Hewlett Packard Enterprise

HPE Intelligent Provisioning User Guide for HPE ProLiant Gen9 Servers

Abstract

This document details how to access and use the Intelligent Provisioning software, including tasks such as installing OSs, updating firmware, software, and drivers, and to performing some diagnostic tests. Intelligent Provisioning is included in the optimized ProLiant server support software from the Service Pack for ProLiant (SPP). This document is intended for administrators experienced in using ProLiant Gen9 servers.

Acknowledgments

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

Intel® and the Intel Inside logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft®, Windows®, Hyper-V Server®, and Windows Server® are trademarks of the Microsoft group of companies.

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

Contents

1 Introduction

TIP: The information in this guide is for using Intelligent Provisioning with ProLiant Gen9 servers. For information on using Intelligent Provisioning with ProLiant Gen8 Servers, see the Intelligent Provisioning user guide for ProLiant Gen8 servers available on the Information Library (**http://www.hpe.com/info/intelligentprovisioning/docs**).

About Intelligent Provisioning

Intelligent Provisioning is a single-server deployment tool embedded in ProLiant Gen9 servers that replaces the SmartStart CDs and Smart Update Firmware DVD used with previous generations of ProLiant servers. Intelligent Provisioning simplifies server setup, providing a reliable and consistent way to deploy servers.

Intelligent Provisioning assists with the OS installation process by preparing the system for installing original, licensed vendor media and Hewlett Packard Enterprise-branded versions of OS software and integrating optimized server support software from the Service Pack for ProLiant (SPP). SPP is a comprehensive systems software and firmware solution for ProLiant servers and server blades and their enclosures. ProLiant Gen9 servers are preloaded with a basic set of firmware and OS components, which are installed along with Intelligent Provisioning 2.xx.

Intelligent Provisioning operation

Intelligent Provisioning for ProLiant Gen9 servers includes the following components:

- Critical boot drivers for ProLiant servers
- Active Health System (AHS)
- StoreVirtual Virtual Storage Appliance (VSA)

IMPORTANT:

- Although ProLiant Gen9 servers are pre-loaded with firmware and drivers, you should update the firmware upon initial setup to ensure you have the latest versions. Updating firmware also ensures you have the latest version of Intelligent Provisioning for the latest supported features, such as Microsoft Windows 2012 installations.
- For ProLiant servers, firmware is updated using the Intelligent Provisioning Firmware Update utility.
- Do not update firmware if the version you are currently running is required for compatibility.

NOTE: Intelligent Provisioning does not function within multihomed configurations. A multihomed host is one that is connected to two or more networks or has two or more IP addresses.

Intelligent Provisioning provides installation help for the following operating systems:

- Microsoft Windows 2012 and Windows 2012 R2
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware ESXi Custom Image
- VMware ESXi/vSphere Custom Image

Not all versions of an OS are supported. For more information about supported OSs for ProLiant Gen9 servers, see the operating systems and virtualization software support for ProLiant servers.

More information

(**http://www.hpe.com/info/ossupport**)

Accessing Intelligent Provisioning

To access Intelligent Provisioning power on or reboot the server, and press **F10** when prompted during the server POST.

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

1. Open a browser and enter `https://<iLO host name or IP address>` to log into the iLO web interface.
2. On the login page, do one of the following:

   - Enter a directory or local user account name and password, and click **Log In**.

   - Click the **HPE Zero Sign In** button.

     This button is displayed when iLO is configured for Kerberos network authentication.

3. Navigate to the **Remote Console→Remote Console** page.
4. Verify that your system meets the requirements for using the remote console application you want to use.
5. Click the **Launch** button for your selected application.

   Alternatively, you can click an Integrated Remote Console link on the **Overview** page.

6. Restart or power on the server.

   The server restarts and the ProLiant POST screen appears

7. Press **F10** when prompted during the server POST.

When accessing Intelligent Provisioning, one of the following happens:

- If this is your first time using Intelligent Provisioning, on-screen prompts guide you through initial configuration and registration tasks.

- If Intelligent Provisioning was previously accessed and the initial configuration and registration tasks are complete, the Intelligent Provisioning home page is displayed. In the home screen, select one of the following options to use Intelligent Provisioning:

  ○ **Configure and Install**

    NOTE: The **Configure and Install** option is not available for ProLiant SL, SE, and XL Servers (except the ProLiant XL420 Gen9 Server).

  ○ **Perform Maintenance**
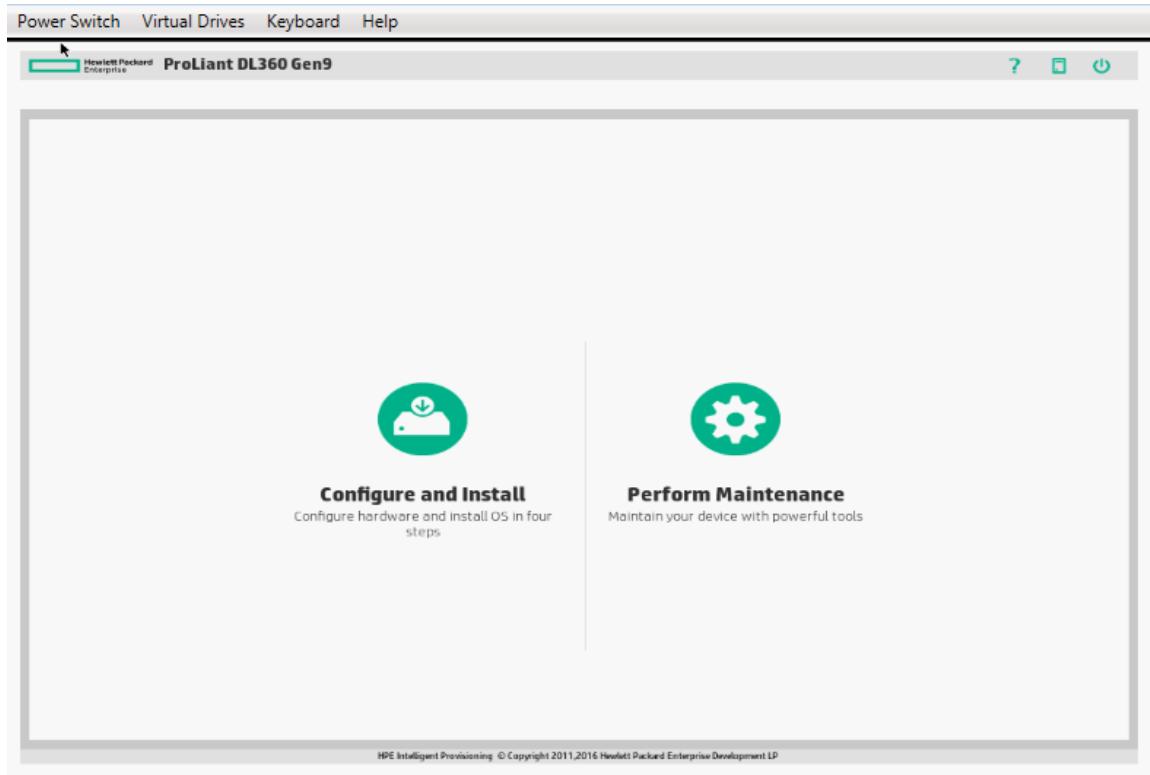
To exit Intelligent Provisioning, reboot the server by clicking the power icon at the top right of the page.

More information

Navigating Intelligent Provisioning

To navigate through and modify settings in this menu-driven interface, use the navigation icons displayed at the top right-hand corner and bottom left- and right-hand corners of the Intelligent Provisioning window.

These navigation icons are screen sensitive and are not displayed on all screens.

Icon	Function
Home ⌂	Returns to the Intelligent Provisioning home page, with the **Configure and Install** and **Perform Maintenance** menus. This icon is available only after completing the initial configuration and registration tasks.
Help ?	Opens the online help to the section about the current screen.
System Information ▢	Displays system information, including the Intelligent Provisioning version.
Power ⏻	Powers down or reboots the server.
Previous ‹	Returns you to the previous screen after validating and saving your choices.
Continue ›	Takes you forward to the next screen after validating and saving your choices.

2 Completing initial configuration and registration tasks

When using Intelligent Provisioning for the first time, follow the on-screen prompts to perform initial configuration and registration tasks.

Initial configuration and registration tasks

Initial configuration and registration includes the following tasks:

Software installed with Intelligent Provisioning

When a Windows system is installed using Intelligent Provisioning with Internet access, all the software applications will be downloaded and installed automatically. On other operating systems or on a Windows system without Internet access, the following applications are not installed automatically with Intelligent Provisioning. They can be installed by running the SPP.

