to **Reboot server (if required)** on the **Select update type** page, the server will be rebooted automatically.

    If the update strategy was selected as **Stage only**, when the installation has completed, the job status will change to **Staged**.

    If the update strategy was selected as **Stage and Deploy**, when the installation has completed, the job 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 refreshing the server inventory after the system has restarted.

12. Click  to view the update parameters and the servers on which the job is run.
13. Click  to **view the job results**, and to see the components that were successfully staged/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

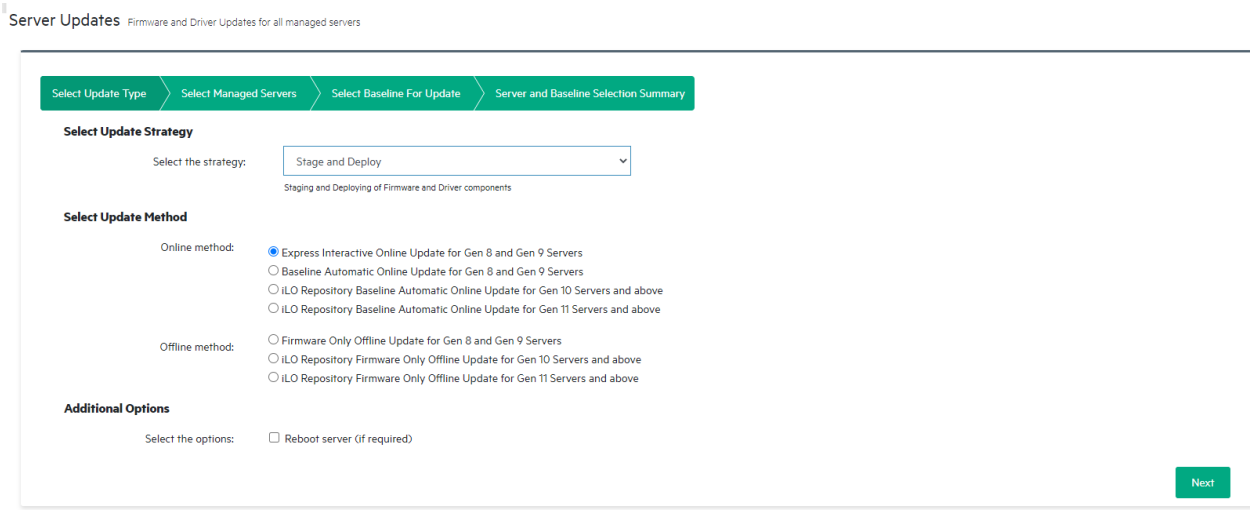
  Bootable baseline ISO image of the firmware update extracted to a shared HTTP/HTTPS location on the network and a dedicated web server for hosting SPP (HPE Support Pack for ProLiant) ISO images and files.

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.

About this task

Offline updates are performed with the server in the powered off state. The user selects a bootable ISO baseline image (SPP). iLO Amplifier Pack then orchestrates the update by configuring the update parameters, mounting the SPP, and setting the server boot order to boot to the mounted media. During the update process, the server boots to the mounted media and the boot environment in the baseline image is loaded with SUT. SUT then calculates the components to be installed and performs the update on the server.



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the update strategy as **Stage and Deploy**.
3. Select the update method as **Firmware Only Offline Update for Gen8 and Gen9 servers**, and then click **Next**.
4. Optional. Select from the additional option to **Force Downgrade** before moving to the next step.
5. Select the servers or the 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.
6. 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.
7. 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.

8. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 30 parallel updates are supported if you are using an internal baseline. Up to 50 parallel updates are supported if you are using an external webserver.

9. Review your selections on the **Server and Baseline Selection Summary page** and then click **Begin Job**. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs.

   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.

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

    NOTE: HPE recommends refreshing 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 and above 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.

iLO repository updates can perform firmware updates using either of the following options:

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

For a list of operating systems supported for performing online updates, see *Operating systems*.

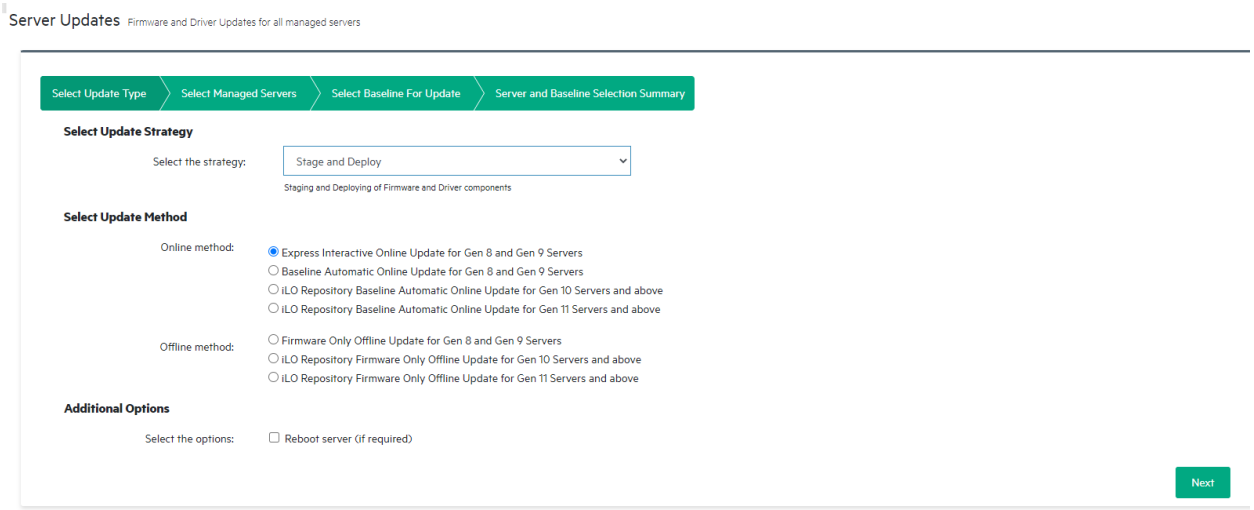
NOTE: iLO Amplifier pack v1.30 onwards supports updates on servers with VMWare ESXi OS version 6.0 and above.

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
  - iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
  - iLO 6 v 1.10 for Gen11 servers
  - The recommended SPP version is 2020.09.0 or later
- iSUT (Integrated Smart Update Tools) v2.5.0 or later installed on all generation of servers
- AMS and SUT should be running, and SUT Mode should be set to 'AutoDeployReboot' or 'AutoDeploy' to ensure that all components are updated.

About this task



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the update strategy as **Stage and Deploy** or **Stage only** based on your requirement.
3. Select the update method as **iLO Repository Baseline Automatic Online Update for Gen 10 servers and above** or **iLO Repository Baseline Automatic Online Update for Gen 11 servers and above** and then click **Next**.
4. Optional. Select from the additional options of **Force Downgrade**, **Clear iLO Repository after update** and **Reboot server (if required)** before moving to the next step. The options listed may change based on the update strategy selected.
5. 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.

6. 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.
7. 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**.
8. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 30 parallel updates are supported.
9. Review your selections on the **Server and Baseline Selection Summary page**, and then click **Begin Job**.

   The update process begins. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs. The job status will be displayed under the **Status** column.
10. Reboot the server, if necessary. If you selected the additional option to **Reboot server (if required)** on the **Select update type** page, the server will be rebooted automatically.

    If the update strategy was selected as **Stage only**, when the installation has completed, the job status will change to **Staged**.

    If the update strategy was selected as **Stage and Deploy**, when the installation has completed, the job status will change to **Completed**.

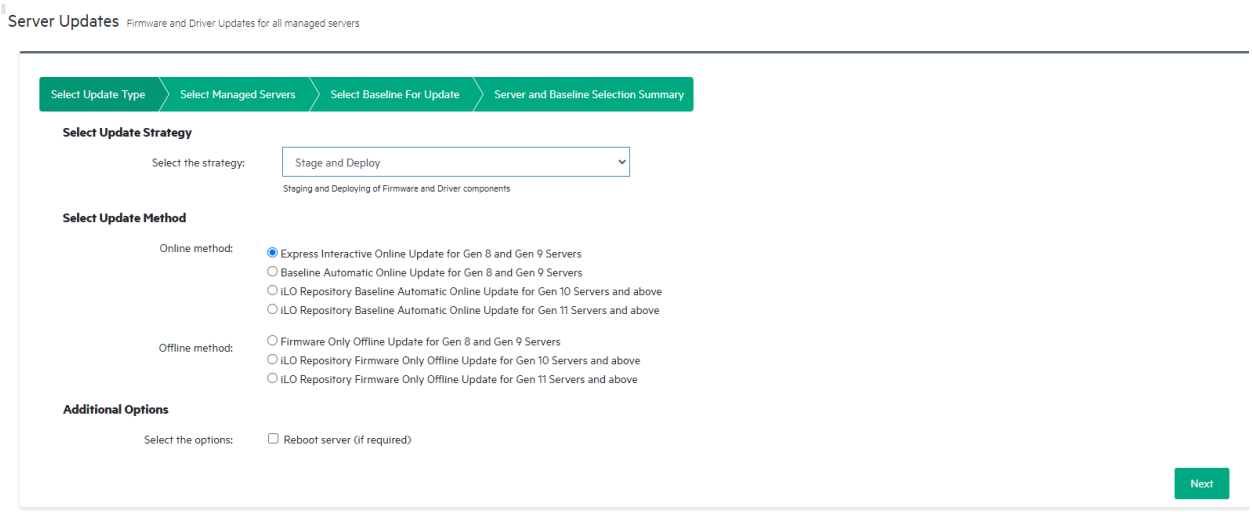
    NOTE: HPE recommends refreshing the server inventory after the system has restarted.
11. Click  to view the update parameters and the servers on which the job is run.
12. Click  to **view the job results**, and to see the components that were successfully staged or updated along with any pending user 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
  - iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
  - iLO 6 v1.10 for Gen11 servers
  - The recommended SPP version is 2020.09.0 or later

About this task



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the update strategy as **Stage and Deploy**.
3. Select the update method as **iLO Repository Firmware Only Offline Update for Gen 10 servers and above** or **iLO Repository Firmware Only Offline Update for Gen 11 servers and above** and then click **Next**.
4. Optional. Select from the additional options of **Force Downgrade**, and **Clear iLO Repository after update** before moving to the next step.

   IMPORTANT: If the Force Downgrade option is selected on servers set to High Security modes (HighSecurity/ FIPS mode), ensure not to downgrade the iLO version below 1.30.

5. 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.

6. 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.
7. 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**.
8. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 30 parallel updates are supported.
9. Review your selections on the **Server and Baseline Selection Summary page** and then click **Begin Job**.

   The update process begins. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs. The job status will be displayed under the **Status** column.
10. Reboot the server, if necessary. If you selected the additional option to **Reboot server (if required)** on the **Select update type** page, the server will be rebooted automatically.

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

For servers set to the HighSecurity/FIPS state, the job status will change to **Completed** with the message **iLO Repository Offline Update Completed. Results of High Security Mode update will be partial/incomplete**. The message will display **HighSecurity/FIPS** depending on the mode selected.

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

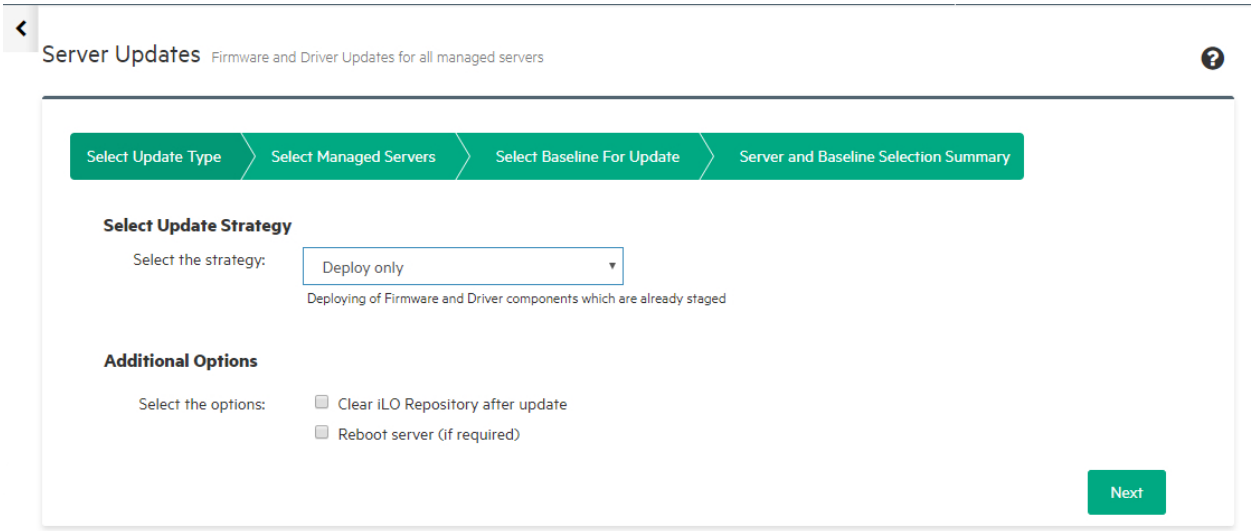
11. Click  to view the update parameters and the servers on which the job is run.
12. Click  to **view the job results**, and to see the components that were successfully updated along with any pending user actions.

Deploying already staged firmware and driver components

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure Devices
  - Configure User
- For servers set to the HighSecurity/FIPS state
  - iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
  - iLO 6 v1.10 for Gen11 servers
  - The recommended SPP version is 2022.03.1 and 2022.09.01.00 (4-Octet) or later
- iSUT 2.7.0, 2.8.0 for Windows and Linux and iSUT 2020.09.00, 2021.04.00 for ESXi 6.5/6.7/7.0 for Gen10 servers.
- iSUT 2.7.0, 2.8.0 for Windows and Linux and iSUT 2020.09.00, 2021.04.00 for ESXi 6.5/6.7/7.0 for Gen10 Plus servers.
- iSUT 3.0.0 for Windows and iSUT 2.9.0, 2.9.1, 2.9.1.0 for Linux and iSUT 2021.09.00, 2021.12.00 for ESXi 6.5/6.7/7.0 for Gen11 servers.
- AMS and SUT should be running, and SUT Mode should be set to 'AutoDeployReboot' or 'AutoDeploy' to ensure that all components are updated.
- Firmware and driver components are already staged

About this task



Procedure

1. Click **Firmware and Drivers** from the left navigation menu, and then click **Server Updates**.
2. Select the **Deploy only** strategy.
3. Optional. Select the additional options to **Clear iLO Repository after update** and **Reboot server (if required)**, and then click **Next**.
4. Select the servers that you want to update. Only servers that have already had their firmware staged will be displayed.

   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.
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. The baseline is already selected and staged during the stage only process. Specify the number of parallel updates you want to perform in the **Batch Size** field, and then click **Next**. Up to 200 parallel updates are supported.
7. Click **Begin Job**.

   The update process begins. Navigate to the **Update Jobs Monitor** page to monitor the status of the update job. Click the right arrow to reveal the job details and sub jobs. The job status will be displayed under the **Status** column.
8. Reboot the server, if necessary. If you selected the additional option to **Reboot server (if required)** on the **Select update type** page, the server will be rebooted automatically.

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

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

9. Click the  icon to view the update parameters and the servers on which the job is run.

10. Click  to **view the job results**, and to see the components that were successfully updated along with any pending user actions.

Update Jobs monitor

The **Update Jobs monitor** page lets you monitor the progress of firmware update jobs, and the results of completed jobs initiated from the **Server Updates** page. The following information is displayed:

- **Name**—Name of the job.
- **ID**—ID assigned to the job.
- **Status**—Progress of the selected job.
- **Message**—Information about the running job and the number of servers/server groups on which it is run.
- Optional: If a job is in the running state, you can click  to cancel the job.

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

Click the right arrow to reveal the job status details and sub jobs.

- **Created by**—Username of the person who initiated the job.
- **Started on**—Date and time of job creation
- **Last updated**—Date and time of last job update
- **Status**—Status of the job

The following details of the sub jobs are displayed. Some sub jobs can be expanded further.

- **Name**—Name of the job or the iLO, Host Name, or server group name on which the job is run
- **Status**—Status of the job
- **Message**—Information about the success or failure of the job

Click  to view the job parameters and the servers on which the job is run.

Click  to view the job results.

The following information will be displayed in the **Results** window for the **Stage and Deploy** and **Deploy only** strategies:

- **Component Name**—Name of the hardware that was updated.
- **Previous Installed version**—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.

The following information will be displayed in the **Results** window for the **Stage only** strategy:

- **Component Name**—Name of the hardware that was updated.
- **Installed Version**—Firmware version that was installed during the update.
- **Staged version**—Firmware version that was staged.
- **Staged Result**—Displays success or failure of the staging job.

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* at **https://www.hpe.com/support/infosight-servers-docs**.

All communication from the iLO to iLO Amplifier Pack is over HTTPS and is encrypted. iLO Amplifier Pack pulls the data from each server and pushes it to HPE InfoSight using the HTTPS protocol. For more details, see the *HPE Remote Device Access Install Guide*.