- HPE ProLiant Agentless Management Service (AMS)

- HPE Network Configuration Utility for Windows

- HPE Smart Storage Administrator (HPE SSA)

- HPE Lights-Out Online Configuration Utility

- HPE Insight Diagnostics

Step 1: Set Intelligent Provisioning preferences

The **Set Preferences** screen appears automatically the first time Intelligent Provisioning runs on a server.
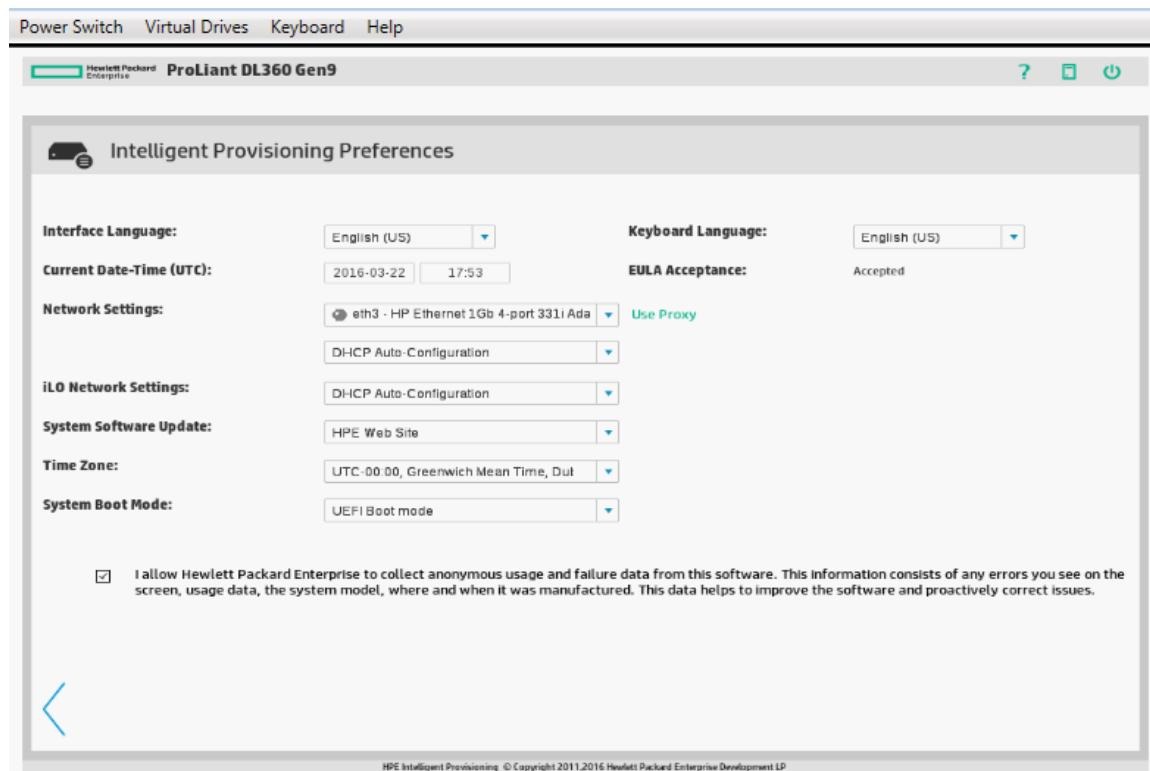
Date selection key sequences

When selecting the date, you can use the following key sequences.

- **PAGE UP**: Select the previous month.
- **PAGE DOWN**: Select the next month.
- **CTRL + PAGE UP**: Select the previous year.
- **CTRL + PAGE DOWN**: Select the next year.
- **CTRL + HOME**: Open the date selector if closed.
- **CTRL/COMMAND + HOME**: Select the current month.
- **CTRL/COMMAND + LEFT**: Select the previous day.
- **CTRL/COMMAND + RIGHT**: Select the next day.
- **CTRL/COMMAND + UP**: Select the previous week.
- **CTRL/COMMAND + DOWN**: Select the next week.
- **ENTER**: Select the focused date.
- **CTRL/COMMAND + END**: Close the date selector and erase the date.
- **ESCAPE**: Close the date selector without selection.

Setting preferences

1. Choose your interface language and keyboard language.
2. Confirm that the system date and time are accurate.

   To change the date or time, click the displayed date or time and use the displayed calendar or clock to select the new values.

3. Read the End User License Agreement (EULA).

   - To continue using Intelligent Provisioning, click **Accept**.

     Included in the EULA is a link for ancillary software, which contains a list of open source and proprietary software developed or obtained through third parties. This link and all other links in the EULA are not enabled, but can be accessed if entered into a browser.

   - To cancel using Intelligent Provisioning, click **Reboot** to exit the utility and reboot the server. Intelligent Provisioning remains accessible.

4. Enter network settings.

   Select the active NIC from the list, and then choose from one of the following IP addressing schemes:

   - **DHCP Auto-Configuration**—Hewlett Packard Enterprise recommends selecting DHCP to have IP addresses assigned automatically to your server.
   - **IPv4 Static**—Selecting IPv4 adds four new fields: the static IPv4 address, network mask, gateway address, and DNS address.
   - **IPv6 Static**—Selecting IPv6 adds two fields: the static IP address and the Gateway address.

5. Specify whether you are using a proxy. If you have a proxy on your network, you might need to configure it for use with features that communicate across the network. If you choose **Use Proxy**, enter a **Proxy Address and Port**.

6. Enter iLO network settings.

    Select one of the following iLO network IP addressing schemes:

    - **DHCP Auto-Configuration**—Hewlett Packard Enterprise recommends selecting DHCP to have IP addresses assigned automatically to your server.
    - **IPv4 Static**—Selecting IPv4 adds four new fields: the static IPv4 address, network mask, gateway address, and DNS address.
    - **Off**—Selecting Off makes this server unavailable through iLO.

    For more information about using iLO, see the iLO 4 user guide on the website (**http://www.hpe.com/info/ilo/docs**).

7. Select a delivery option for System Software Updates for Intelligent Provisioning.

    - **Hewlett Packard Enterprise website**—Hewlett Packard Enterprise recommends selecting this option to be prompted when updates are available and download all software updates for your server from hpe.com.
    - **HTTP/FTP**—When prompted, enter an address in the URL field.
    - **Disable**—Select this to disable automatic updates if you plan to update your system software manually.

8. Select the correct **Time Zone**.
9. Select the desired **System Boot Mode**.

    NOTE: Changes to the system boot mode are implemented during the OS installation process or in the next POST.

10. Click the **Continue** right arrow to proceed automatically to .

NOTE: To access this screen to change preferences at a later time, open the **Perform Maintenance** menus, and then click **Intelligent Provisioning Preferences** .

More information

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

Step 2: Activate Intelligent Provisioning

When logging on to Intelligent Provisioning for the first time, the Activation screen is viewable after the Setting Preferences screen.
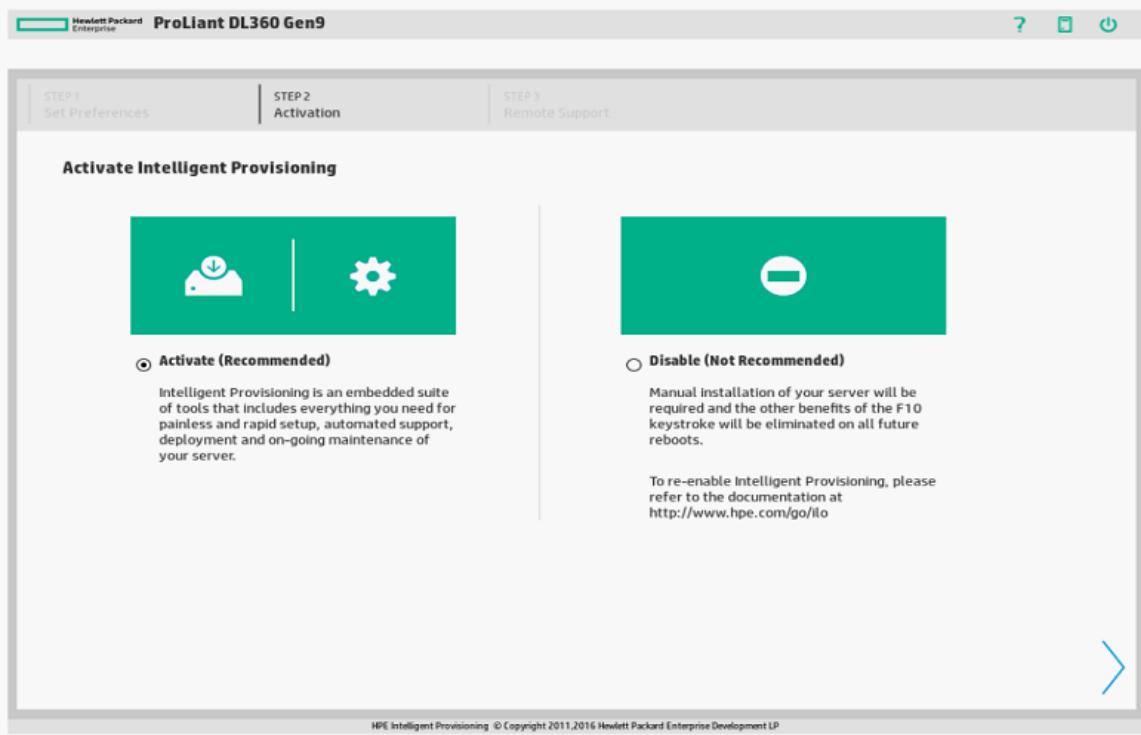
To activate Intelligent Provisioning and make it available during server POST:

1. Select **Activate (Recommended)**.
2. Click the **Continue** right arrow to proceed automatically to .

Disabling Intelligent Provisioning

1. Select **Disable (Not Recommended)**.
2. Click the **Continue** right arrow. The server reboots. During POST, **F10** is in red text on the screen, indicating that the **F10** key is disabled and Intelligent Provisioning is no longer accessible.

Re-enabling Intelligent Provisioning

1. Reboot the server and, when prompted, press **F9** to access the UEFI System Utilities.
2. From the System Utilities screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Server Security→Intelligent Provisioning (F10 Prompt)** and press **Enter**.
3. Select **Enabled**.

For more information on UEFI System Utilities, see the HPE UEFI System Utilities user guide (**http://www.hpe.com/support/UEFIGen9_UG_en**).

Step 3: Registering for HPE remote support

HPE embedded remote support

Intelligent Provisioning includes the embedded remote support feature, which allows you to register supported servers for HPE remote support.

Connecting a server to Hewlett Packard Enterprise allows it to be remotely supported and to send diagnostic, configuration, telemetry, and contact information to Hewlett Packard Enterprise. No other business information is collected, and the data is managed according to the Hewlett Packard Enterprise privacy statement, which you can review at the following website: **http://www.hpe.com/info/privacy**.

When you use the embedded remote support feature, choose from the following configuration options: Insight Online direct connect and Insight Remote Support central connect.

Insight Online direct connect

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

Insight Online is a Hewlett Packard Enterprise Support Center feature that enables you to view your remotely monitored devices anywhere, anytime. It provides a personalized dashboard for simplified tracking of IT operations and support information, including a mobile dashboard for monitoring when you are on the go.

Figure 1 (page 14) shows the direct connect configuration with a server.

Figure 1 Insight Online direct connect

Server   Firewall
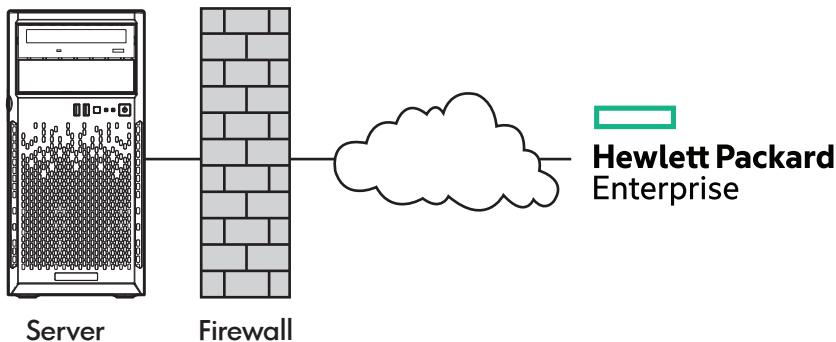
Insight Remote Support central connect

Register a server with Hewlett Packard Enterprise through an Insight Remote Support centralized host server in your local environment. All configuration and service event information is routed through the host server. This information can be viewed by using the local Insight RS Console or the web-based view in Insight Online (if it is enabled in Insight RS).

Figure 2 (page 14) shows the central connect configuration with a server.

Figure 2 Insight Remote Support central connect

Server   Insight RS   Firewall
              host server
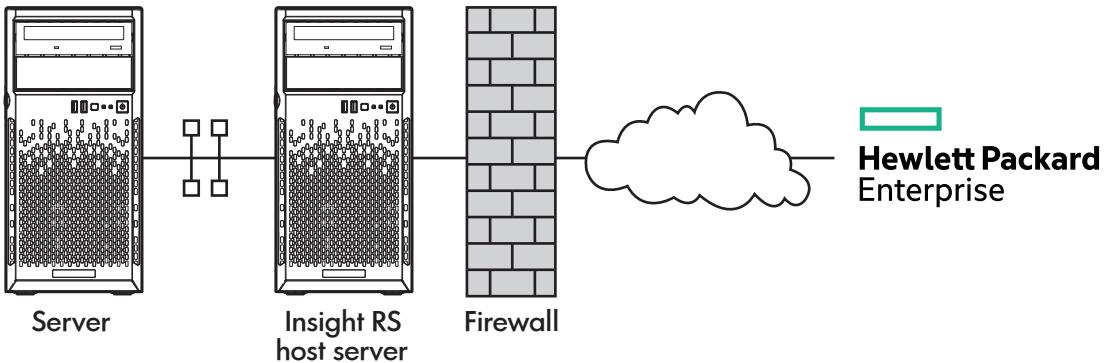
Device support

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

Insight Online direct connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

Insight Remote Support central connect

- ProLiant Gen8 servers
- ProLiant Gen9 servers

If you use HPE OneView to manage your environment, use HPE OneView to register for remote support. For more information, see the HPE OneView user guide.

Data collected by HPE remote support

When a server is registered for remote support, iLO collects Active Health System and server configuration information, and then iLO or the Insight RS host server sends this information to Hewlett Packard Enterprise. Active Health System information is sent every 7 days, and configuration information is sent every 30 days. The following information is included:

- **Registration**—During server registration, iLO collects data to uniquely identify the server hardware. Registration data includes the following:
  - Server model
  - Serial number
  - iLO NIC address
- **Service events**—When service events are recorded, iLO collects data to uniquely identify the relevant hardware component. Service event data includes the following:
  - Server model
  - Serial number
  - Part number of the hardware component
  - Description, location, and other identifying characteristics of the hardware component
- **Configuration**—During data collection, iLO collects data to enable proactive advice and consulting. Configuration data includes the following:
  - Server model
  - Serial number
  - Processor model, speed, and utilization
  - Storage capacity, speed, and utilization
  - Memory capacity, speed, and utilization
  - Firmware/BIOS
  - Installed drivers, services, and applications (if AMS is installed)
- **Active Health System**—During data collection, iLO collects data about the health, configuration, and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis.

For information about data collection, see the iLO user guide.

HPE Proactive Care service

HPE Proactive Care service customers must register their servers for remote support to receive the following Proactive Care features: Proactive Scan Report and Firmware and Software Version Report.

- The direct connect option requires the installation of AMS.

- The central connect option requires the installation of AMS or the SNMP/WBEM agents.

For more information, see the following website: **http://www.hpe.com/services/proactivecarecentral**.

Prerequisites for remote support registration

- The server supports embedded remote support registration through Intelligent Provisioning.

ⓘ **IMPORTANT:** If you use HPE OneView to manage your environment, use HPE OneView to register for remote support. For more information, see the HPE OneView documentation at **http://www.hpe.com/info/oneview/docs**.

- Your environment meets the requirements for remote support registration. For more information, see the Insight Remote Support and Insight Online setup guide for ProLiant Servers and BladeSystem c-Class Enclosures at the following website: **http://www.hpe.com/info/insightremotesupport/docs**.

- A supported version of Intelligent Provisioning is installed.

  Version 2.01 or later is required for remote support registration.

- iLO is configured as follows:

  ○ A supported version of the iLO firmware is installed.

    To address third-party software vulnerabilities, Hewlett Packard Enterprise recommends using iLO 4 2.03 or later.

  ○ The time zone is set in iLO.