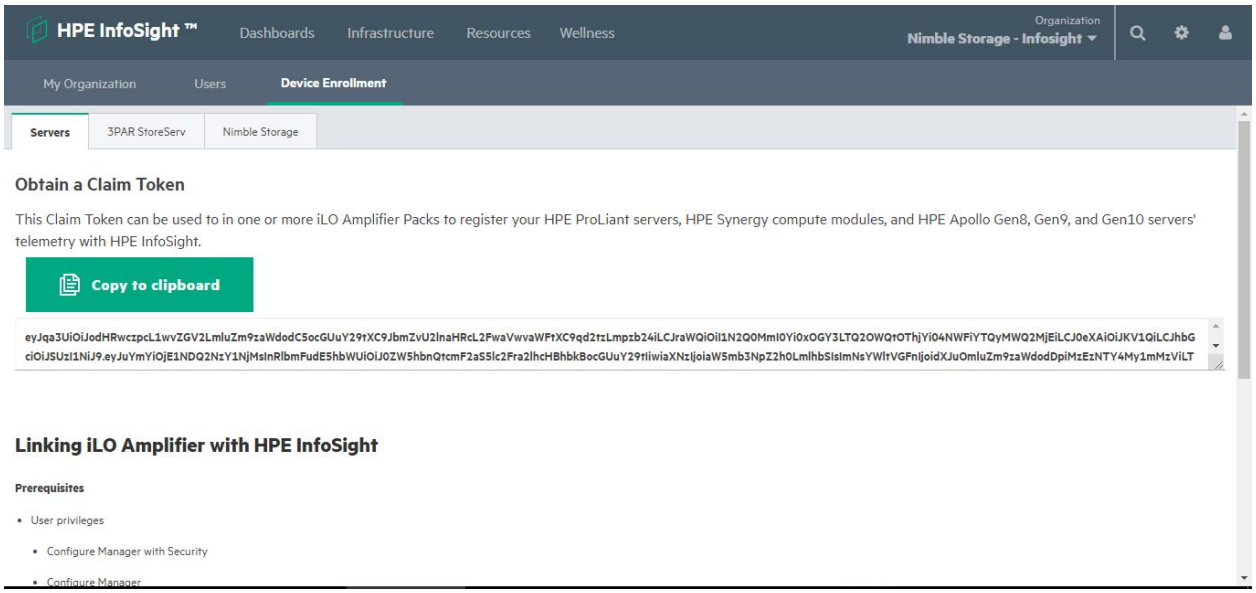
NOTE: HPE recommends using iLO 4 version 2.54 or later, iLO 5 version 1.37 or later, or iLO6 version 1.10 for HPE InfoSight.

Obtaining a claim token

Prerequisites

HPE Passport Login credentials

About this task



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 will have to be generated for registration when:

- You are linking 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.

Procedure

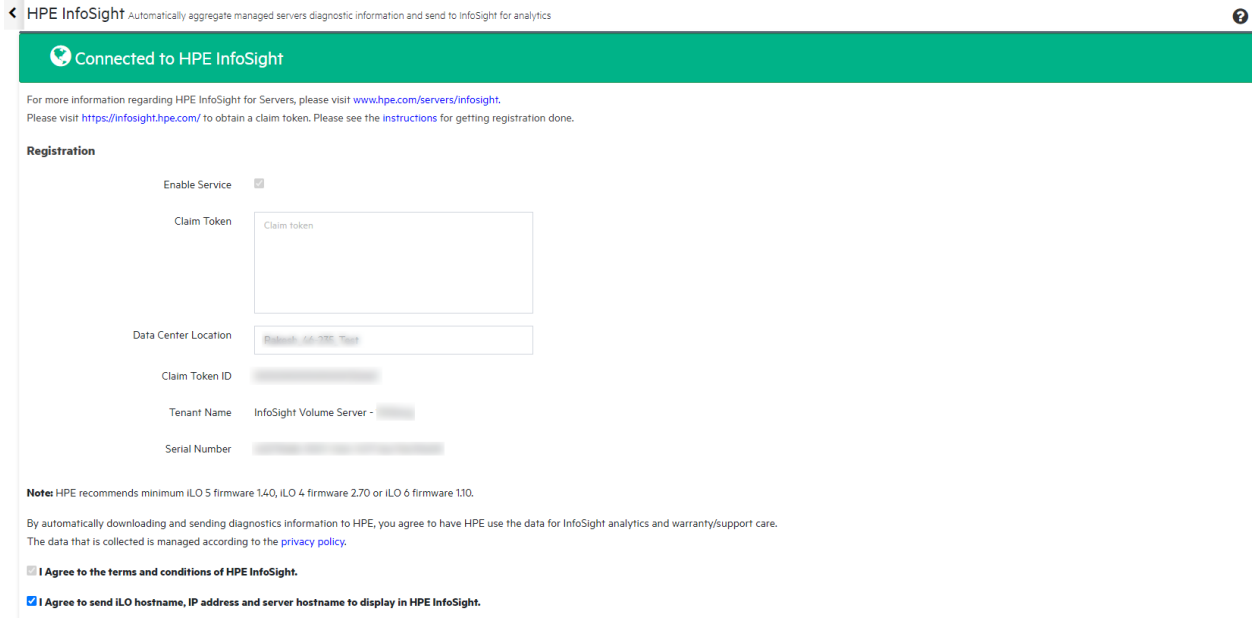
1. Go to the HPE InfoSight login webpage at **https://infosight.hpe.com/app/login**.
2. Login with your HPE Passport Login credentials.
3. Acknowledge the message bulletins and terms of use.
4. The dashboard is displayed. Click **Main Menu** > **InfoSight Administration** > **Device Enrollment**.
5. 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 Setup page** in iLO Amplifier Pack.

Linking iLO Amplifier Pack with HPE InfoSight

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
- DNS configured to allow iLO Amplifier Pack to connect with HPE InfoSight
- Firewall allows outbound connection to HPE InfoSight
- Proxy settings if required. See **Configuring network settings** for more details.

About this task



Procedure

1. Click **HPE InfoSight** on the left navigation menu, and then click **InfoSight Setup.**
2. Select the **Enable service** check box for activating 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.

   Optional: You can choose to send the iLO hostname, server hostname, and iLO IP address to HPE InfoSight as part of the heartbeat file by selecting the appropriate check box.
6. Optional: Select the **Enable Daily AHS Logs Collection** check box for activating the **Daily AHS Logs Collection Start Time** entry fields. You can enter a custom time value in the 24-hour time format to automatically schedule the daily transmission of the AHS files.
7. Optional: Click the links for more information about the sample **Heartbeat File**, **AHS Telemetry**, **FirmwareTelemetry**, 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, update iLO 4 to version 2.70 and iLO 5 to version 1.40. You can also use iLO6 version 1.10. Reboot the server after the firmware update for reduced AHS file sizes.
8. In the **InfoSight Triggered Server Operations** section, choose a policy to allow or disallow server operations that are triggered in HPE InfoSight.

   - Select **Allow InfoSight triggered server operations** if you want to allow server operations to be initiated from the HPE InfoSight user interface.
   - Select **Do not allow InfoSight triggered server operations** if you do not want any server operations to be initiated from the HPE InfoSight user interface.
9. Click the **Confirm** button to link iLO Amplifier Pack with HPE InfoSight.

10. 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**

11. 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**.

12. You can use the **Test Connection** button to test the connectivity between iLO Amplifier Pack and the `infosight.hpe.com` and `midway.ext.hpe.com` servers.

    For more information on resolving connectivity error messages, see the *iLO Amplifier Pack User Guide*.

    For more information on configuring the IP addresses for a successful connection, see the **Prerequisites for midway server connectivity**.

13. In case you are unable to resolve the InfoSight connectivity issues, you can also capture the network diagnostic logs and share it with support personnel. Click the **Diagnose Infosight Connectivity** button to begin the network diagnostic job.

    The network diagnostic job runs the following sub jobs:

    a. Resolves Midway and InfoSight servers and queries the IP list.

    b. Checks the connection/communication to Midway & InfoSight Servers.

    c. Checks the connection between iLO Amplifier Pack and four random Midway servers.

    d. Captures the client certificate.

    To see details about the job, click the **Job status** link in the message banner at the top of the page. When the diagnostic job finishes, click  to download the logs from the **Job status** page.

Prerequisites for midway server connectivity

IMPORTANT:

- If your enterprise DNS server does not forward DNS queries for external DNS names outside the network, you must configure your DNS server to add the entries for `midway.ext.hpe.com` and `infosight.hpe.com`. HPE highly recommends using the `midway.ext.hpe.com` and `infosight.hpe.com` DNS names to avoid future connectivity problems when the following IP addresses change. Open the firewall for outbound communication to all the midway servers either using the following DNS names or IP addresses along with `midway.ext.hpe.com` and `infosight.hpe.com`. These addresses are subject to change. If an intercepting proxy or firewall is configured, then the FQDN or IP address must enable the listed IP address connectivity to the midway servers.
- When you add entries to a DNS server, configure the onward and reverse lookups.

Ensure that the following IP addresses are open to allow iLO Amplifier Pack to communicate with HPE InfoSight and the midway servers:

IPv4 Address	IPv6 Address	Server Hostname	Alias
16.230.110.14	2602:fca3::e	p1lg501824.it.hpe.com	midway.ext.hpe.com
16.230.110.13	2602:fca3::d	p1lg501825.it.hpe.com	midway.ext.hpe.com
16.230.110.17	2602:fca3::11	p1lg501826.it.hpe.com	midway.ext.hpe.com
16.230.110.28	2602:fca3::12	p1lg503763.it.hpe.com	midway.ext.hpe.com
16.230.110.29	2602:fca3::13	p1lg503764.it.hpe.com	midway.ext.hpe.com
16.228.110.20	2602:fca3:10::14	p2lg501868.it.hpe.com	midway.ext.hpe.com
16.228.110.21	2602:fca3:10::15	p2lg501869.it.hpe.com	midway.ext.hpe.com
16.228.110.22	2602:fca3:10::16	p2lg501870.it.hpe.com	midway.ext.hpe.com
16.228.110.11	2602:fca3:10::17	p2lg504047.it.hpe.com	midway.ext.hpe.com
16.228.110.27	2602:fca3:10::18	p2lg504048.it.hpe.com	midway.ext.hpe.com

NOTE: To establish connection to HPE InfoSight, the entries for `midway.ext.hpe.com` and `infosight.hpe.com` are automatically added to the `/etc/hosts` files. The automatic addition happens when your Enterprise DNS server is unable to forward the DNS queries for external DNS names.

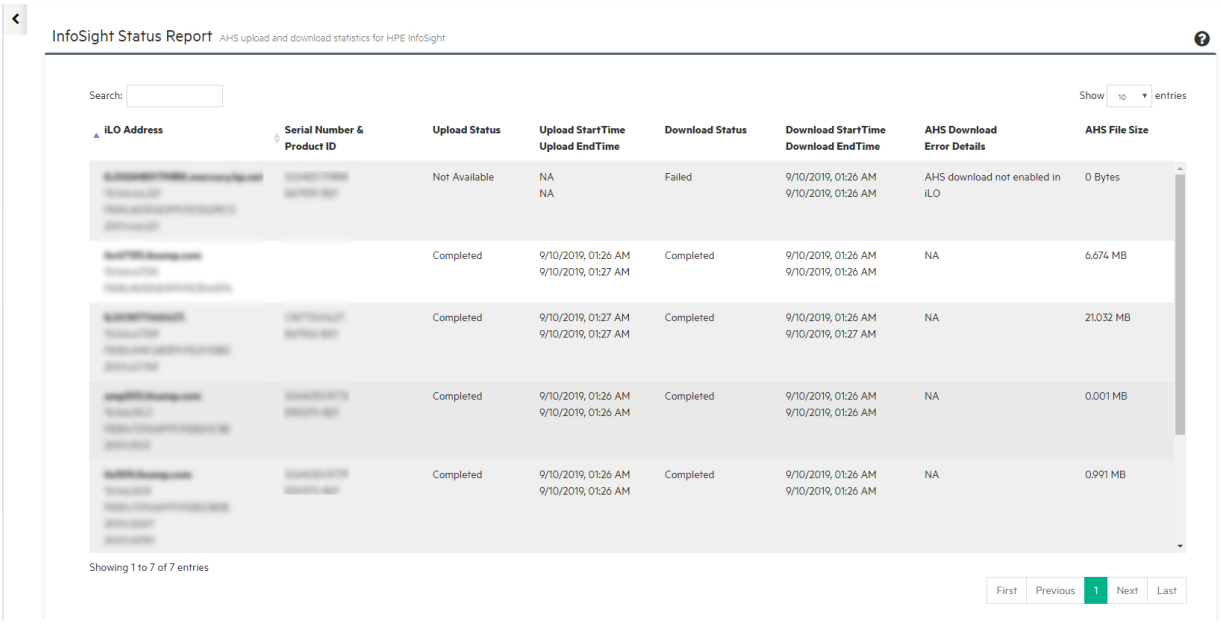
Viewing the InfoSight Status Report and sending AHS data

Prerequisites

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

- Configure Devices
- Login

About this task



Procedure

1. Click **HPE InfoSight** on the left navigation menu, and then click **InfoSight Status Report**.
2. This page provides information about the AHS upload and download statistics for HPE InfoSight for each server.

   The following information appears for each managed server:

   - **iLO Address**—The network IP address of the iLO subsystem.
   - **Serial number & Product ID**—The server serial number, which is assigned when the system is manufactured, and the product ID of the server.
   - **Upload status**—The upload status of the AHS log.
   - **Upload StartTime**—The upload start time of the AHS log.
   - **Upload EndTime**—The upload end time of the AHS log.
   - **Download Status**—The download status of the AHS log.
   - **Download StartTime**—The download start time of the AHS log.
   - **Download EndTime**—The download end time of the AHS log.
   - **AHS Download Error Details**—The download error details when the AHS log download fails.

     For more information on resolving AHS download error messages, see *AHS download error troubleshooting*.
   - **AHS File Size**—The file size of the AHS log.

3. Options on this page:

- Enter a value in the **Search** box and press the enter key to search for specific information.
- 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.

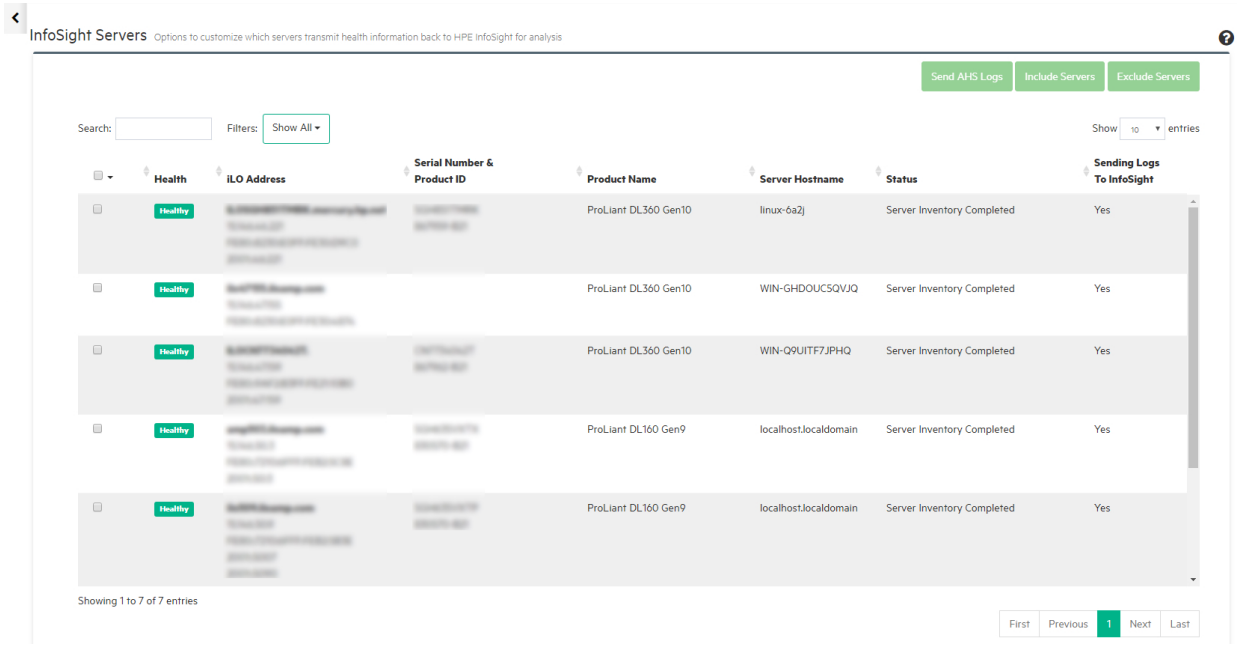
4. Click **Export to CSV** to download the information in CSV format.

Managing servers for InfoSight

Prerequisites

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

About this task



Procedure

1. Click **HPE InfoSight** on the left navigation menu, and then click **InfoSight Servers**.
2. This page allows you to select which servers can transmit health information back to HPE InfoSight.

   The **InfoSight Servers** page displays 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 FQDN (fully qualified domain name) of the iLO, along with the IPv4 and IPv6 addresses (and port, when applicable) of the iLO subsystem.
- **Serial number and Product ID**—The server serial number, which is assigned when the system is manufactured, and the product ID of the server.
- **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.

- **Sending Logs to InfoSight**—If the AHS logs for the server are sent to HPE InfoSight.

3. Options on this page:
   - Enter a value in the **Search** box and press the enter key to search for specific information.
   - 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.
4. To exclude servers from sending their AHS logs to HPE InfoSight, perform the following steps:
   a. Select the servers whose AHS log transmissions are to be stopped, and then click the **Exclude Servers** button. A new pop-up window appears listing the applicable servers.

      NOTE: Only servers that are already linked to HPE InfoSight will be listed for exclusion.

   b. Review the list of servers selected, and then click **Apply**.
5. To allow excluded servers to send their AHS logs to HPE InfoSight, perform the following steps:
   a. Select the servers whose AHS log transmissions are to be initiated, and then click the **Include Servers** button. A new pop-up window appears listing the applicable servers.

      NOTE: An error message will be displayed if the AHS logs for the selected servers are already being sent to HPE InfoSight.

   b. Review the list of servers selected and then click **Apply**.
6. You can also refresh the AHS data for any server on the HPE InfoSight portal from this page. Select the servers whose AHS data you want to prioritize during the next AHS transmission cycle, and then click the **Send AHS Logs Now** button. A new pop-up window appears listing the various servers.
7. Review the list of servers selected and then click **Apply**.
8. You can view the jobs created for any of the above actions on the **Jobs Status** page.