  ○ A DNS server is configured in iLO.

    This is required for communication between iLO and Insight Online.

  For information about configuring iLO, see the iLO 4 user guide.

- For Insight Remote Support central connect only: A supported version of the Insight RS software is installed and configured on the Insight RS host server.

- For Insight Remote Support central connect only: The RIBCL protocol credentials for the server are configured in the Insight RS Console.

  For more information about the RIBCL protocol credentials, see the Insight Remote Support installation and configuration guide.

More information

Device support
Updating firmware

Registering for Insight Online direct connect

When you register for Insight Online direct connect, you must complete steps in both Intelligent Provisioning and the Insight Online portal.

Prerequisites

- Your environment meets the prerequisites described in "Prerequisites for remote support registration" (page 16).

- You have an HP Passport account. For more information, see **http://www.hpe.com/info/insightonline**.

Registering for Insight Online direct connect (step 1)

1. If the **Get Connected to Hewlett Packard Enterprise** window is not already open from the previous step of the initial configuration and registration tasks, navigate to the **Perform Maintenance** page in Intelligent Provisioning, and then select **HPE Insight Remote Support**.

2. Select **Connect this server directly to HPE**.
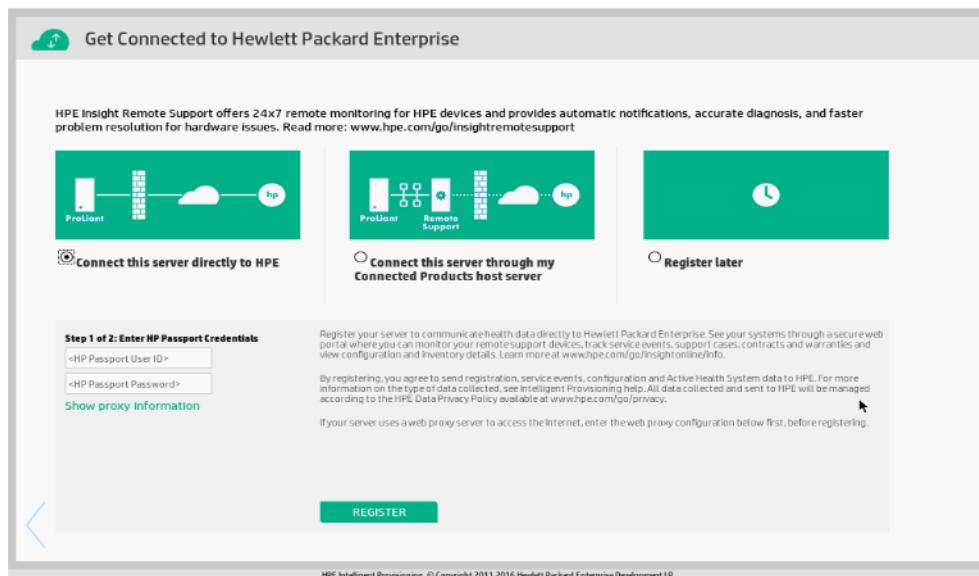
3. Enter your HP Passport user ID and password.

4. Optional: If the server uses a web proxy server to access the Internet, click **Show proxy information**, and then enter the following:

    - **Web Proxy Server**—Enter the hostname or IP address.

    - **Web Proxy Port**

    - **Web Proxy Username**

    - **Web Proxy Password**

5. Click **Register**.

   Intelligent Provisioning notifies you that Step 1 of the registration process is finished, and prompts you to complete Step 2.
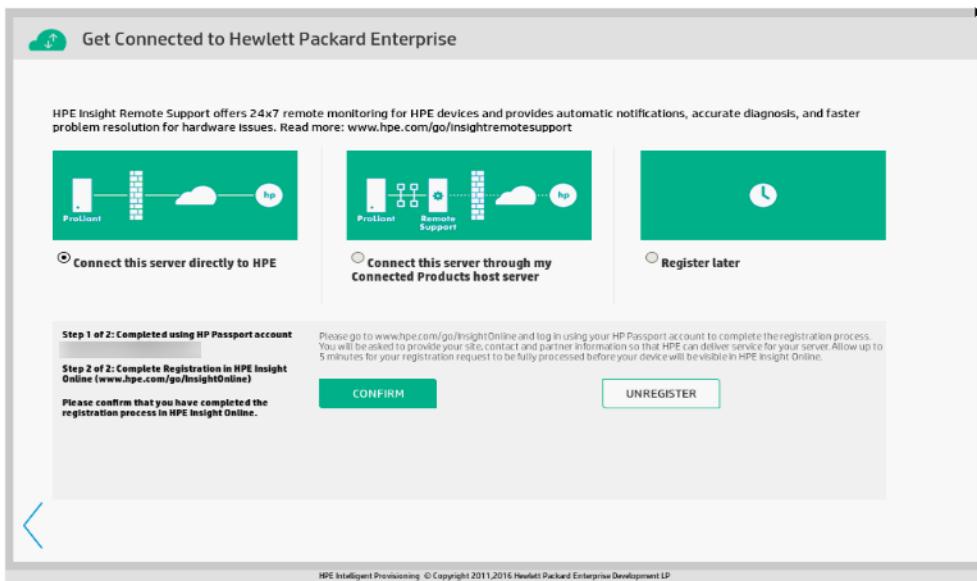
   Allow up to 5 minutes for your registration request to be fully processed.

Registering for Insight Online direct connect (step 2)

1. Navigate to the Insight Online website at **http://www.hpe.com/info/InsightOnline**, and then log in with your HP Passport credentials.
2. Follow the onscreen instructions in Insight Online, and provide your site, contact, and partner information so Hewlett Packard Enterprise can deliver service for your server.

   To streamline the process when you have multiple servers to register, complete Step 1 for all of the servers, and then complete Step 2 for all of the servers during one Insight Online session.

   For detailed instructions, see the Insight Remote Support and Insight Online setup guide for ProLiant servers and BladeSystem c-Class enclosures.

Confirming that registration is complete

1. Return to the remote support registration page in Intelligent Provisioning, and then click **Confirm**.

   Intelligent Provisioning notifies you that the registration process is finished.
2. To proceed to the Intelligent Provisioning home page, click the **Continue** right arrow.

Completing the post-registration steps

To ensure successful remote support operation, complete the following steps after you install the system software:

1. Optional: Verify that the server operating system is running and AMS is installed.

   Hewlett Packard Enterprise recommends installing AMS. For more information, see the iLO 4 user guide.

   AMS is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.

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

   Using AMS is one way in which iLO can obtain the server name. If iLO cannot obtain the server name, the displayed server name in Insight Online and Insight RS is derived from the server serial number.

2. If you did not install AMS, do one of the following to ensure that the server name is displayed correctly in Insight Online and Insight RS:

   - For Windows systems only, start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.

   - Configure the **Server Name** on the **Administration→Access Settings** page in the iLO web interface.

     To protect your privacy, do not use sensitive information in the names of your ProLiant servers. When you register a server for remote support, the server name is displayed in Insight Online and Insight RS.

3. Verify that the ProLiant iLO 3/4 Channel Interface Driver is installed.

   This driver is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.

   This driver ships standard with SUSE Linux Enterprise Server 11 and 12 and Red Hat Enterprise Linux 6 and 7, and it is automatically loaded.

   For more information, see the iLO 4 user guide.

4. Optional: If you want to receive email alerts about system events, configure AlertMail on the **Administration→Management→AlertMail** page in iLO.

   For more information, see the iLO 4 user guide.

Registering for Insight Remote Support central connect

Prerequisites

Your environment meets the prerequisites described in .

Registering for Insight Remote Support central connect

1. If the **Get Connected to Hewlett Packard Enterprise** window is not already open from the previous step of the initial configuration and registration tasks, navigate to the **Perform Maintenance** page in Intelligent Provisioning, and then select **HPE Insight Remote Support**.
2. Select **Connect this server through my Connected Products host server**.
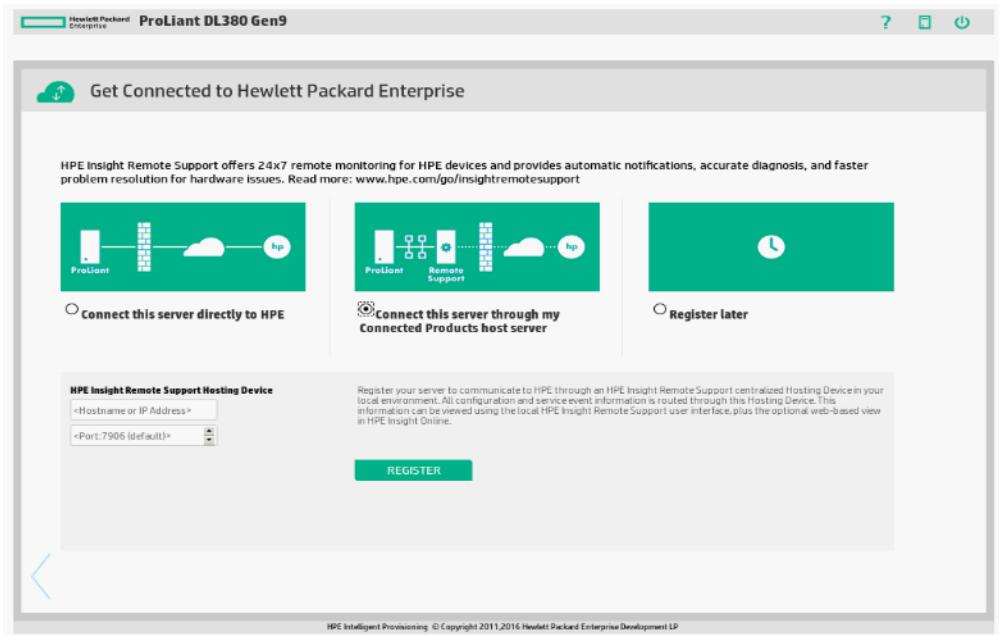
3. Enter the host server host name or IP address and port number.

   The default port is 7906.

4. Click **Register**.

   Intelligent Provisioning notifies you that the registration process is finished.

5. To proceed to the Intelligent Provisioning home page, click the **Continue** right arrow.

Completing the post-registration steps

To ensure successful remote support operation, complete the following steps after you install the system software:

1. Optional: Verify that the server operating system is running and AMS is installed.

   Hewlett Packard Enterprise recommends installing AMS. For more information, see the iLO 4 user guide.

   AMS is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.

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

   Using AMS is one way in which iLO can obtain the server name. If iLO cannot obtain the server name, the displayed server name in Insight Online and Insight RS is derived from the server serial number.

2. If you did not install AMS, do one of the following to ensure that the server name is displayed correctly in Insight Online and Insight RS:

   - For Windows systems only, start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.

   - Configure the **Server Name** on the **Administration→Access Settings** page in the iLO web interface.

     To protect your privacy, do not use sensitive information in the names of your ProLiant servers. When you register a server for remote support, the server name is displayed in Insight Online and Insight RS.

3. Verify that the ProLiant iLO 3/4 Channel Interface Driver is installed.

This driver is installed automatically if you use the Intelligent Provisioning **Recommended** installation method for Windows installation.

This driver ships standard with SUSE Linux Enterprise Server 11 and 12 and Red Hat Enterprise Linux 6 and 7, and it is automatically loaded.

For more information, see the iLO 4 user guide.

Registering for remote support after the initial configuration and registration tasks

If you want to register this server for remote support after the initial configuration and registration tasks:

1. Select **Register Later** on the registration page.
2. Click the **Continue** right arrow.

When you are ready to register this server for remote support, navigate to the **Perform Maintenance** screen and select **HPE Insight Remote Support**.

For registration instructions, see "Registering for Insight Online direct connect" (page 16) and "Registering for Insight Remote Support central connect" (page 19).

Reinstalling Intelligent Provisioning

You can reinstall Intelligent Provisioning instead of using the Firmware Update Utility to ensure you have the latest version. There are two methods for reinstalling Intelligent Provisioning.

Reinstalling from ISO image

1. Download the ISO image file for the latest Intelligent Provisioning recovery media from the Intelligent Provisioning website (**http://www.hpe.com/info/intelligentprovisioning**).
2. Boot to the Intelligent Provisioning recovery media. The installation automatically begins.
3. When the update is complete, the server automatically reboots.

Reinstalling from RPM package (Linux only)

1. Download the RPM package file for the latest Intelligent Provisioning recovery RPM package from the SDR website (**https://downloads.linux.hpe.com/SDR/repo/ip/**).
2. Execute command: `#rpm -ivh gaius_installer-2.xx-xx.noarch.rpm`.
3. Execute command: `#reboot`.

3 Server configuration and OS installation

Configuring the server and installing an OS

To use Intelligent Provisioning to configure the hardware and install an OS on your ProLiant Gen9 server, follow the on-screen prompts in the **Configure and Install** menu to complete the following tasks:

Server support and special characters

- The ProLiant ML10 Gen9 Server and the ProLiant ML10 v2 Server do not support Intelligent Provisioning. For information on installing an OS on these servers, see the server documentation.

- ProLiant SL, SE, and XL Servers (except the ProLiant XL420 Gen9 Server) do not support operating system installations with Intelligent Provisioning. These servers do support the maintenance features described in "Performing maintenance" (page 36), except deploying the operating systems installations.

- Special characters can be used in passwords only. Do not use special characters in any other data fields. Special characters and spaces are not supported in any path name.

Available install methods, source media types, and formats supported for each OS family

Each Configure and Install screen provides a guided method of configuring the server, installing an OS, and updating the system software. The following table shows the install methods, source media types, and formats supported for each OS family.

ⓘ **IMPORTANT:** Intelligent Provisioning only supports original, licensed vendor media or Hewlett Packard Enterprise-branded versions. Demo or developer versions of the OS, or media which has been modified to slipstream custom software or service packs, are not supported and may not be correctly identified by the installation process.

	Recommended install method				Customized install method				Manual
	Disc	**Network Share**	**FTP**	**USB**	**Disc**	**Network Share**	**FTP**	**USB**	**Disc**
Microsoft Windows (64–bit)	ISO VM ISO	Flat ISO	—	Flat ISO	ISO VM ISO	Flat ISO	—	Flat ISO	ISO VM ISO
VMware ESXi	ISO VM ISO	Flat ISO	Flat	Flat ISO	ISO VM ISO	Flat ISO	Flat	Flat ISO	ISO VM ISO
SUSE Linux Enterprise Server	ISO VM ISO	Flat ISO	—	—	—	—	—	—	ISO VM ISO (kISO is required if the latest CPU/chipset

	Recommended install method				Customized install method				Manual
	Disc	Network Share	FTP	USB	Disc	Network Share	FTP	USB	Disc
									is not supported)
Red Hat Enterprise Linux	ISO VM ISO	—	Flat	—	—	—	—	—	ISO VM ISO

Formats:

- Flat—Standard folder structure

- ISO—ISO or UDF file

- VM ISO—iLO Virtual Media ISO

- VM NET—iLO Virtual Media folder share

- VM USB—iLO Virtual Media USB

More information

http://www.hpe.com/info/ossupport

Using an SD card as a boot device

With Intelligent Provisioning, you can use an Hewlett Packard Enterprise-supplied SD card as a target for deploying an OS. Only the following SD cards are supported as an alternative OS boot device:

VMware

- 8 GB USB Enterprise Mainstream Flash Media Drive Key Kit (737953-B21)

- 8 GB microSD Enterprise Mainstream Flash Media Kit (726116-B21)

VMware and Windows

- 32 GB SD Enterprise Mainstream Flash Media Kit (700136-B21)

- 32 GB microSD Enterprise Mainstream Flash Media Kit (700139–B21)

NOTE:
- Intelligent Provisioning does not support installing a VMware ESXi operating system to any SD or microSD card.

- SD Boot does not support deployment installations.