Viewing HPE InfoSight Recommendation Alerts

Prerequisites

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

About this task

iLO Amplifier Pack can receive hotfix or patch recommendations from HPE InfoSight. Users can then act on these recommendations or choose to dismiss them. These alerts can also be forwarded through email or IFTTT.

Procedure

1. Click **HPE InfoSight** on the left navigation menu, and then click **InfoSight Recommendation Alerts**.
2. The following information appears for each recommended alert:
   - **Severity**—The severity of the alert.
   - **iLO Address**—The network IP address of the iLO subsystem.
   - **Serial number & Product ID**—The server serial number, which is assigned when the system is manufactured, and the product ID of the server.
   - **Alert Name**—The type of the alert.
   - **Updated Time**—The last updated time of the alert.
   - **Acknowledged**—Displays if the alert was acknowledged or not.
3. Options on this page:
   - Enter a value in the **Search** box and press the enter key to search for specific information.
   - 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.
4. Click a row for viewing more information about the alert.
   - The **Overview** tab provides the following details about the alert:
     - **Serial Number**—The server serial number, which is assigned when the system is manufactured.
     - **Product ID**—The product ID of the server.
     - **Host Name**—The hostname assigned to the server.

- **Server Name**—The server name.
- **Severity**—The severity of the alert.
- **Category**—The category of the alert.
- **Description**—The description of the alert.
- **Updated Time**—The last updated time of the alert.
- **Summary**—A summary of the alert.
- **Recommendation**—The recommended action for the alert.
- **Acknowledged**— Displays if the alert was acknowledged or not.

- The **Components** tab provides the following information about the firmware or software components:
  - **Component Name**—Name of the affected component.
  - **Installed Version**—The currently installed version of the component.
  - **Available Version**—The latest available version of the component.
  - **Recommendation**—The severity of the recommendation.
  - **Link**—The download link to the recommended version of the component.

5. To acknowledge alerts, perform the following steps:

   a. Select the alerts to be acknowledged, and then click . A new pop-up window appears asking you to confirm your action.

   b. Review the number of alerts, and then click **Apply**.

NOTE:

- A maximum of 100 alerts can be selected at a time to be acknowledged.
- Once an alert is acknowledged, the value in the **Acknowledge** column changes to **Yes**. The alert cannot be selected to acknowledge again.
- This action is only available to users with a privilege of **Configure Manager** and above.

---

6. Click  for downloading the alert information in CSV format.
7. To clear acknowledged or unacknowledged alerts, perform the following steps:

   a. Select the alerts to be cleared, and then click . A new pop-up window appears asking you to confirm your action.

   b. Review the number of alerts, and then click **Apply**.

NOTE:

- A maximum of 100 alerts can be selected at a time to be cleared.
- Clearing the alert notifications from this page will not clear the alerts seen in HPE InfoSight.
- This action is only available to users with a privilege of **Configure Manager** and above.

Monitoring InfoSight jobs

Prerequisites

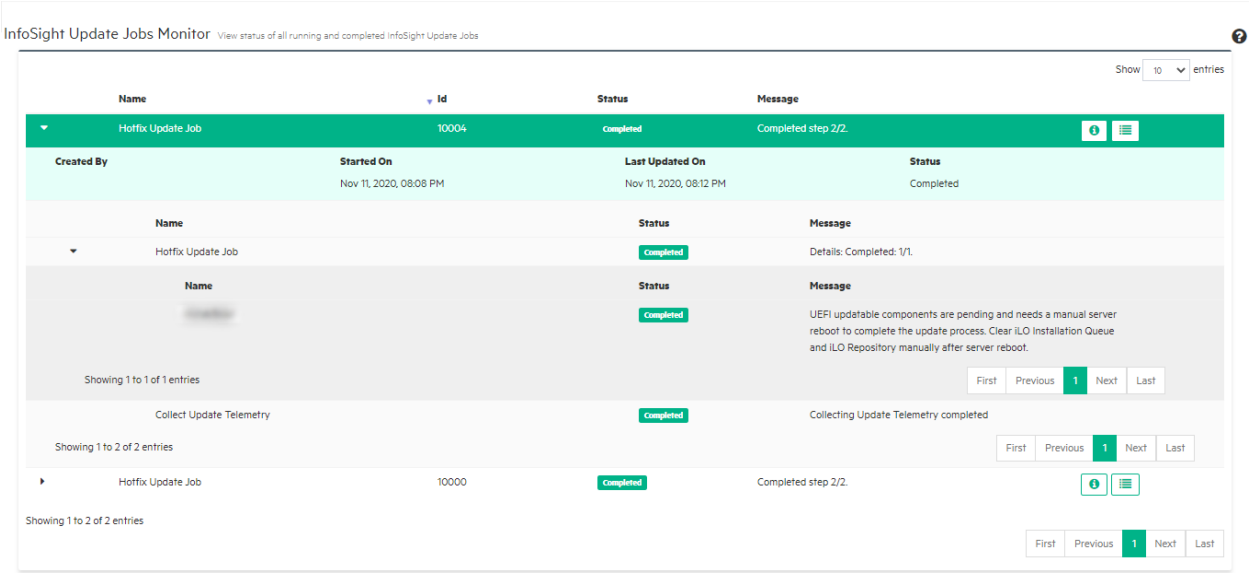
- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- The **Allow InfoSight triggered server operations** option must be selected on the **InfoSight Setup** page.

About this task

iLO Amplifier Pack 1.80 and above allows customers to perform hotfix updates from HPE InfoSight. Users can now update multiple components on servers that have been discovered and added to the inventory. Once the update is initiated in HPE InfoSight, iLO Amplifier Pack automatically downloads the required hotfix components and performs the update. These update jobs can be observed and cancelled from the **InfoSight Jobs Monitor** page.

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

NOTE: Updates initiated from HPE InfoSight can only be performed on Gen10 servers and above.



Procedure

1. Click **HPE InfoSight** on the left navigation menu, and then click **InfoSight Jobs Monitor**.
2. The following information appears for each running or completed update job:

   - **Name**—Name of the job.
   - **ID**—ID assigned to the job.
   - **Status**—Progress of the selected job.
   - **Message**—Information about the running job.
   - Optional: Click  to view the job parameters and the servers on which the job is run. If a job is in the **pending** state, you can click  to cancel the job.

     NOTE:

     - Users must have a privilege of Configure Devices and above to cancel any pending hotfix update jobs.
     - Only the jobs which are in pending state can be cancelled during the update process.
     - If jobs are cancelled from HPE InfoSight, the status of the job on the **InfoSIght Jobs Monitor** page will also display as **Cancelled**.

   Click the right arrow to reveal the job status details and sub jobs.

   - **Created by**—Username of the person who initiated the job.
   - **Started on**—Date and time of job creation
   - **Last updated**—Date and time of last job update
   - **Status**—Status of the job

   The following details of the sub jobs are displayed. The sub jobs can be expanded further.

   - **Name**—Name of the job being run
   - **Status**—Status of the job
   - **Message**—Information about update and the action being performed on the server.

   Once the job is complete, click <results_icon> to view the details of the components that were updated for each server.
3. Options on this page:

   - 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.

HPE Unified Supportability Pipeline

The Unified Supportability Pipeline feature enables an increased coverage for wellness alerts and automatic support case creation. Unified Supportability Pipeline feature helps you to manage automatic support case creation. A case is created automatically when a service event occurs. Previously, in HPE InfoSight for Gen9 and Gen 10 servers, only six service events were supported. With the implementation of Unified Supportability Pipeline, the automatic support case creation capability can now be used for all the iLO 4, iLO 5, and iLO 6 generated service events for Gen8, Gen9, Gen 10, and Gen 11 servers. The Unified Supportability Pipeline feature will be available to all the managed servers in the organization.

For all managed servers in an organization, this feature is delivered through a prepackaged add-on service pack in the HPE iLO Amplifier pack and it enables remote support settings in iLO. This feature will be enabled from HPE InfoSight when you configure the **Wellness Configuration** page.

NOTE: Once this feature is enabled, you cannot disable this feature either from HPE iLO Amplifier Pack or HPE InfoSight. The only way to disable the feature is to exclude servers from connecting to HPE InfoSight.

Salient Features

- Simplified HPE InfoSight user experience for wellness configuration.
- Wellness configuration provisioned only for admin users.
- Automatically configures remote support on iLO when Wellness Configuration on HPE InfoSight is enabled.
- Periodic check of iLO settings for the required remote support configuration.
- Add-on service to receive eRS events (from iLO) and send AHS file that contains the eRS events to HPE InfoSight.

Supported Platforms

All servers and platforms that HPE iLO Amplifier Pack supports can use this feature.

The following servers with iLO 4, iLO 5, and iLO6 are supported:

- HPE ProLiant Gen8 and later servers
- HPE ProLiant Gen10 servers
- HPE ProLiant Gen11 servers
- HPE Alletra 4K Gen11 servers

NOTE: HPE Unified Supportability Platform is offered for HPE InfoSight managed servers and not for manually uploaded logs.

Working with HPE Unified Supportability Pipeline add-on services

Prerequisites

- Ensure that you are connected to HPE InfoSight to enable this add-on service.
- Ensure that you have Wellness Dashboard Configuration set on HPE InfoSight user interface to enable the plugin in iLO Amplifier Pack.

About this task

Procedure

1. In the details pane, click **USP**.

   HPE Unified Supportability Pipeline add-on service window appears.

2. Toggle the **Quick Filters** option to show or hide the eRS disable entries.

3. The following fields appear:

   - iLO Address
   - Serial Number & Product ID
   - Product Name
   - iLO Type and iLO Version
   - Status
   - Connection Type
   - eRS Enabled
   - Host Server

4. Click **Export to CSV** to export all the values into a comma-separated value spreadsheet.

   NOTE: If you are not connected to HPE InfoSight, the add-on service page prompts you to connect to HPE InfoSight.

Baseline Compliance report

The Baseline 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.

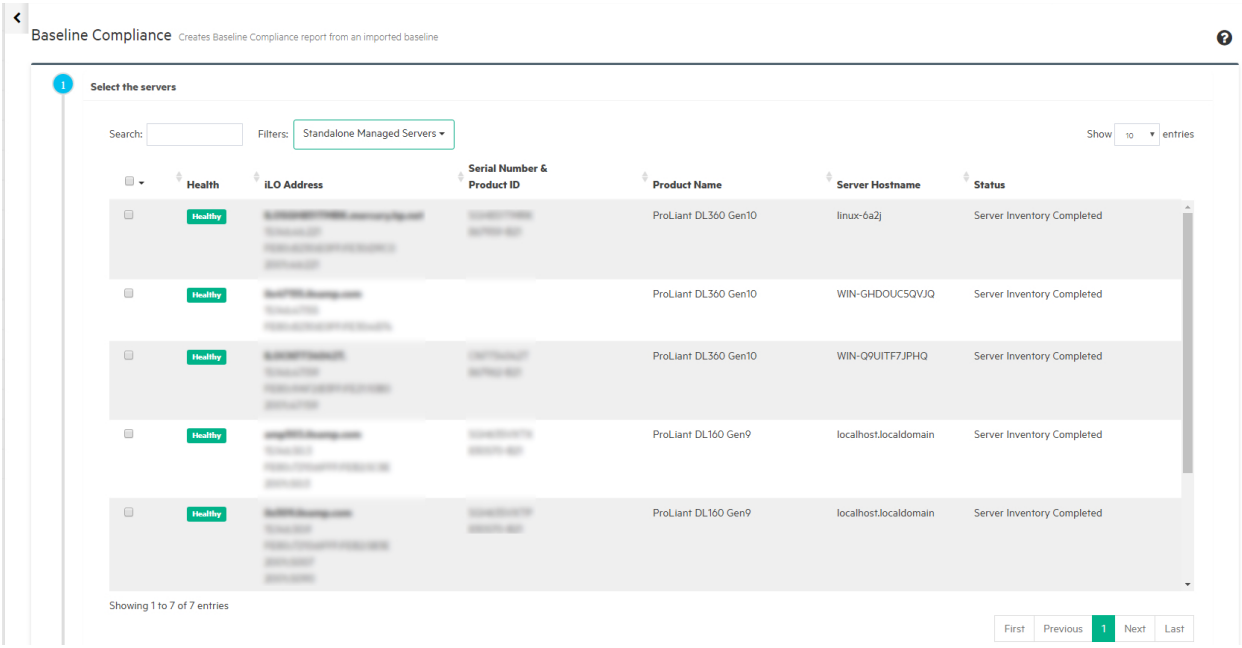
iLO Amplifier Pack allows the users to generate Baseline Compliance reports for multiple servers at a time.

Creating the Baseline 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 a Baseline Compliance report

About this task



Procedure

1. From the left navigation menu, select **Baseline Compliance Report** > **Create Baseline 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.
3. Select the Baseline for creating the Baseline Compliance Report.
4. To view **Baseline Compliance Summary**, click **Begin Job**.

5. To create the Baseline Compliance report, click **Start**.
6. A job is created, which may show one or all the following states of job:
   - **Pending**
   - **Running**
   - **Complete**
   - **Exception**
   - **Failed**
7. The Baseline Compliance report is generated.

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

Viewing the Baseline Compliance report

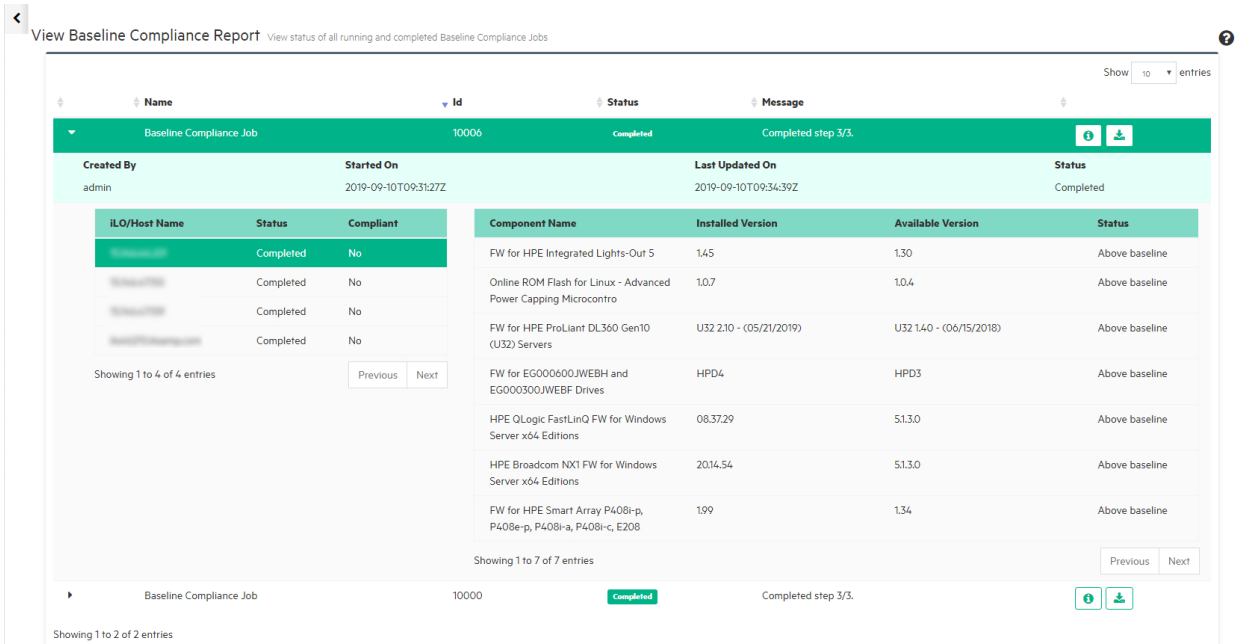
Prerequisites

The Baseline Compliance report is generated.

For detailed information, see **Creating the Baseline Compliance report**.

About this task

NOTE: If HPE ProLiant Gen8 servers, HPE ProLiant Gen9 servers, HPE ProLiant Gen10 servers, and HPE ProLiant Gen10 Plus servers (except HPE ProLiant Gen11 servers) are selected together when creating a Baseline Compliance Report, three separate reports are created – one for Gen8 and Gen9 servers, one for Gen10 and Gen10 Plus servers, and the other for Gen11 servers.



Procedure

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

   The table with servers provides the following details:

   - **Compliant**—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.

   A Baseline 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. Click  to view the baseline and the servers on which the job is run.
4. Click  to export the report to a CSV file.

Recovery Management

Introduction

The Server System Restore feature works with iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers to recover 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

- iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
- For servers set to the HighSecurity/FIPS state
  - iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
  - The recommended SSP version is 2020.09.0 or later.
- 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 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
- For recovery administration of Gen10 servers and above, 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.

IMPORTANT: In HPE Integrated Lights-Out 5 (iLO 5) v1.40, a Downgrade Policy Feature was added that has the option to permanently disallow downgrades. The automatic recovery will not complete as expected under all the following conditions:

- The iLO Downgrade Policy is set to **Permanently Disallow Downgrades**.
- The iLO/BIOS version in the System Recovery Set is older than the currently installed version.
- The firmware is corrupted.

To ensure that the System Recovery completes as expected, update the System Recovery Set with the latest or currently installed component versions from iLO Amplifier Pack using "Assign Recovery Policy" or directly from iLO 5.

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 Jobs 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, or Gen10 Plus servers running iLO 5 v2.10 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 job 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**.