These SD cards can be used as an alternative to hard drive or solid state drive storage for deploying an OS on ProLiant Gen9 servers. Using an SD card as a target for deploying an OS provides the following advantages:

- Deploys OSs to diskless servers and SAN storage

- Uses less power than traditional drives

- Reduces temperature, decreasing throttling and A/C costs

- Reduces vibration, particularly in environments with high G-force

- Frees drive bays for other uses

More information

Step 1: Selecting hardware settings

In the first configuration screen, enter global settings to control power use, software updates, and array configuration.
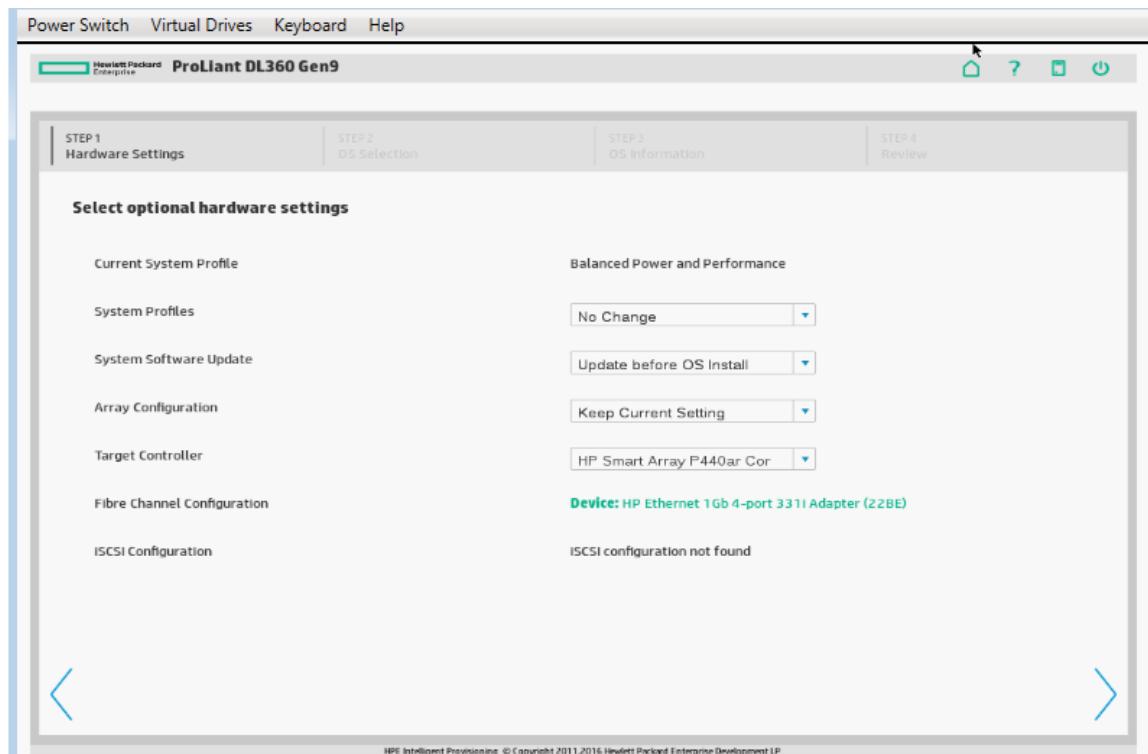
⚠ **IMPORTANT:** If unsupported media devices are connected at this point, an error appears. To resolve the issue, remove the unsupported media device, and make sure you have network share information available, a disk or ISO, or USB drive installed when prompted.

1. Select the power management System Profile to use. These profiles set a basic policy for performance versus power usage without having to configure individual settings through the UEFI System Utilities menus.

   The current (or a recommended) profile is displayed, but to change the settings, the options include:

   - **No Change**

   - **Balanced Power and Performance**

   - **Minimum Power Usage**

   - **Maximum Performance**

   The suggested default varies. If Intelligent Provisioning detects existing settings on the server that match one of these profiles, that profile is displayed in the System Profiles field. If Intelligent Provisioning detects settings that do not match one of the profiles, **No Change** is displayed in this field.

2. Select whether to perform a software update before the OS is installed.

3. Enter array configuration specifications for the server's storage subsystem.

Options include:

- **Keep Current Setting**—Uses existing settings to maintain any previously constructed arrays. Use this option when reprovisioning a server. This option is displayed only when valid logical drives are present on the server. For new server installations, this option is not displayed.

  NOTE:

  Secure Boot is available on systems running Windows Server 2012 R2 and Windows Server 2012.

- **Recommended Settings**—HPE SSA polls any drives that are present and builds an appropriate array for those drives. For example, if two drives are connected to the Smart Array card, the setup defaults to RAID 1. Hewlett Packard Enterprise recommends selecting this option when initially provisioning a server.

  △ **CAUTION:** Selecting this choice resets all disks (and arrays, if any are present). Because no arrays or disk data are present during a first-time setup, this does not affect your server. However, if you choose this option when reprovisioning your server, you can lose your data and any disk arrays. For more information about HPE SSA, see the HPE Smart Storage Administrator user guide (**http://www.hpe.com/support/SSA_UG_en**).

- **Customize**—Opens HPE SSA (after clicking the **Continue** right arrow) and enables you to choose array settings.

  NOTE: Some controllers other than Smart Array controllers can be configured through HPE SSA.

4. Select the Target Controller you want to use from the drop-down menu if more than one is available.

5. Confirm Fibre Channel and iSCSI configuration settings.

   If discovered, the Fibre Channel and iSCSI information is displayed at the bottom of the screen.

   Intelligent Provisioning supports installation to iSCSI targets and to shared storage devices. Before starting an installation, the devices need to be set up outside of Intelligent Provisioning, using options that appear during POST, or through their setup applications. In addition, the boot controller order needs to be set correctly in the UEFI System Utilities before installation.

6. Confirm SD Card Configuration settings. If a supported SD card is installed, the device details appear.

7. Click the **Continue** right arrow.

More information

Step 2: Selecting the OS
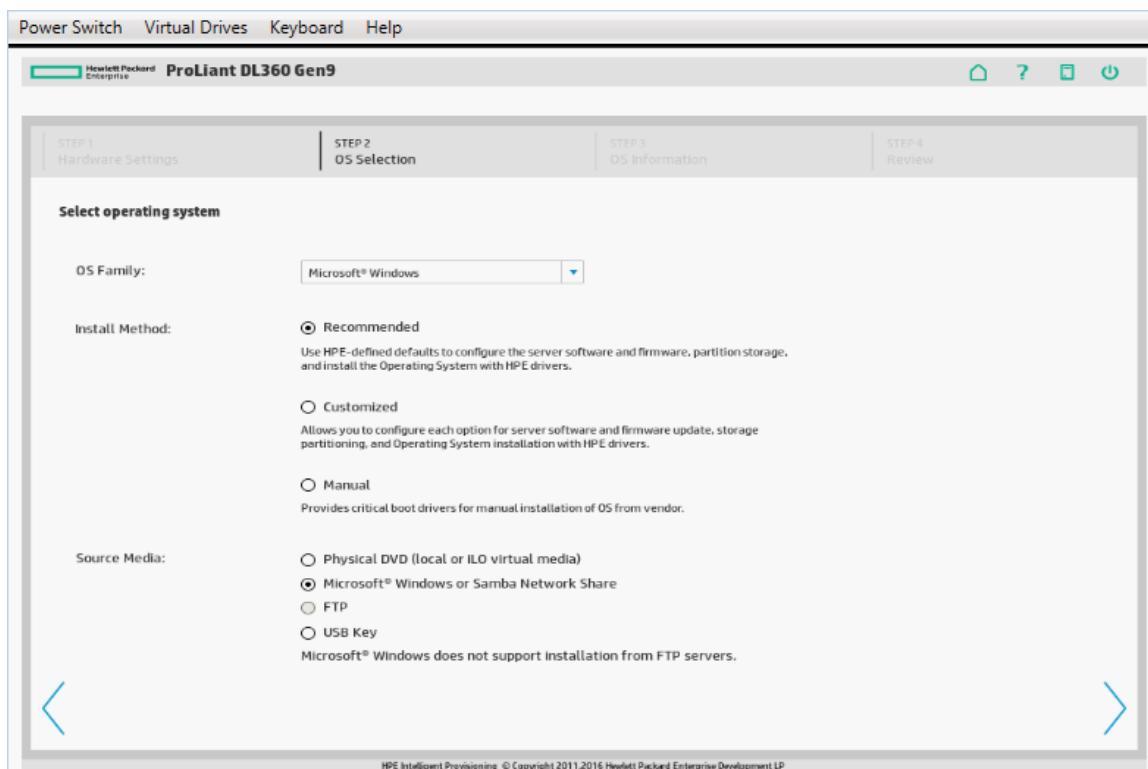
IMPORTANT: If unsupported media devices are connected at this point, the following error appears: `There are no physical disks attached`. To resolve the issue, remove the unsupported media device, and make sure you have network share information available, or a disk or ISO, or USB drive installed when prompted.

1. Select an OS family.

    Available supported OS families include:

    - Microsoft Windows

    - VMware ESXi/vSphere Custom Image

    - SUSE Linux Enterprise Server

    - Red Hat Enterprise Linux

IMPORTANT:

- When installing VMware, download an HPE Custom ISO before the installation from the website (**http://www.hpe.com/info/esxidownload**). Ethernet port 0 must be active.