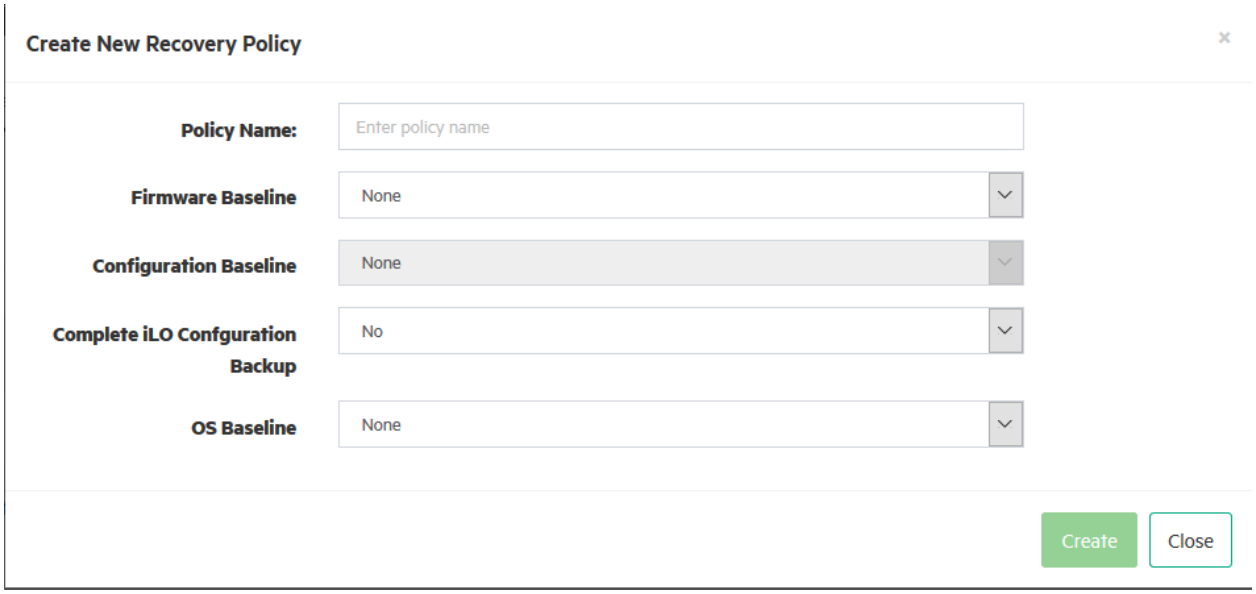
Recovery policy

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.

About this task



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 5 v1.37 and later, or Gen10 Plus servers running iLO 5 v2.10 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 must 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

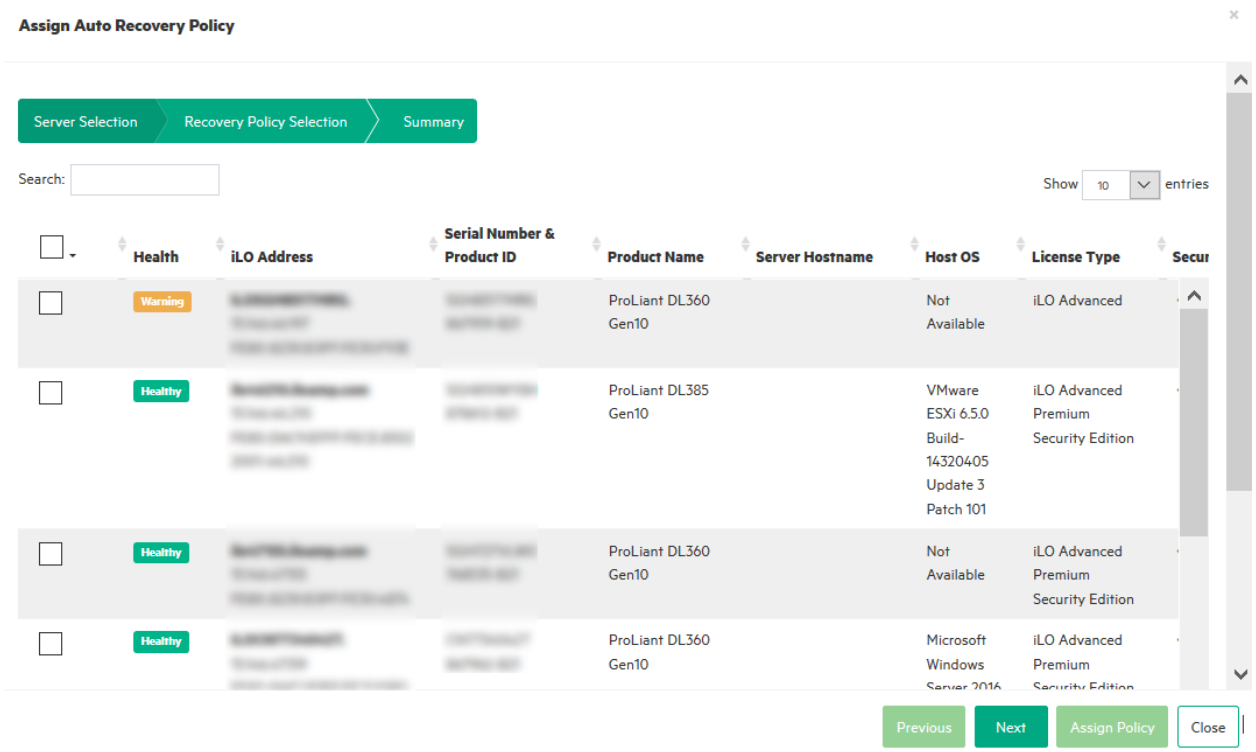
The **Recovery Administration** page lists all the Gen10 servers and above with an iLO Advanced license that are managed by iLO Amplifier Pack. When a firmware corruption occurs on a system, iLO detects this corruption and sends out an event to iLO Amplifier Pack. iLO Amplifier Pack then initiates the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

Assign a recovery policy

Prerequisites

- User privileges
  - Configure Manager with Security
- iLO 5 v2.30 or later for Gen10 servers and iLO 5 v2.30 or later for Gen10 Plus servers
- iLO Advanced license

About this task



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:

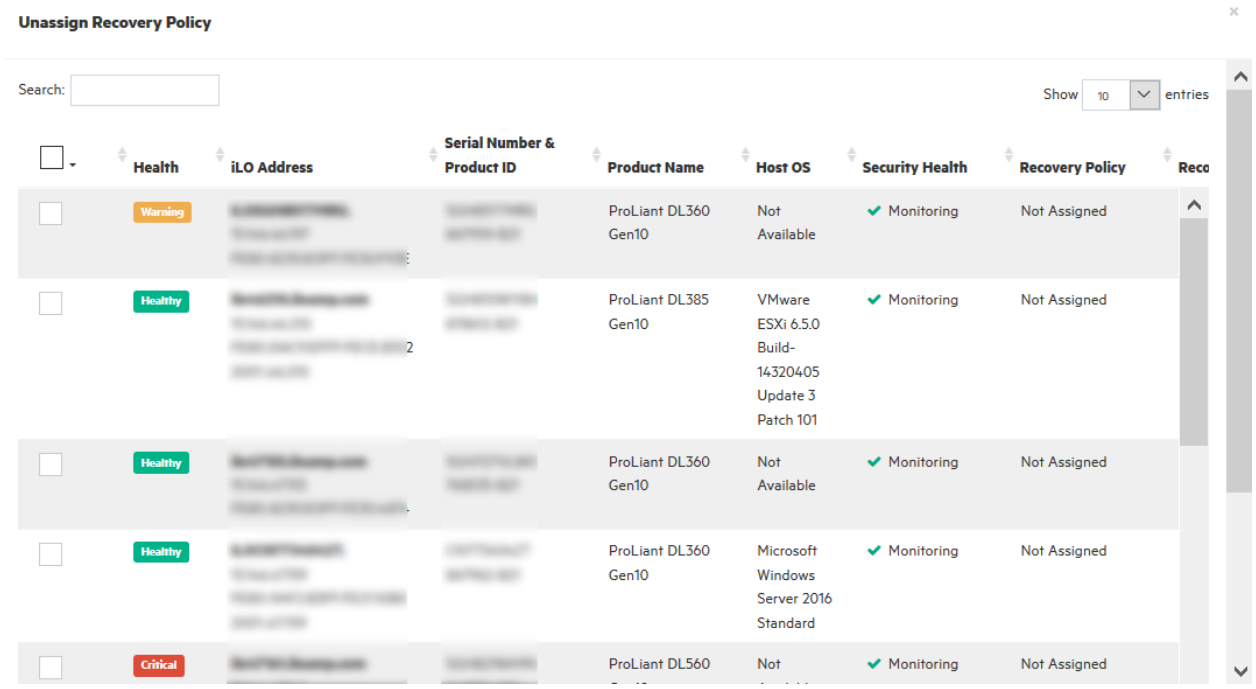
Firmware + Configuration + Operating System

Unassign a recovery policy

Prerequisites

- User privileges
  - Configure Manager with Security

About this task



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

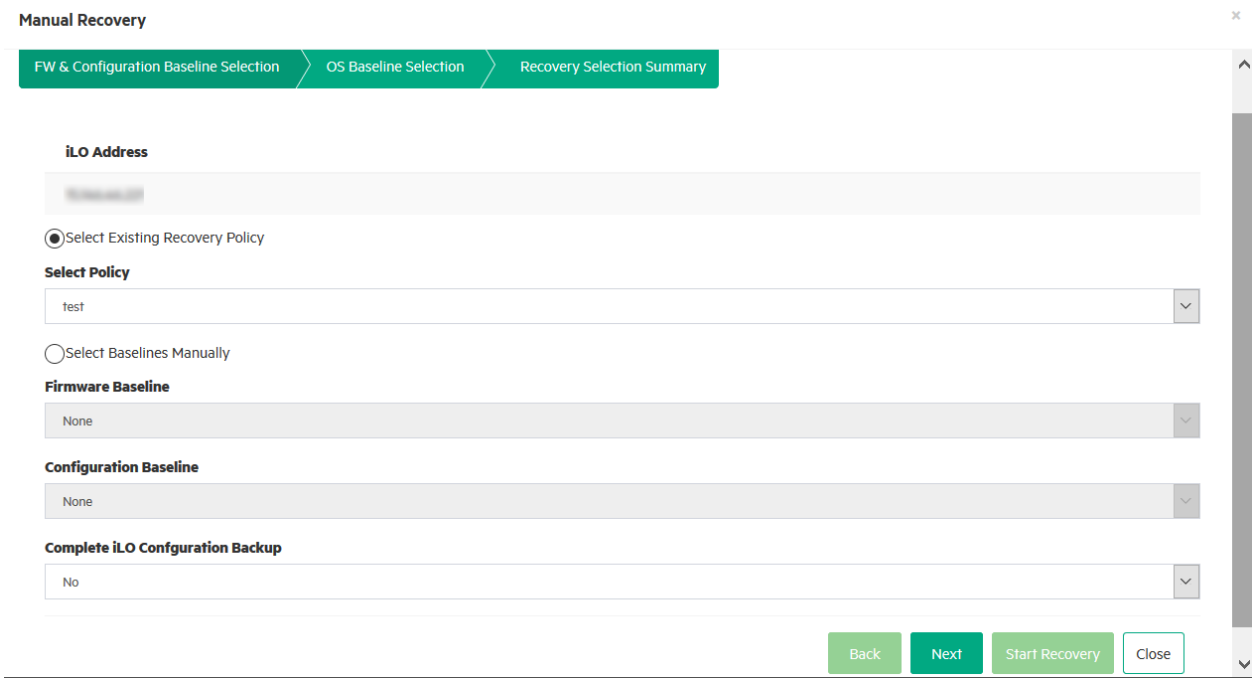
Prerequisites

- User privileges
  - Configure Manager with Security

About this task

The **Recovery Administration** page lists all the Gen10 servers and above 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.



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 job 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 job on the **Recovery Jobs 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.

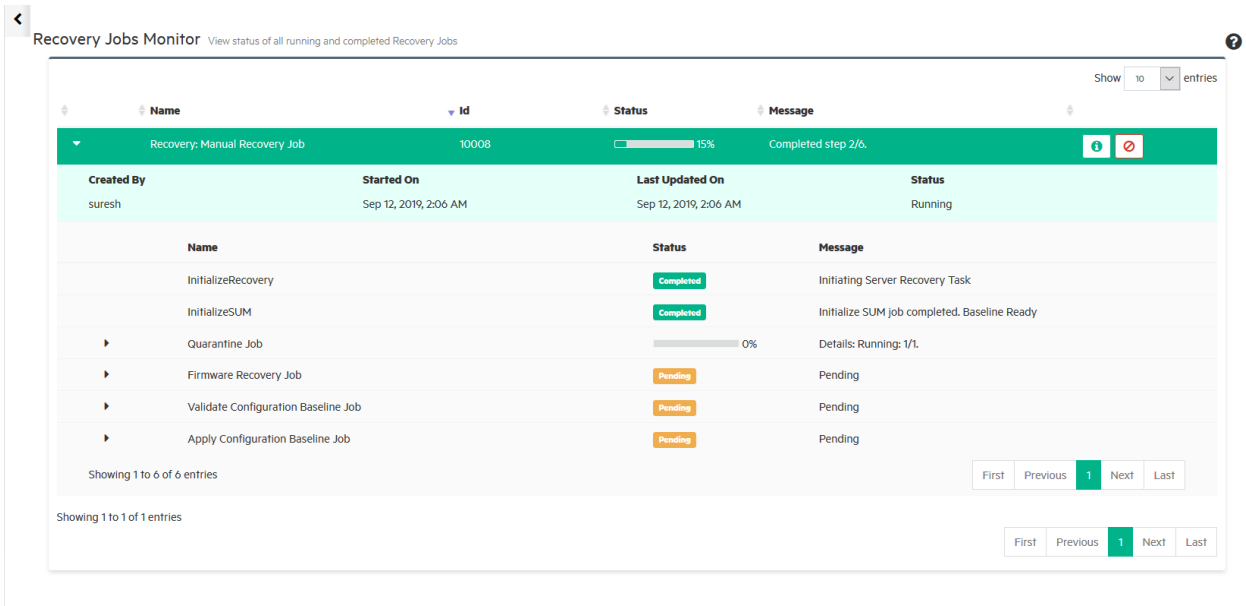
   Check the progress of the quarantine job on the **Recovery Jobs Monitor** page.

Monitoring recovery jobs

Prerequisites

- User privileges
  - Configure Manager with Security

About this task



Procedure

1. Click **Recovery Management** from the left navigation menu, and then click **Recovery Jobs Monitor** to view all the status of all running and completed jobs.
2. Click the right arrow to see the details of the job 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.

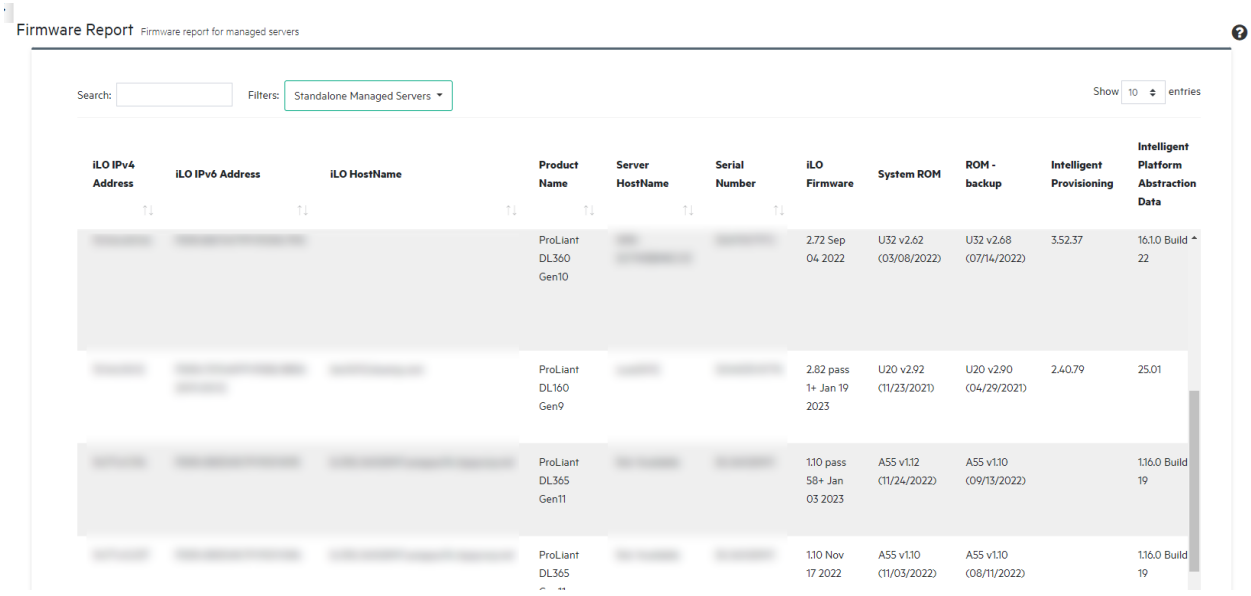
The recovery process may take a while to complete. See the **Activity Logs and Alerts** page for the status of the recovery process.

Viewing the firmware report

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- AMS (iLO Agentless Management Service) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- AMS v2.50 or later for Windows, AMS v3.1.0 or later for Linux, and AMSv2022.11.01 or later for ESXi

About this task



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 press the enter key to search for specific information.
- Use the **Filters** menu 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

- Physical drives information:
  - Physical drives - Name
  - Physical drives - Version

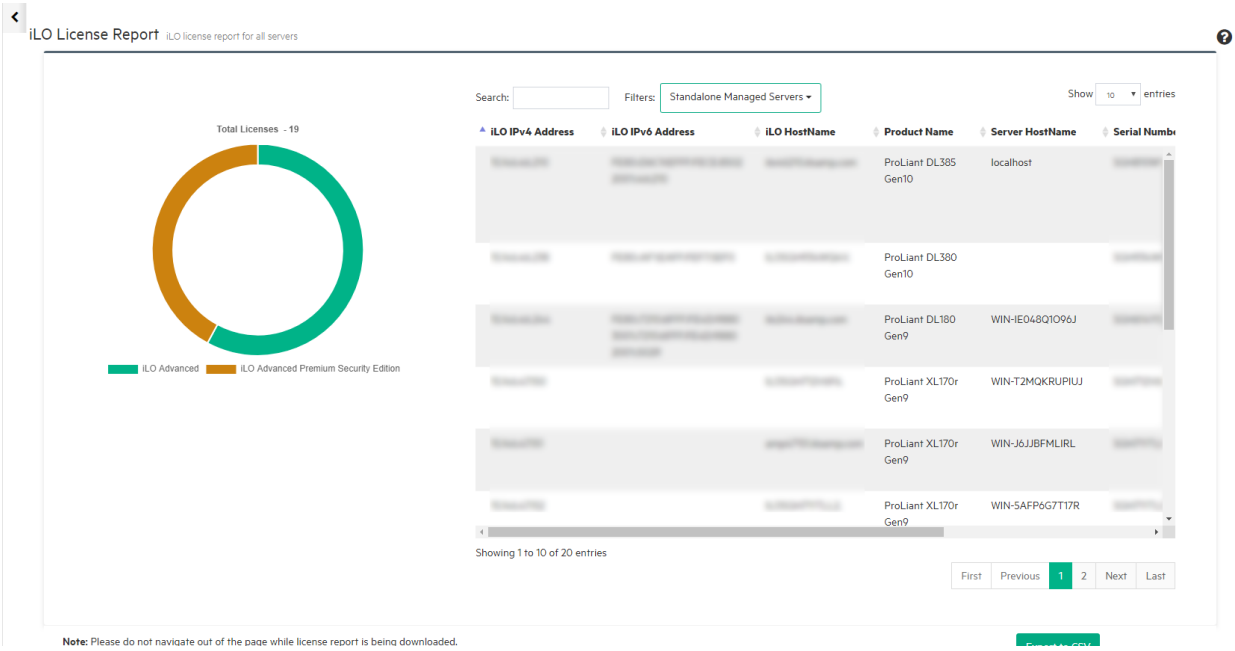
Viewing the iLO license report

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager
  - Configure User
  - Configure Devices
  - Login
- For Gen8 and Gen9 servers: AMS (iLO Agentless Management Service) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- For Gen10 and Gen10 plus servers: AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- For Gen11 servers: AMS v2.50 or later for Windows, AMS v3.1.0 or later for Linux, and AMSv2022.11.01 or later for ESXi

About this task

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



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**—The key provided with the iLO license.
   - **License**—The license level purchased with the iLO
     - iLO Standard
     - iLO Essentials
     - iLO Scale-Out
     - iLO Advanced
   - **License Type**—The level of the 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.

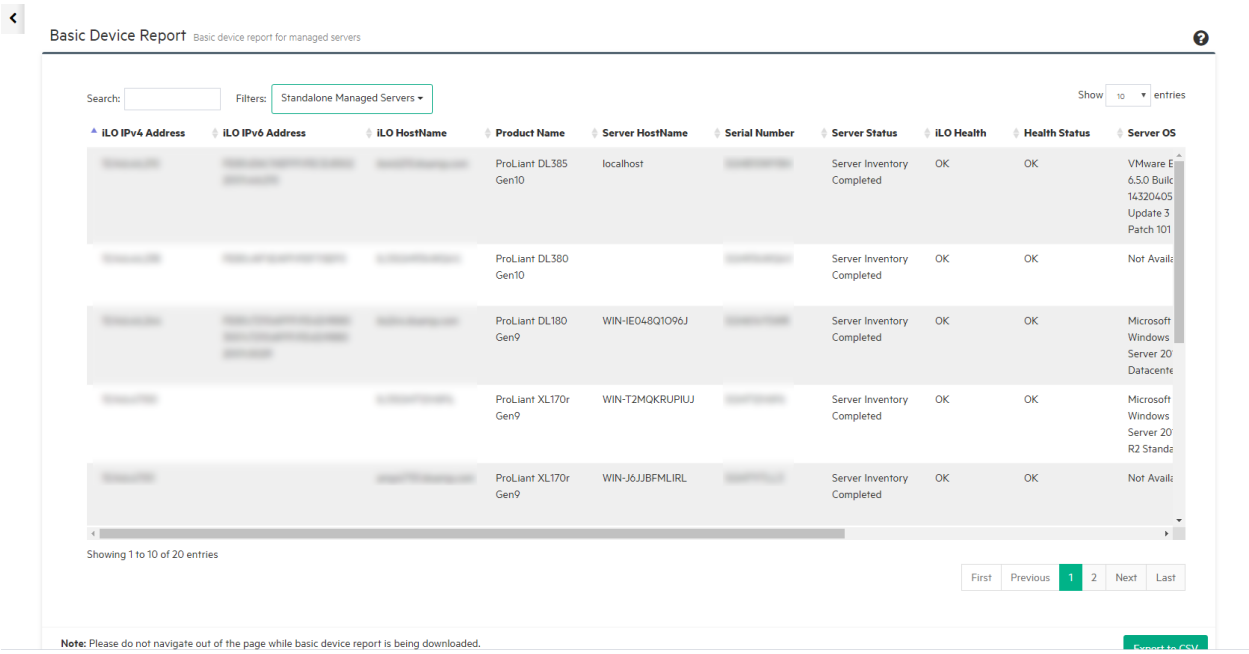
3. Options on this page:
   - Enter a value in the **Search** box and press the enter key to search for specific information.
   - Use the **Filters** menu to customize the display.
   - Use the **Show entries** menu to choose the number of entries to display per page.
   - Use the navigation buttons 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 the 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) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- For Gen10 and Gen10 plus servers: AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- For Gen11 servers: AMS v2.50 or later for Windows, AMS v3.1.0 or later for Linux, and AMS v2022.11.01 or later for ESXi.

About this task



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.
   - **iLO Health**—The health of the iLO firmware and other subsystems.
   - **Health Status**—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.
   - **Server Groups**—The server groups that the server is part of.

3. Options on this page:

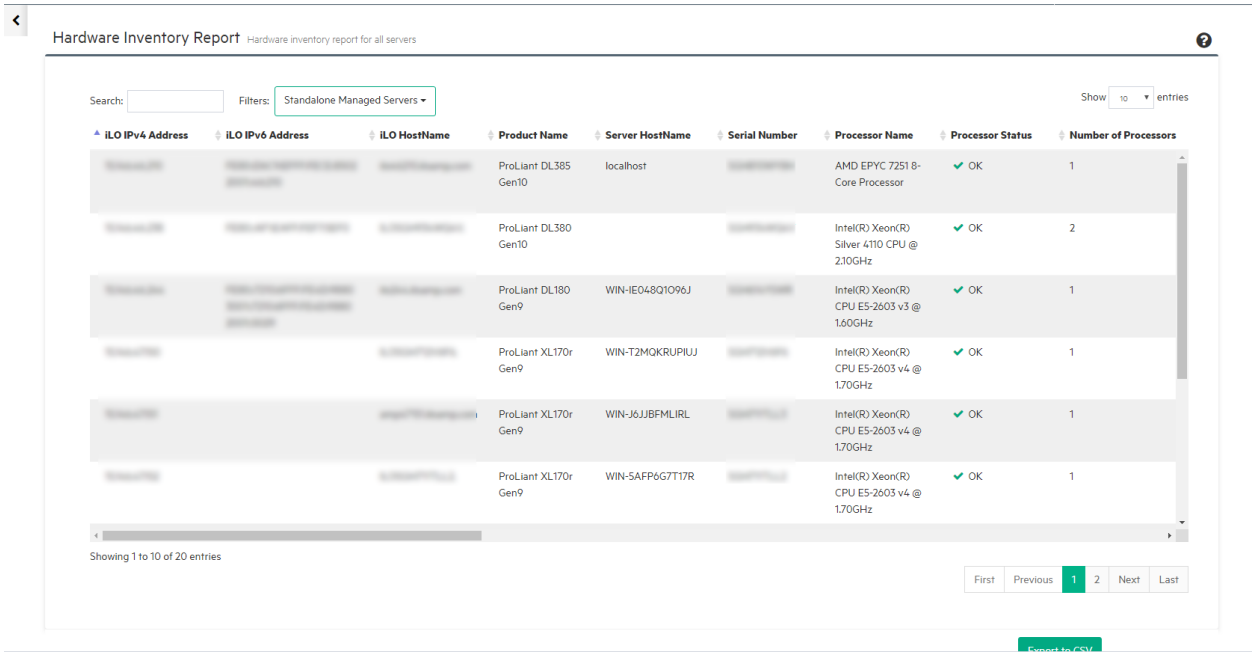
- Enter a value in the **Search** box and press the enter key to search for specific information.
- Use the **Filters** menu to customize the display.
- Use the **Show entries** menu to choose the number of entries to display per page.
- Use the navigation buttons to view the first, previous, next, or 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) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- For Gen10 and Gen10 plus servers: AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- For Gen11 servers: AMS v2.50 or later for Windows, AMS v3.1.0 or later for Linux, and AMSv2022.11.01 or later for ESXi

About this task



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 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.
   - 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
     - Fan Health
     - Fan Redundancy
     - Number of Power Supplies
     - Power Supplies Health
     - Power Supply Redundancy
   - Miscellaneous inventory
     - BIOS/Hardware Health
     - Network Health
     - Storage Health
     - Smart Storage Battery Health
     - Temperatures

3. Options on this page:

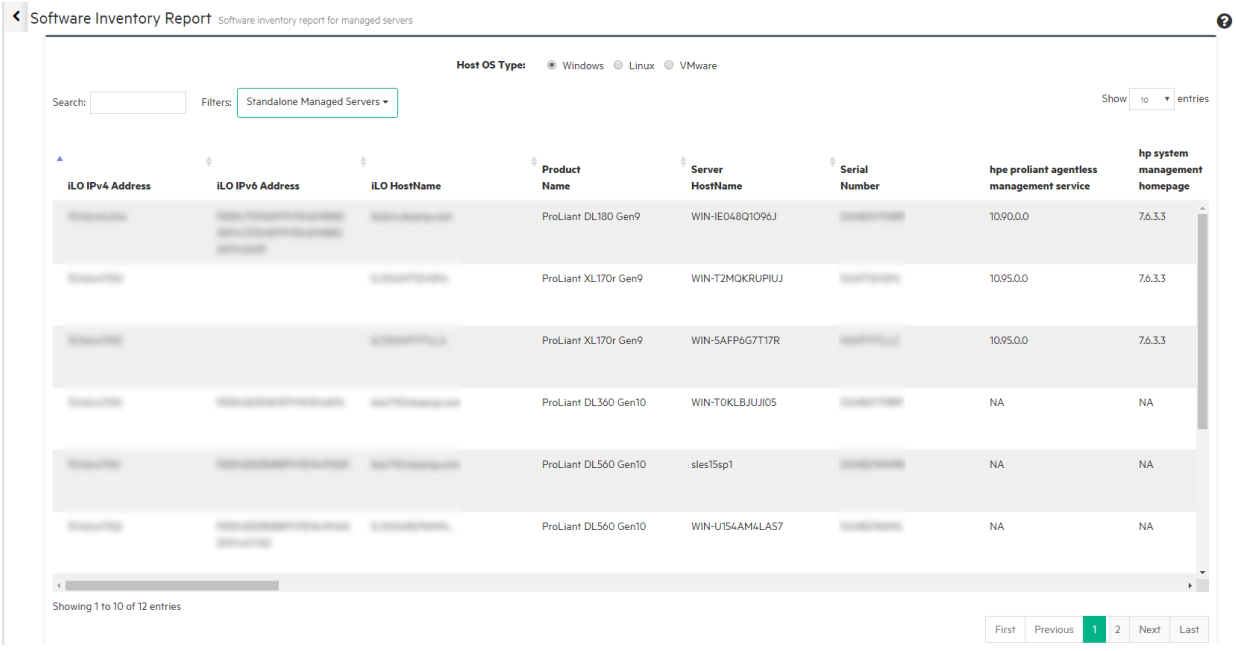
- Enter a value in the **Search** box and press the enter key to search for specific information.
- Use the **Filters** menu to customize the display.
- Use the **Show entries** menu to choose the number of entries to display per page.
- Use the navigation buttons to view the first, previous, next, or 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 the CSV format.

Viewing the Software 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) v10.95.0 or later for Windows or AMSv2.10.0 or later for Linux
- For Gen10 and Gen10 plus servers: AMS v2.10 or later for Windows, AMS v2.3.0 or later for Linux, and AMSv2020.09.01 or later for ESXi
- For Gen11 servers: AMS v2.50 or later for Windows, AMS v3.1.0 or later for Linux, and AMSv2022.11.01 or later for ESXi

About this task



Procedure

1. Click **Reports** on the left navigation menu.
2. Click **Software Inventory Report**.
3. Select the **Host OS type** for which you want to view the software details. **Windows** is selected by default.

   The report provides software inventory information based on the OS type selected. The columns displayed change dynamically based on the software installed on each server. This information can also be viewed by navigating to **Assets** > **Servers**, clicking **View Details** and then selecting the **Software Inventory** tab.
4. Options on this page:
   - Enter a value in the **Search** box and press the enter key to search for specific information.
   - 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.

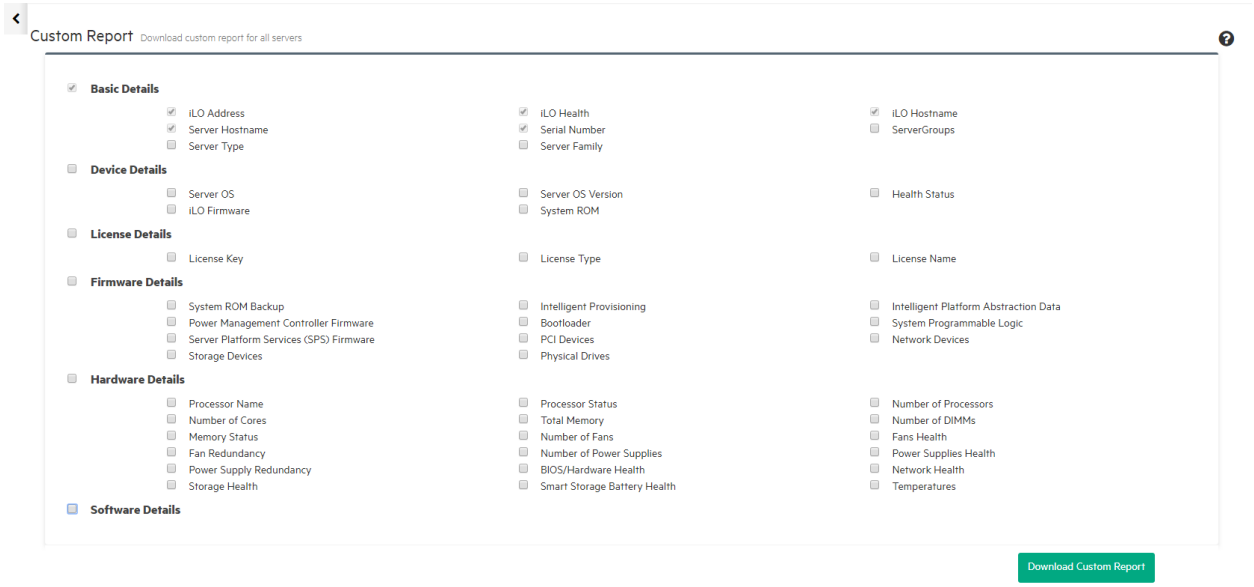
Viewing the Custom Report

Prerequisites

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

About this task

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.



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. For more information, refer **Software inventory report details**.

Server troubleshooting

Discovery of servers fail for external multiple storage enclosures that have too many hard drives

Symptom

Unable to view the server information on the `Assests` page.

Cause

Action

1. Perform a managed system configuration factory reset.
2. Add servers with restricted number of hard drives.

Downloading the server Active Health System log

About this task

The Active Health System monitors and records changes in the server hardware and system configuration. The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data. Host resources are not consumed in the collection and logging of Active Health System data.

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 **https://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.

   NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.

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 **https://www.hpe.com/servers/ahsv** in a supported browser. Supported browsers include:
   - Chrome v51 or later
   - Firefox v46 or later
2. Enter your **User ID** (email address) and **Password**, and then click **Sign In**.

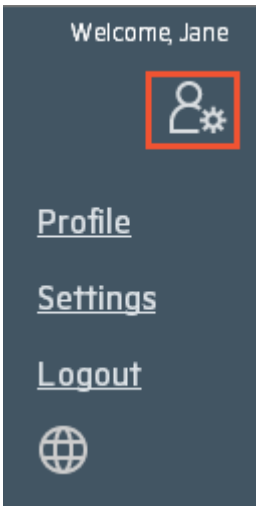
NOTE: To log in using an HPE Passport account, or to create an HPE Passport account, go to **https://www.hpe.com/info/insightonline**. In most cases, your HPE Passport account is the same as the email address you used during the HPE Passport account registration process. If you changed your user ID in 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.

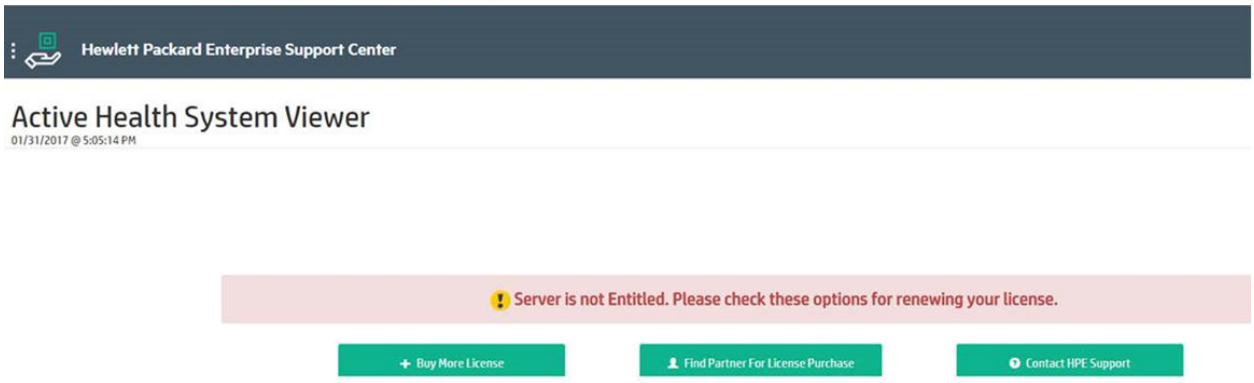


2. Click **Logout**. You will be logged off and the log in page is displayed.

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.