NOTE:

- A software license must be accepted when installing Microsoft Windows or Red Hat Enterprise Linux 7.X.

- If updates are available, a message appears on the screen directing you to the proper steps for incorporating them into Intelligent Provisioning.

2. Select an installation method.

    Depending on the OS family selected, installation choices vary, including the suggested default. For more information, see "Available install methods, source media types, and formats supported for each OS family" (page 22).

Options may include:

- **Recommended**—This express installation process uses Hewlett Packard Enterprise-defined defaults to configure the server software and firmware, partition storage, and install the OS with drivers. It also performs a software and firmware update if the network is available at your location. Hewlett Packard Enterprise recommends selecting this option for first-time server setup. For more information about recommended installation options, see "Entering OS information required for recommended installations" (page 29).

  NOTE: AMS and the ProLiant iLO 3/4 Channel Interface Driver are installed automatically if you use the **Recommended** installation method for Windows installation. The ProLiant iLO 3/4 Channel Interface Driver is standard for SUSE Linux Enterprise Server 11 and 12 and Red Hat Enterprise 6 and 7.

- **Customized**—A full interview with a wizard that provides the network setup, remote support registration, the systems software, the server hardware configuration, RAID configuration, options for server software and firmware updates, storage partitioning, and OS installation with drivers. Select this option if you have specific parameters that differ from the recommended settings, such as for storage partitioning. For more information about customized installation options, see "Entering OS information required for customized installations" (page 32).

- **Manual**—Installs the OS from a custom OS CD/DVD without searching the Web. After selecting this option, insert the provided CD/DVD so that the server can reboot from the OS CD/DVD.

  The Virtual Install Disk (VID) is disabled by default. If you enable VID, a USB mass-storage device appears with the name of the VID during the OS installation process. The VID contains a limited set of storage and networking drivers, so any required SAS/iSCSI/FCoE adapter can be loaded in the event that the OS disc does not have the appropriate drivers. Because the VID and the custom CD/DVD might not contain all of the needed drivers, you might need to create a driver CD/DVD to ensure that all required drivers are installed and that the OS can install successfully. For information about creating a driver disk, see the OS installation guide. For information on enabling the VID, see "Enabling the VID" (page 35).

  In all Linux environments, add `dd` (Red Hat Enterprise Linux 6), `inst.dd` (Red Hat Enterprise Linux 7), `dud=1` (SUSE Linux Enterprise Server 11 and 12) on the command line to provide a driver location only when installing the OS in special storage devices such as iSCSI and FC LUNs.

  In Red Hat Enterprise Linux 6 installations with a SATA controller, the selected Install Target Device must be a drive connected to the lowest bay number.

  The following table contains information about Linux boot driver parameters.

Linux edition	Issue	Solution	Example
SUSE Linux Enterprise Server	Because of a naming convention conflict between	To access the SP2 drivers in the VID, include the	`updatedir=` `/linux/suse/i386-sles11.2`

Linux edition	Issue	Solution	Example
	SUSE Linux Enterprise Server 11 SP1 and SP2, the SP2 drivers are located in a directory that the SUSE installer does not see.	*updatedir* kernel parameter for the appropriate OS.	`broken_modules=ahci for sles11, sles12`
Red Hat Enterprise Linux	Because the AHCI driver is loaded before the HPE Dynamic Smart Array B140i Controller drivers, the logical drive for B140i is not recognized.	Enter the following boot parameters to prevent the driver from taking over the controller.	`blacklist=ahci for rhel6 modprobe.blacklist=ahci for rhel7`

3. Select the source media from which you are installing the OS.

    Media types include:

    - **Physical DVD or iLO virtual media** (default)—A standard bootable OS DVD/CD-ROM media, and virtual media through iLO.

        NOTE: Select this option when using a DVD drive connected to a USB port.

    - **Microsoft Windows or Samba Network Share**—The network share that contains the OS installation files.

    - **FTP**—The FTP server that contains OS installation files.

        NOTE: The FTP media option is supported for VMware and Red Hat Enterprise Linux only.

    - **USB Key**—The USB flash drive that contains the OS installation files

        NOTE: Only FAT-formatted USB drives are supported. For OS image files that cannot copy to the USB unless it is NTFS-formatted, use a different source media, such as a DVD, network share, or FTP server.

4. If you are installing from a CD/DVD disk or USB drive, insert the media.
5. Click the **Continue** right arrow to go to the next screen, which varies, depending on the media type.

    Insert the disc or USB media, or enter the information needed to access the installation files on the network share or FTP site. Depending on the media type, supply the following information.

Media type	Required information/action
Disc	Insert the disc.
Network share	Enter network connection information, including: - **Server Name or IP Address**—Server name or IP address of the server that hosts the OS contents. If a server name is specified, a DNS entry is also required. - **Share Name**—The name of the network share using Server Message Block (SMB) protocol that hosts the OS contents.

Media type	Required information/action
	• **Network Share User**—User name used to access the network share. • **Network Share Password (not encrypted)**—Password for the user name used to access the network share.
FTP	Enter network connection information, including: • **Server Name or IP Address**—FTP server name or IP address of the server that hosts the OS contents. FTP support requires anonymous access to the FTP server and does not support connecting to an FTP server through a proxy. IMPORTANT: When entering an FTP path, remove spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).
USB	Insert the USB drive and browse to the location of the OS installation files on the USB drive. Then, double-click the ISO file.

6. Click the **Continue** right arrow to proceed to the next screen in the automated process.

Step 3: Entering OS information

In this step the necessary OS information is specified.

Entering OS information required for recommended installations

Depending on the OS you are installing, you may be prompted to enter or confirm the following information:

1. Select the OS family and edition.

    - When installing Microsoft Hyper-V Server 2012, you must select the Windows 2012 OS family and the Hyper-V OS.

    - When installing Microsoft Hyper-V Server 2012 R2, you must select Windows 2012 R2 as OS family and the Hyper-V OS.

2. Select the OS and the keyboard language.

3. Enter the product key. (Not displayed for all OSs)

    This is the Product Identification (Product ID) number. If you do not enter a product key and one is required, the OS installation pauses indefinitely, prompting you to enter the key. The installation resumes after you enter the product key.

4. Enter the computer name (optional) and an administrator password (optional).

5. Click the **Continue** right arrow to proceed to .

Using StoreVirtual VSA (Virtual Storage Appliance) software

Using StoreVirtual VSA involves the following steps:

StoreVirtual VSA

During OS installation you can deploy StoreVirtual VSA, which enables you to create fully featured shared storage on a virtualized server. The StoreVirtual VSA software is a virtual machine that supports hypervisor environments. VSA provides shared storage for both VMware ESX / ESXi and Microsoft Hyper-V hypervisor environments. When deploying VSA, you can retrieve your free 1 TB license key and activate it.

StoreVirtual VSA system requirements

- The deployment of StoreVirtual VSA is supported only during recommended and custom installations for Windows, and only during custom installations for VMware. It is not supported during manual installation.

- The server must be connected to a network to deploy StoreVirtual VSA.

- StoreVirtual VSA is supported with vSphere or Microsoft Hyper-V on the following operating systems:

    - VMware ESXi 5.5 Update 3, ESXi 5.1 Update 3, vSphere 6.0 Update 2

    - Microsoft Windows Server 2012

    - Microsoft Windows Server 2012 R2

More information

www.hpe.com/storage/tryVSA

Deploying StoreVirtual VSA

1. Navigate to the **Software-Defined Storage** page and select a VSA type.

   If you do not want to deploy the StoreVirtual VSA software, select **Continue without deploying VSA** and click the **Continue** right arrow. A screen is displayed indicating VSA will not be installed. Click the **Continue** right arrow to continue.