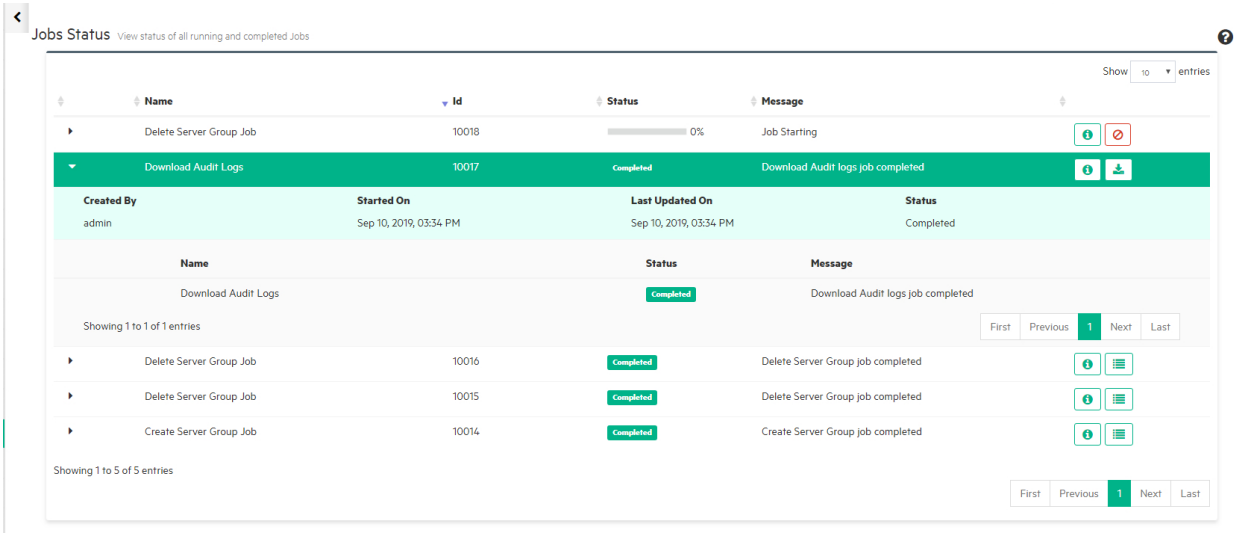
- A window is displayed that shows parsing and log loading states. To cancel the load process, click **Cancel**.
- This window also displays videos for different platforms. You can search and play different videos while you are waiting for the log file to load.
- As the AHS log loads, the screen displays 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 job status

About this task

You can view and abort any job from the **Jobs Status** page.

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



Procedure

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

   The following information appears:

   - **Name**
   - **ID**—Job IDs are not always sequential. This is normal behavior.
   - **Status**—A progress bar shows the job completion percentage. Once the job is run, any of the following states can appear:
     - **Running**—The job is executing.
     - **Pending**—The job is pending and has not started.

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

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

- **Message**—Information about the running job and the number of servers/server groups on which it is run.

2. Click the right arrow to reveal the job status details and sub jobs.

   - **Created by**—Username of the person who initiated the job.
   - **Started on**—Date and time of job creation
   - **Last updated**—Date and time of last job update
   - **Status**—Status of the job

   The following details of the sub jobs are displayed. Some sub jobs can be expanded further.

   - **Name**—Name of the job or the iLO, Host Name, or server group name on which the job is run
   - **Status**—Status of the job
   - **Message**—Information about the success or failure of the job

3. Optional: If a job is in the **Running** state, you can click  to cancel the job.
4. Click  to view the job parameters and the servers on which the job is run.
5. Click  to view the job results.

   NOTE: This icon will only be available for certain jobs.

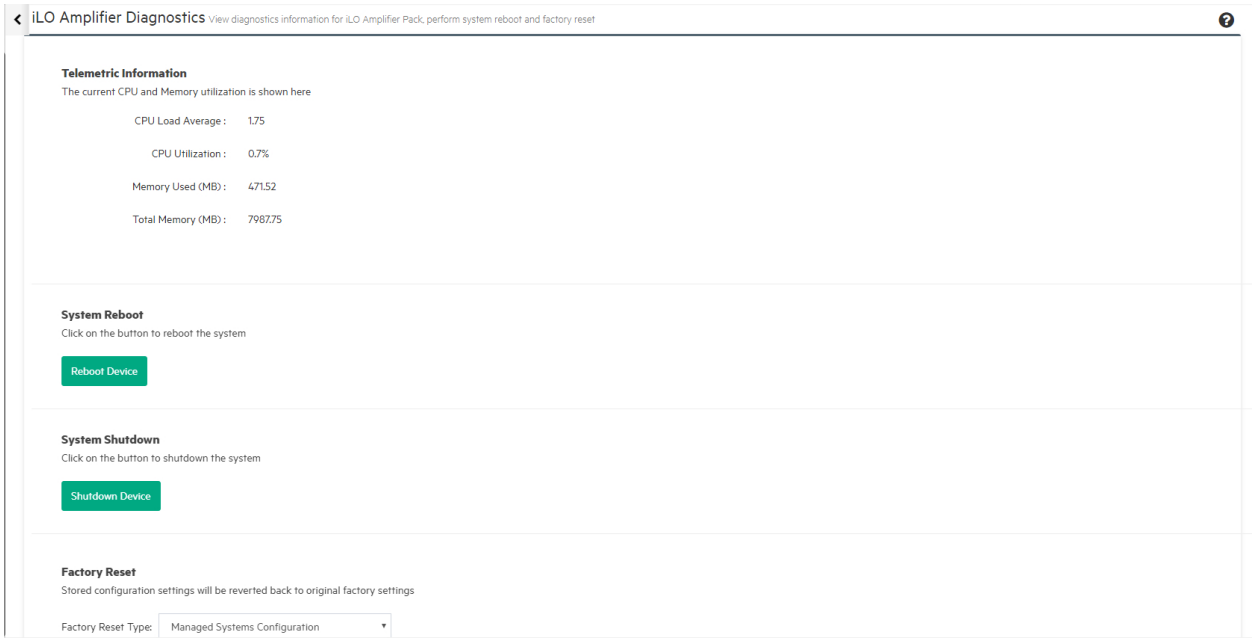
6. Click  to download export a report to a CSV file.

   NOTE: This icon will only be available for **Reports** download and **Product Entitlement Report** download jobs.

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.

IMPORTANT: Users with Configuration Manager role and above are allowed to perform the appliance related operations.



- **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:
  - Refrain from performing any modifications when the factory reset operation is in progress.

    Reset is performed on iLO Amplifier and the iLOs discovered in such iLO Amplifiers where remote support settings on those iLOs point to iLO Amplifier are cleared.
  - Factory reset will erase all configuration from iLO Amplifier Pack, based on the factory reset type selected.
  - When you perform a factory reset, the existing Remote Support setting for the connected iLO Amplifier Pack is cleared.

- **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

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.

HPE recommends upgrading the appliance firmware to version 1.40 or 1.50 before upgrading to version 1.55.

Users upgrading the appliance firmware to 1.70 or above from any version prior to 1.70 will be shown a pop up to opt in to anonymous data usage collection when logging in for the first time. This selection can be modified at any time by navigating to the **General settings** page.

iLO Amplifier Pack offers two methods to upgrade the appliance firmware:

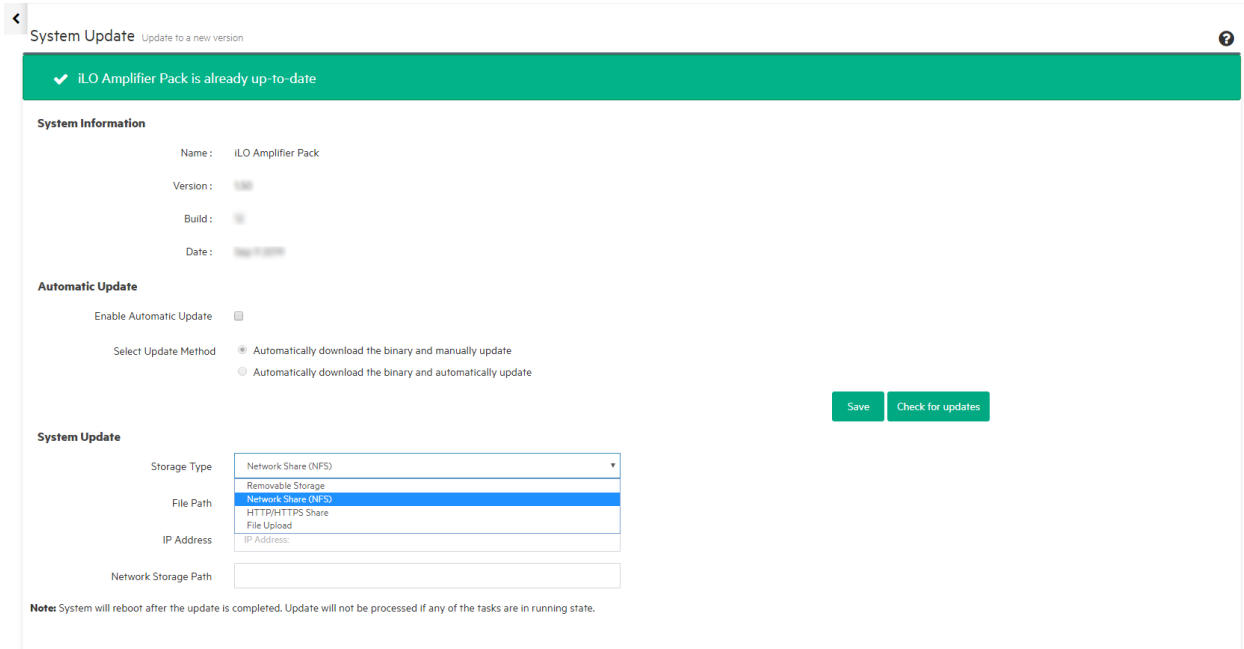
- **Upgrading the appliance firmware manually**
- **Upgrading the appliance firmware automatically**

Upgrading the appliance firmware manually

Prerequisites

- An HTTPS outbound connection on port 443 to `infosight.hpe.com` and `midway.ext.hpe.com`.
- iLO Amplifier Pack user with either of the following privileges:
  - Configure Manager
  - Configure Manager with Security

About this task



Procedure

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

1. Click the download link on the My HPE Software Center page for downloading the **`iLOAmplifierPack.bin`** file.
2. Check the integrity of the downloaded bin file by comparing the checksum of the file with the checksum value listed on the download page by using an appropriate checksum verification tool.
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`.

     NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.
   - 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 system manually**.

   The system will reboot once the update is complete. The installation and reboot may take up to 10 minutes to complete. The progress of the installation and reboot process will be displayed in the browser.

   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 jobs are still running.
   - Keep the initial registration email for use with future updates.

Upgrading the appliance firmware automatically

Prerequisites

- An HTTPS outbound connection on port 443 to `infosight.hpe.com` and `midway.ext.hpe.com`.
- iLO Amplifier Pack user with either of the following privileges:
  - Configure Manager
  - Configure Manager with Security
  - DNS configuration

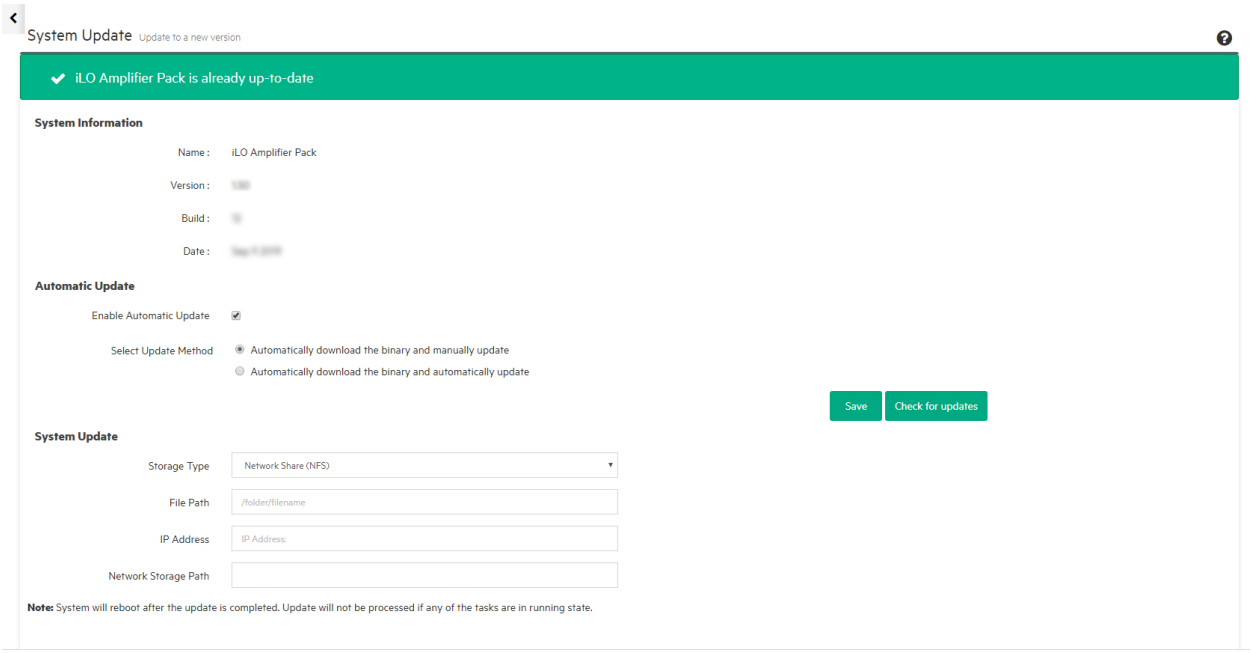
- Firewall allows outbound connection to `midway.ext.hpe.com`.
- Proxy settings if required. See **Configuring network settings** for more details.

About this task

iLO Amplifier Pack version 1.50 onwards allows you to automatically download the binary files when an update is available. You can then choose to allow iLO Amplifier Pack to update the appliance automatically when no jobs are running or you can trigger the update manually.

NOTE: Users must be on iLO Amplifier Pack v1.60 to auto update to v1.70. Any user on an appliance version lower than iLO Amplifier pack 1.60 will first be updated to v1.60, and then to v1.70.

For more information on configuring the IP addresses for a successful connection, see the **Prerequisites for midway server connectivity**.



Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **System Update**.
2. Under **Automatic Update**, select the **Enable Automatic Update** check box and choose from one of the following options:
   - Select **Automatically download the binary and manually update** for iLO Amplifier Pack to automatically download the update binary. Once the package is downloaded, a banner message will be displayed at the top of the page. The upgrade must then be initiated manually from the **System Update** page. This option will be selected by default if automatic updates are turned on.
   - Select **Automatically download the binary and automatically update** for iLO Amplifier Pack to automatically update itself when an update is available. The update will be scheduled for later if any jobs are running.

   NOTE: The system will reboot once the update is complete. The installation and reboot may take up to 10 minutes to complete. The progress of the installation and reboot process will be displayed in the browser.

3. Click **Save**.
4. Optional. Click **Check for updates now** to check if any new updates are available.

Appliance firmware upgrade storage types

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

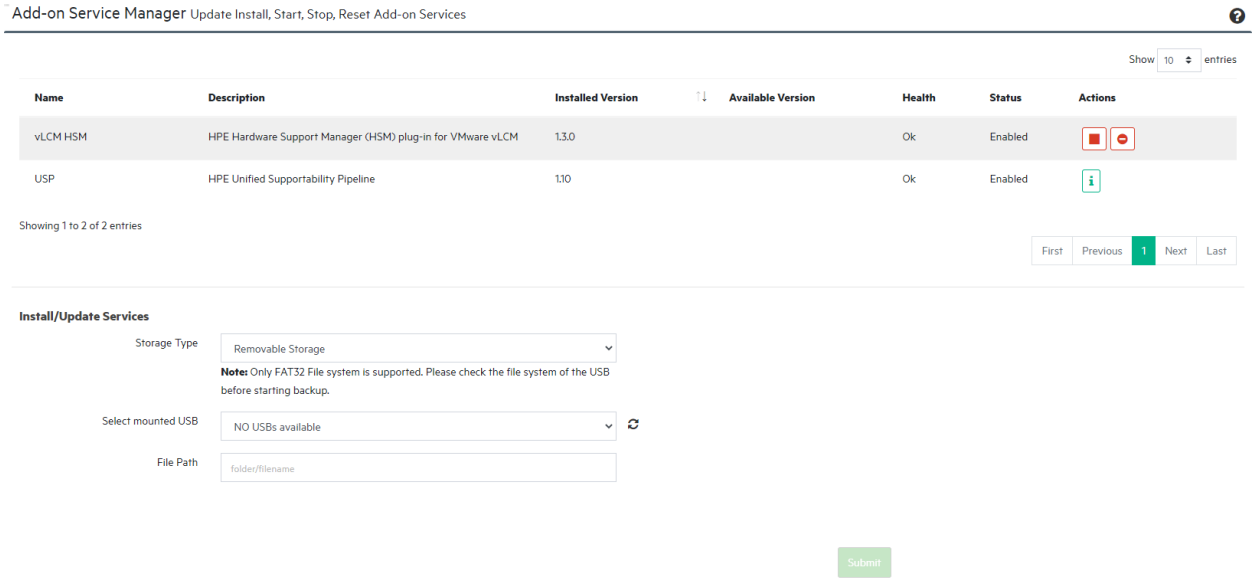
- **Removable Storage (USB)**—Upgrade the firmware from a file saved on a removable storage device.

  NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.

- **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.

Configuring Add-on Services

iLO Amplifier Pack 1.90 and later versions allow you to enable add-on services. These services run natively in iLO Amplifier Pack and integrate with certain other services to extend the functionality of the appliance.



HPE allows users to download additional add-on services separately and upload them into iLO Amplifier Pack, as long as the appliance version is 1.60 or newer. These add-on services are provided in the form of binary files. These binary files can be downloaded from the **My HPE Software Center** when available.

NOTE: Add-on services prepackaged with the appliance are not installed, nor enabled.

If an All Configuration factory reset is performed, the appliance will only display prepackaged services. These services must be installed and enabled again.

The following service is available for iLO Amplifier Pack:

- **HPE Hardware Support Manager (HSM) plug-in for VMware vSphere Lifecycle Manager**

The Hardware Support Manager plug-in is an extension to vSphere Lifecycle Manager provided by HPE to perform firmware or software updates using Hardware Support Packages (Service Pack for ProLiant).

For more information, see the *HPE Hardware Support Manager plug-in for VMware vSphere Lifecycle Manager* document.

- **Unified Supportability Pipeline**

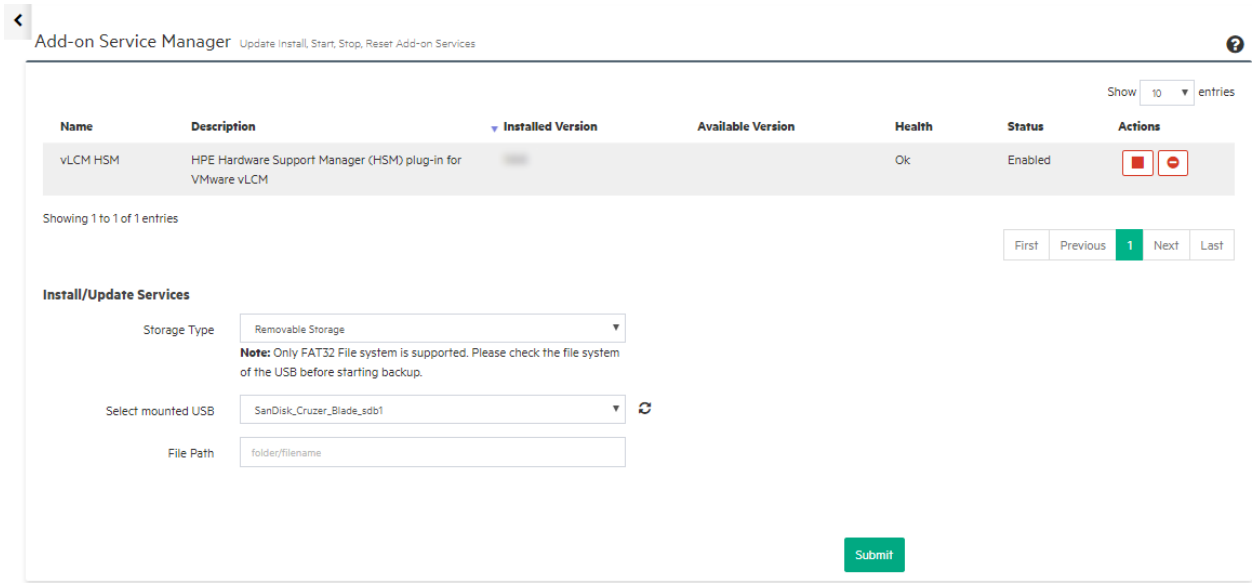
  The Unified Supportability Pipeline feature enables an increased coverage for wellness alerts and automatic support case creation. Unified Supportability Pipeline feature helps you to manage automatic support case creation. A case is created automatically when a service event occurs. Previously, in HPE InfoSight for Gen9 and Gen 10 servers, only six service events were supported. With the implementation of Unified Supportability Pipeline, the automatic support case creation capability can now be used for all the iLO 4, iLO 5, and iLO6 generated service events for Gen8, Gen9, Gen 10, and Gen11 servers. The Unified Supportability Pipeline feature will be available to all the managed servers in the organization.

Installing, disabling, and uninstalling an add-on service

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

About this task



Procedure

1. Click **Configuration and Settings** on the left navigation menu , and then click **Add-on Service Manager**. Prepackaged add-on services if any, will be listed in a table.

   Depending on the status of the service, icons to install, uninstall, start or stop a service are displayed.

2. Click  to install and enable the add-on service.
3. Once enabled, a new page for the add-on service will be available in the left navigation menu.

4. Once the service is installed, click  to disable it, or click  to uninstall the service.
5. To enable a stopped service, click .

Installing an add-on service using a binary file

Prerequisites

- iLO Amplifier Pack 1.60 or newer
- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Download and save the iLOAmpPack_AddOn_X.XX.zip and its corresponding checksum file.

   NOTE: Use an appropriate checksum verification tool to verify the integrity of the downloaded files.
2. Extract the binary file from the compressed zip package.
3. Click **Configuration and Settings** on the left navigation menu, and then click **Add-on Service Manager**.
4. Under the **Install/Update Services** section, select the storage type that corresponds to the location where you saved the binary file.
5. 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.

     NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.
   - 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 binary file.
   - For a file upload, click **Browse**, and then navigate to the binary file on the client computer.
6. Click **Submit**. The system will automatically reboot if necessary after the update is finished and the service will be listed on the **Add-on Service Manager** page.

Updating add-on services

iLO Amplifier Pack add-on services may be updated by different methods.

- Updates to existing add-on services may be included with updates to the iLO Amplifier Pack appliance. The **Available Version** column will indicate newer versions of any add-on services.
- Users can **update add-on services using binary files** if an update to an add-on service is made available prior to an appliance release.

New add-on services can also be introduced as part of an appliance update. A banner message is displayed at the top of the screen to notify users in such cases. Click **Dismiss** to clear this notification.

NOTE:

- Add-on services cannot be downgraded to lower versions.
- If an installation of the same version of the add-on service is attempted, a message will be displayed stating that the service is already up-to-date.

Updating an add-on service using a binary file

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

Procedure

1. Download and save the iLOAmpPack_AddOn_X.XX.zip and its corresponding checksum file.

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

2. Extract the binary file from the compressed zip package.
3. Click **Configuration and Settings** on the left navigation menu, and then click **Add-on Service Manager**.
4. Under the **Install/Update Services** section, select the storage type that corresponds to the location where you saved the binary file.
5. 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.

     NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.

   - 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 binary file.
   - For a file upload, click **Browse**, and then navigate to the binary file on the client computer.
6. Click **Submit**. The system will automatically reboot if necessary after the update is finished.

Configuring general settings

Prerequisites

- User privileges

- Configure Manager with Security
- Configure Manager

About this task

You can discover and managed the inventory of the available servers using Service Account. iLO Amplifier Pack automatically creates and manages these service accounts.

You can set the refresh settings for iLO Amplifier Pack to wait for a manually specified time limit between inventory processes or refresh automatically. You can also enable iLO Amplifier Pack to refresh inventory based on alerts from the iLO.

Procedure

1. Click **Configuration and Settings** from the left navigation menu, and then click **General Settings**.
2. Select or clear **Enable Service Account Creation** option.
3. Set the **Password Reset Interval (in days)** to any value between 30-365 days.

   IMPORTANT:

   - The selected option for **Enable Service Account Creation** cannot be modified.
   - The confirmation popup appears for **Password Reset Interval (in days)** only when the settings are enabled for the first time.

4. Select one of the following:

   - To have iLO Amplifier Pack automatically refresh server inventory, click to select the **Enable Auto Refresh** check box.

     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.
   - To specify the refresh interval time, clear the **Enable Auto Refresh** check box, and select a number from the **Refresh Interval (in hours)** menu.

     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.

     NOTE: If auto refresh is disabled, the server inventory information in iLO Amplifier Pack may not always be up to date.

5. To have iLO Amplifier Pack automatically refresh server inventory on receiving an iLO alert event, select the **Enable Alert Based Refresh** check box.

   NOTE: HPE recommends that this setting be enabled to ensure that the inventory is always up to date.

6. Click **Save**.

Configuring Server Connection Settings

7. For data center locations with high latency and poor bandwidth, the HTTPS connection to iLO can be configured to timeout after a longer duration. Enter a value in the **HTTPS Connection Timeout to iLO** in seconds.

NOTE:

- This value must be in the range of 30-60 seconds.
- A higher value will affect the overall time taken for discovery operations like IPV4 range, CSV discovery, or periodic refresh of the servers. Some servers that do no respond will wait for the timeout to fail and hence the overall time for the operation could increase.

Opting in to Anonymous Usage Data Collection

8. Optional: You can choose to share anonymous usage data with HPE to improve the product experience. Select the **I agree to send anonymous data usage to HPE** check box and click **Save**.

   You can choose to stop sharing at any time by clearing this check box and clicking **Save**.

Server inventory and service account

Evolution of service account

Historically, an HPE iLO amplifier Pack server discovery and inventory requires credentials to the iLO. User environments require the credential to iLO be rotated one time in a year or a lesser duration. As a result, the users were unable to update password on multiple systems. Moreover, to change passwords, a user is required to rediscover the servers.

HPE iLO Amplifier Pack uses the credentials to perform the following:

- Discovery of servers
- Inventory Refresh
- Refresh operations.
- Perform Firmware updates.

Every server that is marked as `Not Reachable` requires the user to key in the new credentials.

Introduction of service account

Going forward, based on the user credentials, HPE iLO Amplifier Pack creates a service account in iLO. This service account is used to perform inventory and various actions on the servers. Also, a user configurable policy is in place to rotate the passwords periodically.

With the advent of service account, the users get the following functionalities:

- One time option to migrate to use service accounts.
- Option to update the credentials for many discovered servers in a single operation.
- The iLO credentials used for initial discovery or Update Credentials must at least have Administer user account and login privilege.
- In iLO5 and iLO6, a service account is created whereas, in iLO4 a local user account is created and the iLO Amplifier Pack manages it.

Salient features of service account

The following are the salient features of Service Account in HPE iLO Amplifier Pack:

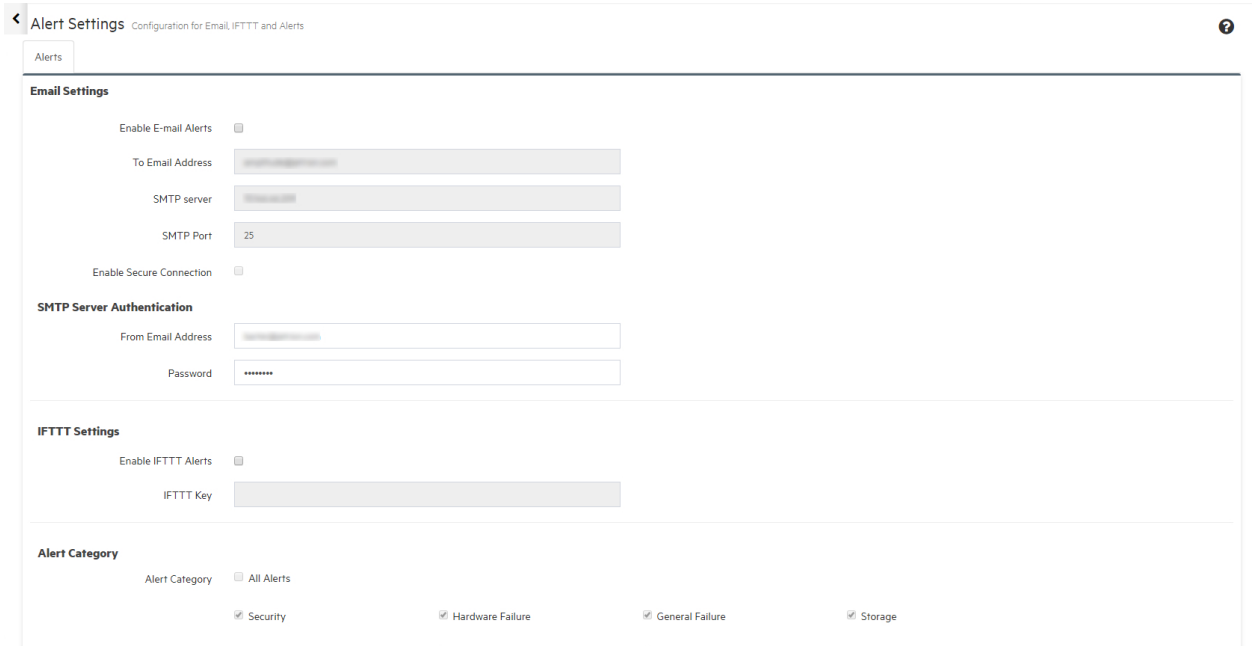
- Service account now enables the users to securely store the created service account credentials.
- Delete the service account when user removes the server for iLO Amplifier Pack or performs a factory reset of the iLO Amplifier Pack.
- Service Account in iLO has the following username format : `iLOAMP_<iLOAmpUniqueID>_RandomBytes`, where, iLOAMP is constant prefix. `iLOAmpUniqueID` is the Unique Numerical value that can be found in the iLO Amplifier Pack General settings page once Service Account is enabled.`Random Bytes`: Consists of Random Alphanumeric value.

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.

About this task



Procedure

1. Click **Configuration and Settings**, and then click **Alert Settings**.
2. Proxy set up on the **Network Settings** page if your Internet connection uses a proxy.
3. 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.server.com`**.

d. Provide the outgoing server port number.

e. To use secure communication to SMTP server, select **Enable Secure Connection** .

f. To use authentication to SMTP server, specify the username and password for the email account that sends the alerts.

NOTE:

- Depending on your network environment, SMTP server may be reachable only through a proxy. Ensure that you have specified the proxy. In case the SMTP server is local to your network environment and if a proxy is specified, ensure that the Bypass Proxy is enabled and SMTP server is specified in the Bypass Proxy list.
- Ensure that you have MS Exchange or GMAIL configured as your mail server.

---

4. 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**.
   - If your Internet connection requires a proxy, ensure that a proxy is setup in the Network Settings page

   ---

5. 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

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

   NOTE: Save the configured settings before sending a test alert.

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. Select **Connect** and enter your email address. Enter the pin you receive on the registered email address on the webpage.
13. Click **Send me an email** on the **Choose action** page.
14. Review the action fields, and then click **Create action**.
15. Click **Finish** on the **Review and finish** page to complete the alert.
16. Open iLO Amplifier Pack, click **Configuration and Settings**, and then click **Alert Settings**.
17. 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

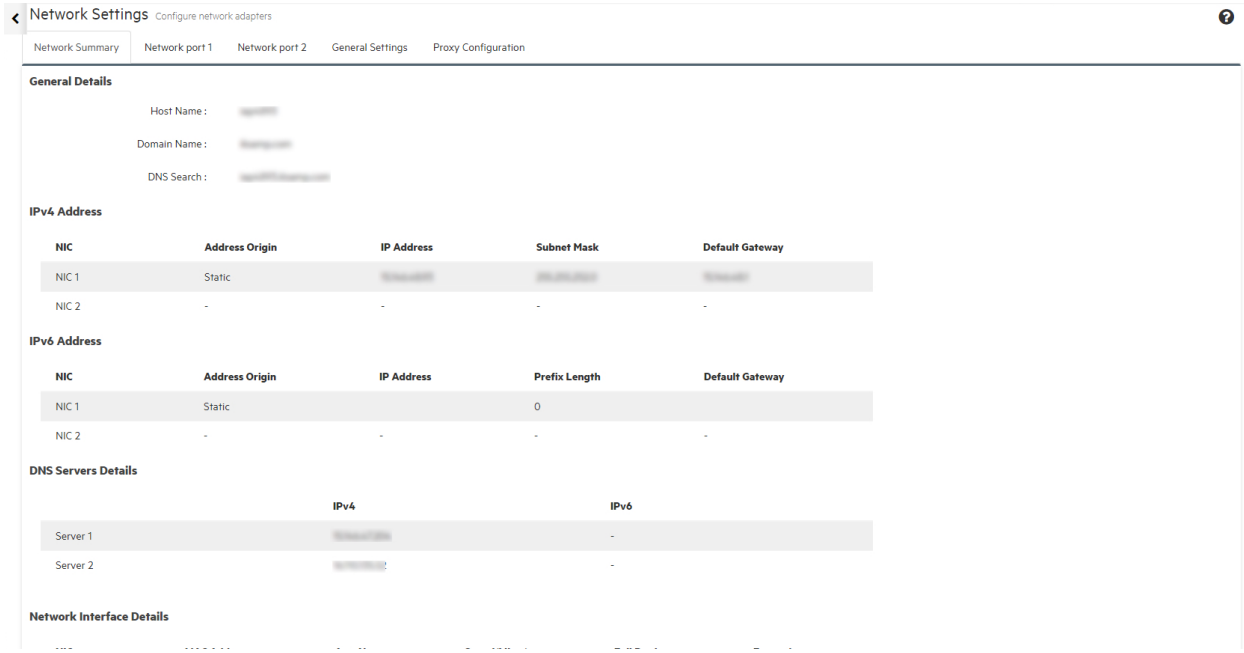
```
{{EventName}}<br>
When: {{OccurredAt}}<br>
Category: {{Value1}}<br>
Action: {{Value3}}
```

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. Up to 5 static routes can be configured for IPv4 and IPv6 addresses. Click  under **Static Route for IPv4** or **Static Route for IPv6** to add more than one static route:
   - Enter the following information in the **Static Route for IPv4** section in the **Network Port 1** or **Network Port 2** tab:
     - Destination
     - Mask
     - Gateway
   - Enter the following information in the **Static Route for IPv6** section in the **Network Port 1** or **Network Port 2** tab:
     - Destination
     - Gateway
     - Prefix Length

   NOTE: If the gateway for the configured static route is not reachable, then the static route will not be in effect and will not be displayed on the **Network Summary** tab.
6. Click **Save** to save your settings.
7. 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:
   - [Optional but it is recommened] **Host Name**
   - [Optional and depends on the network configuration] **Domain Name**
   - [Optional and depends on the network configuration] **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 **Preferred 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 your proxy server port number in the **Port number** field.
6. Optional: Click to select the **Enable Secure Proxy Connection** check box.
7. Optional: Enter a **Username** and **Password** to enable proxy authentication.
8. Optional: Click to select the **Enable Bypass Proxy** check box.
9. Optional: Enter the IP address, range of IP addresses in CIDR format, or a specific FQDN for which the proxy connection should not be used. You can enter multiple values if required, but each value must be separated by a comma.
10. Click **Save** to save your settings.
11. Click **Reboot** to restart the iLO Amplifier Pack appliance.

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

Prerequisites

- User privileges
  - Configure Manager

About this task

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**.

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

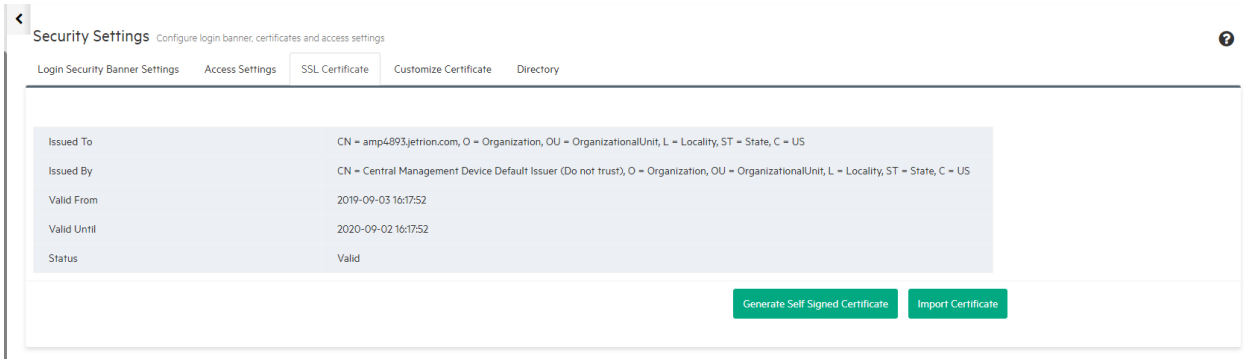
1. Click **Configuration and Settings** on the left navigational menu, click **Security Settings**, and then click the **Access Settings** tab.
2. Set the minimum password length in the **Min Password Length** field.
3. Select the time-out period from the **Session Idle Time Out (Min)** menu.
4. Click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

Obtaining and importing an SSL certificate

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

About this task



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

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

About this task

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

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

Lightweight Directory Access Protocol (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. iLO Amplifier Pack version 1.20 onwards lets you 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. iLO Amplifier Pack will only authenticate users from groups declared at the parent level and not from nested groups. Add any nested groups as separate entries. 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

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

About this task

Use this page to configure the Directory Server Settings.

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).

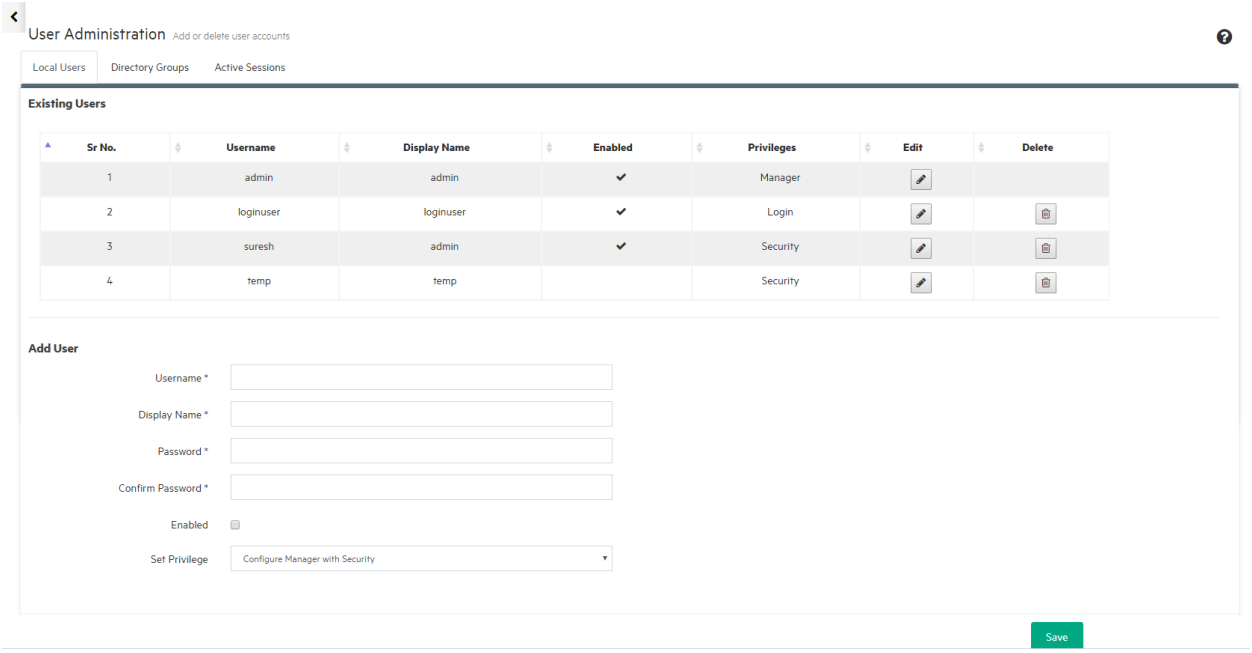
   NOTE: To avoid LDAP timeout, users are advised to use a more specific base DN value. For example, instead of using "DC=domain,DC=com", use specific values such as "CN=path1,DC=domain,DC=com" or "OU=path2,DC=domain,DC=com" or "CN=path1,OU=path2,DC=domain,DC=com" (assuming the users are present in this 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**.

NOTE: Configure LDAP in the directory settings before you add a group account.

Managing iLO Amplifier Pack user accounts and active sessions

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



Adding a group account

Prerequisites

User privileges

- Configure Manager with Security
- Configure Manager
- Configure User
- Before you add a group account, configure LDAP in the directory settings

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

Instructions for editing a group account.

Prerequisites

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

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**.

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

Instructions for 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

Instructions for 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 jobs, including Recovery Management.
- **Configure Manager**—Allows a user to perform all iLO Amplifier Pack jobs, 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 jobs 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

Disabling a group account

Instructions for disabling a group account.

Prerequisites

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

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 jobs, including Recovery Management.
- **Configure Manager**—Allows a group to perform all iLO Amplifier Pack jobs, 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 jobs on devices. This privilege includes the **Login** privilege.
- **Login**—Allows a user to log in to iLO Amplifier Pack with read-only access.

Active sessions

Prerequisites

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

Procedure

1. Click **Configuration and Settings** on the left navigational menu, click **User Administration**, and then click the **Active Sessions** tab.
2. Click  for the session you want to delete, and then click **Ok** to confirm the deletion.

Backup and Restore

Backing up the iLO Amplifier Pack configuration

Prerequisites

- User privileges
  - Configure Manager with Security
  - Configure Manager

About this task

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

Procedure

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

   The **Backup** tab opens by default.
2. Click to select **NFS Share**, **USB Share**, or **Local File** from the **Storage Type** menu.
3. Do one of the following:
   - For **NFS Share**, enter the IPv4 or IPv6 address, the destination file path, and the network storage path.
   - For **USB Share**, select the mounted device and enter the file path in the format `/folder/ filename`.

     NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.
   - For **Local File**, enter the file name for the backup file.
4. For any **Storage Type** you select, enter the following information:
   - **Backup File Passphrase**—used to encrypt the configuration data; required to restore from this file.
   - **Confirm Passphrase**
5. 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. Click to select **NFS Share**, **USB Share**, or **Local File** from the **Storage Type** menu.
4. Do one of the following:
   - For **NFS Share**, enter the IPv4 or IPv6 address, the destination file path, and the network storage path.
   - For **USB Share**, select the mounted device and enter the file path in the format `/folder/ filename`.

     NOTE: USB mounting is supported only in iLO Amplifier Pack installed using VMware ESXi or KVM.
   - For **Local File**, click **Choose File** to open the file explorer and choose the backup file stored on your local drive.
5. HPE recommends that you turn off the old iLO Amplifier Pack instance during restoration to avoid IP conflicts. You can power the appliance back on after the Restoration process is completed.
6. For any **Storage Type** you select, enter the **Backup File Passphrase**.

7. Click **Restore** to begin the restoration process.
8. During the restoration, the new iLO Amplifier Pack instance changes its IP address to the same IP address as the old appliance. To avoid IP conflicts, you must manually change the IP address on the new iLO Amplifier Pack instance.

iLO Amplifier Pack Redfish API Implementation

Starting with iLO Amplifier Pack v1.50, customers can now programmatically access iLO Amplifier Pack using REST API calls that are compliant to the Redfish standards.

iLO Amplifier Pack now allows users to subscribe and automate alerts programmatically using the Redfish API. A maximum of 10 subscribers can listen to one iLO Amplifier Pack instance. For more information on the iLO Amplifier Pack scripts, see the **iLO Amplifier Pack API documentation**.

IMPORTANT: The Redfish APIs for iLO Amplifier Pack are a technical preview, and may not offer the full feature set offered by the GUI.

For more details about the Redfish standards, see the "Redfish Scalable Platforms Management API Specification" on the **DMTF website**.

iLO Amplifier Pack troubleshooting

Discovery of servers fail for external multiple storage enclosures that have too many hard drives

Symptom

Unable to view the server information on the `Assests` page.

Cause

Action

1. Perform a managed system configuration factory reset.
2. Add servers with restricted number of hard drives.

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 job is created

Symptom

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

Cause

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

Action

To check whether the job was created or has failed, see the **Job 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

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

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 job 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.

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 and 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.

iLO Repository offline update on servers with High Security modes configured fails when force downgrade option is selected

Symptom

The iLO Repository Firmware Only Offline Update fails when the additional option to "Force downgrade" is selected on servers which are configured with HighSecurity/FIPS modes.

Cause

The install set downgrades the iLO component to version 1.20 which does not support HighSecurity mode.

Action

While performing a force downgrade during an offline update on servers set to High Security modes, use SPP version 2018.11 or higher to ensure that the iLO version is not downgraded below version 1.30.

InfoSight and appliance update connectivity troubleshooting

Users can use the **Test Connection** button on the **InfoSight Setup** page to test the connectivity between iLO Amplifier Pack and the `infosight.hpe.com` and `midway.ext.hpe.com` servers. If iLO Amplifier Pack cannot establish a successful connection with the midway servers, a banner with an error message will be displayed at the top of the page.

Users can use the **Check for updates now** on the **System Update** page to test the connectivity between iLO Amplifier Pack and the update servers. If iLO Amplifier Pack cannot establish a successful connection with the midway servers, a banner with an error message will be displayed at the top of the page.

This section will help you resolve these errors, and establish a successful connection to the midway servers. If you are still unable to resolve these errors, contact HPE support as described in **Accessing Hewlett Packard Enterprise Support**.

Invalid midway or DNS address. Check the network settings and retry.

Symptom

The **InfoSight Setup** or **System Update** page displays an "Invalid midway or DNS address. Check the network settings and retry" error message.

Cause

iLO Amplifier Pack cannot connect to the midway server or resolve the DNS address.

Action

Check the **network settings** to ensure that the proper DNS settings are used and iLO Amplifier appliance can connect to the midway servers. If using a firewall, ensure that no restrictions are being applied on connections being made by the iLO Amplifier Pack appliance.

Failed to establish connection to midway server. Check the network settings (Proxy/DNS) and retry

Symptom

The **InfoSight Setup** or **System Update** page displays a "Failed to establish connection to midway server. Check the network settings(Proxy/DNS) and retry" error message.

Cause

iLO Amplifier Pack cannot connect to the midway server as the network settings may not be configured properly.

Action

If using a proxy network, check the **proxy settings** to ensure that they are properly configured. Check the **network settings** to ensure that the proper DNS settings are used and the iLO Amplifier Pack appliance can connect to the midway

servers. If using a firewall, ensure that no restrictions are being applied on connections being made by the iLO Amplifier Pack appliance.

Invalid proxy address

Symptom

The **InfoSight Setup** or **System Update** page displays an "Invalid proxy address" error message.

Cause

The proxy settings are not configured properly.

Action

If using a proxy network, check the **proxy settings** to ensure that they are properly configured.

Failed to establish connection to proxy server. Verify the proxy settings

Symptom

The **InfoSight Setup** or **System Update** page displays a "Failed to establish connection to proxy server. Verify the proxy settings" error message.

Cause

The proxy settings are not configured properly.

Action

If using a proxy network, check the **proxy settings** to ensure that they are properly configured.

Service not running. Enable/Re-submit the InfoSight Settings.

Symptom

The **InfoSight Setup** page displays a "Service not running. Enable/Re-submit the InfoSight Settings" error message.

Cause

iLO Amplifier Pack is unable to connect to the midway servers.

Action

Check the **network settings** to ensure that the proper DNS settings are used and iLO Amplifier appliance can connect to the midway servers. If using a proxy network, check the **proxy settings** to ensure that they are properly configured. If

using a firewall, ensure that no restrictions are being applied on connections being made by the iLO Amplifier Pack appliance.

Not Registered

Symptom

The **InfoSight Setup** page displays a "Not Registered" error message.

Cause

The HPE InfoSight service is not running.

Action

Obtain a fresh claim token from the HPE InfoSight webpage, and **link iLO Amplifier Pack to HPE InfoSight** again.

AHS download error troubleshooting

If the download of the AHS logs from the server iLO to iLO Amplifier fails, an error message will be displayed in the **AHS Download Error Details** column on the **InfoSight Status Report** page.

This section lists the most common errors and their troubleshooting methods. If you are still unable to resolve these errors, contact **HPE support**.

AHS file size exceeds max size. Recommended to update the iLO firmware to the latest version.

Symptom

InfoSight Status Report page displays an "AHS file size exceeds max size. Recommended to update the iLO firmware to the latest version" error message.

Cause

iLO is not updated to the recommended firmware version.

Action

Update iLO firmware to the latest version. For iLO 4 update to version 2.70, and for iLO 5 update to version 1.40. Reboot the server after the firmware update for reduced AHS file sizes.

AHS download not enabled in iLO

Symptom

InfoSight Status Report page displays an "AHS download not enabled in iLO" error message.

Cause

AHS download is not enabled in iLO settings.

Action

Enable Active Health System Logging from iLO settings. For more details, see the *HPE iLO 5 User guide*.

Connection to iLO failed

Symptom

InfoSight Status Report page displays a "Connection to iLO failed" error message.

Cause

iLO Amplifier Pack was unable to establish a successful communication with the server iLO.

Action

Check iLO connectivity for any network issues.

AHS file location invalid in iLO

Symptom

InfoSight Status Report page displays an "AHS file location invalid in iLO" error message.

Cause

An invalid location was configured for the download of the AHS logs.

Action

Configure a valid file location to download the AHS logs from the iLO settings. For more details, see the *HPE iLO 5 User Guide* (**https://www.hpe.com/support/ilo-docs**) or the *HPE iLO 4 User Guide* (**https://www.hpe.com/info/ilo/docs**) for your release of iLO.

Connection to iLO failed. Could not get the Authentication Token

Symptom

InfoSight Status Report page displays a "Connection to iLO failed. Could not get the Authentication Token" error message.

Cause

iLO Amplifier Pack was unable to establish a successful communication with the server iLO.

Action

Check iLO connectivity for any network issues. Verify if the iLO Credentials are valid. Ensure that there is a session available in iLO for iLO Amplifier to connect.

Server Serial Number/Product ID is Blank

Symptom

InfoSight Status Report page displays a "Server Serial Number/Product ID is Blank" error message.

Cause

iLO is unable to obtain the serial number or product ID of the server.

Action

Ensure that the server serial number, product ID, and other details are configured, and are reflected in iLO.

AHS download failed due to NAND failures. Verify the NAND health

Symptom

InfoSight Status Report page displays an "AHS download failed due to NAND failures. Verify the NAND health" error message.

Cause

A NAND failure has been observed and hence the iLO is unable to download and save the AHS logs.

Action

Check the status of the NAND on the server and raise a support case if there is component failure.

Websites

iLO Amplifier Pack

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

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

Product page

www.hpe.com/servers/iloamplifierpack

Download portal

https://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

https://www.hpe.com/info/ilo/docs

iLO 5

https://www.hpe.com/info/ilo/docs

iLO 6

https://www.hpe.com/support/ilo6

iLO licensing

https://www.hpe.com/info/ilo/licensing

HPE ProLiant Servers

HPE ProLiant Gen8 servers

https://www.hpe.com/info/proliantgen8/docs

HPE ProLiant Gen9 servers

https://www.hpe.com/support/proliantgen9/docs

HPE ProLiant Gen10 servers

https://www.hpe.com/info/proliantgen10-docs

HPE InfoSight

HPE InfoSight for Servers

https://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:

  https://www.hpe.com/info/assistance

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

  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

  https://www.hpe.com/support/hpesc

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter

- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates

- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  https://www.hpe.com/support/AccessToSupportMaterials

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

Remote support

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

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

HPE Get Connected

https://www.hpe.com/services/getconnected

HPE Tech Care Service

https://www.hpe.com/services/techcare

HPE Complete Care Service

https://www.hpe.com/services/completecare

Warranty information

To view the warranty information for your product, see the **warranty check tool**.

Regulatory information

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

https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

https://www.hpe.com/info/reach

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

https://www.hpe.com/info/ecodata

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

https://www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, use the **Feedback** button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (**https://www.hpe.com/support/hpesc**) to send any errors, suggestions, or comments. This process captures all document information.