   VSA validation begins. If VSA is not available, click the **Continue** right arrow to confirm OS selections.
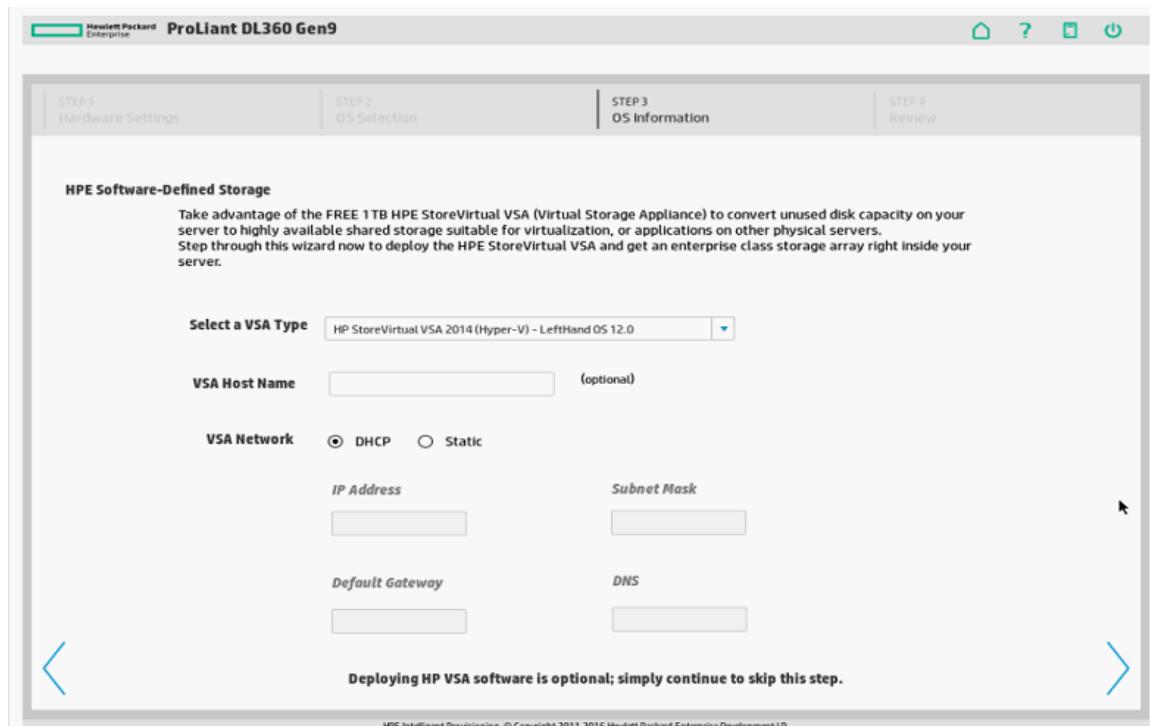
2. Enter an optional **VSA Host Name**.
3. Select the **VSA Network** type (**DHCP** or **Static**).
4. If **Static** is selected, enter the associated network parameters.
5. Click the **Continue** right arrow.

Entering VSA contact information

You must provide all required contact information to deploy StoreVirtual VSA. If you do not wish to provide contact information, it will be necessary to select **Continue without deploying VSA**.

1. Enter the appropriate contact information. All required fields must be entered.

   The contact information is validated and if any fields are not valid you are prompted to enter them.

2. Optional: To receive new product information, select the **Sign me up...** option.
3. Click the **Continue** right arrow.

Data privacy

The collected contact data is managed according to the Hewlett Packard Enterprise privacy statement, available at **http://www.hpe.com/info/privacy**. You may be contacted by Hewlett Packard Enterprise.

Completing VSA deployment

1. Select the appropriate StoreVirtual Centralized Management Console, download and install it
2. Retrieve your free 1 TB license key and activate it.
3. Configure the Centralized Management Console.

More information

http://www.hpe.com/info/vsa1TB

Entering OS information required for customized installations

If you selected a Windows-based OS and a **Customized** installation method on the OS Selection screen ("Step 2: Selecting the OS" (page 26)), additional screens are displayed for you to enter custom operating installation and monitoring management protocol information.

Microsoft Windows configuration information for a customized installation
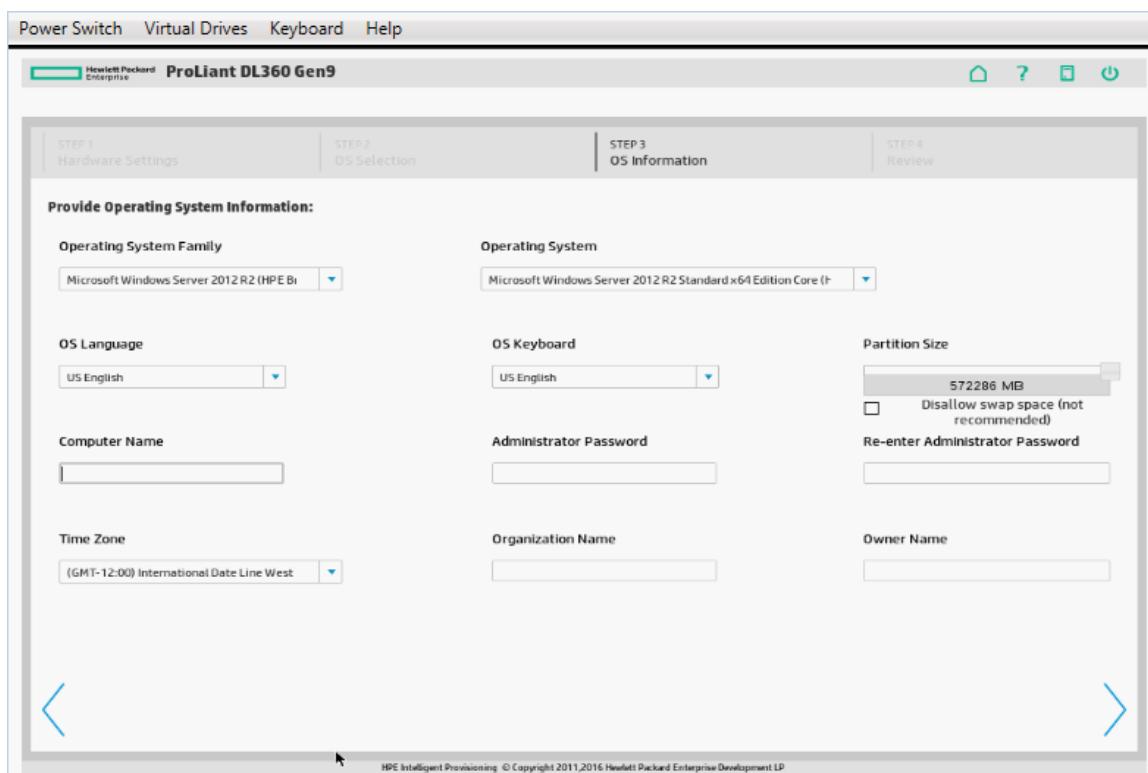
Depending on the type of Microsoft OS you are installing, you may be prompted to enter the following information:

1. Select the OS family and edition.

    When installing Microsoft Hyper-V Server 2012, you must select the Windows 2012 OS family and the Hyper-V OS. If a different OS family is selected, the installation will fail, generating the following error message: `Unattended settings error.`

    NOTE: When installing Windows 2012 R2, you must select Windows 2012 R2 as the OS family and an appropriate OS must be selected.

2. Select the OS and keyboard language.
3. Select a partition size.

    This is the size of the partition to create as the C: drive and in which to install the OS.

By default, the value is set to the maximum-allowed size (the size of the logical drive.) The minimum-allowed size varies and is determined by the selected OS.

- To change the size of the partition from the default, slide the bar above the field left or right to reduce or increase size. This option is not available when installing Microsoft Windows Essentials OSs, because custom partitioning is not supported in the Essentials OSs.)

- To create a partition size based on the provided default, but reducing it by the amount set aside for the swap space (pagefile), select **Disallow swap space (not recommended)**. Select this option only when the pagefile is located elsewhere.

NOTE: Partitioning the disk might take up to 20 minutes to complete.

4. Enter the product key.

   This is the Microsoft Product Identification (Product ID) number. (Not displayed for all OSs).

5. Enter the computer name and an administrator password (optional).

   Hewlett Packard Enterprise recommends entering a personalized name instead of using the suggested default. When installing Microsoft Smart Business Server, Hewlett Packard Enterprise recommends entering the final system name during the installation.

   To protect your privacy, do not use sensitive information for the computer name. This name is visible in Insight RS and Insight Online, and can be viewed by support and your authorized service provider, reseller/distributor, and installer.

   If an administrator password is not entered at this time, you are prompted for a password during the first login. (Not displayed for all OSs.)

6. Select a time zone.

   The time zone is used by the OS to perform daylight saving time updates and other time-related functions.

7. Enter organization and owner names (optional).

VMware configuration information for customized Installation

If you selected a VMware OS and a **Customized** installation method on the OS Selection screen (), additional screens are displayed for you enter custom operating installation and monitoring management protocol information.

1. Enter a host name (optional).

   This name must be a minimum of three characters.

2. Enter a root password.

   For VMware, the initial password defaults to "password".

3. Specify the network type.

   Select **DHCP** or **Static**.

Step 4: Reviewing your settings
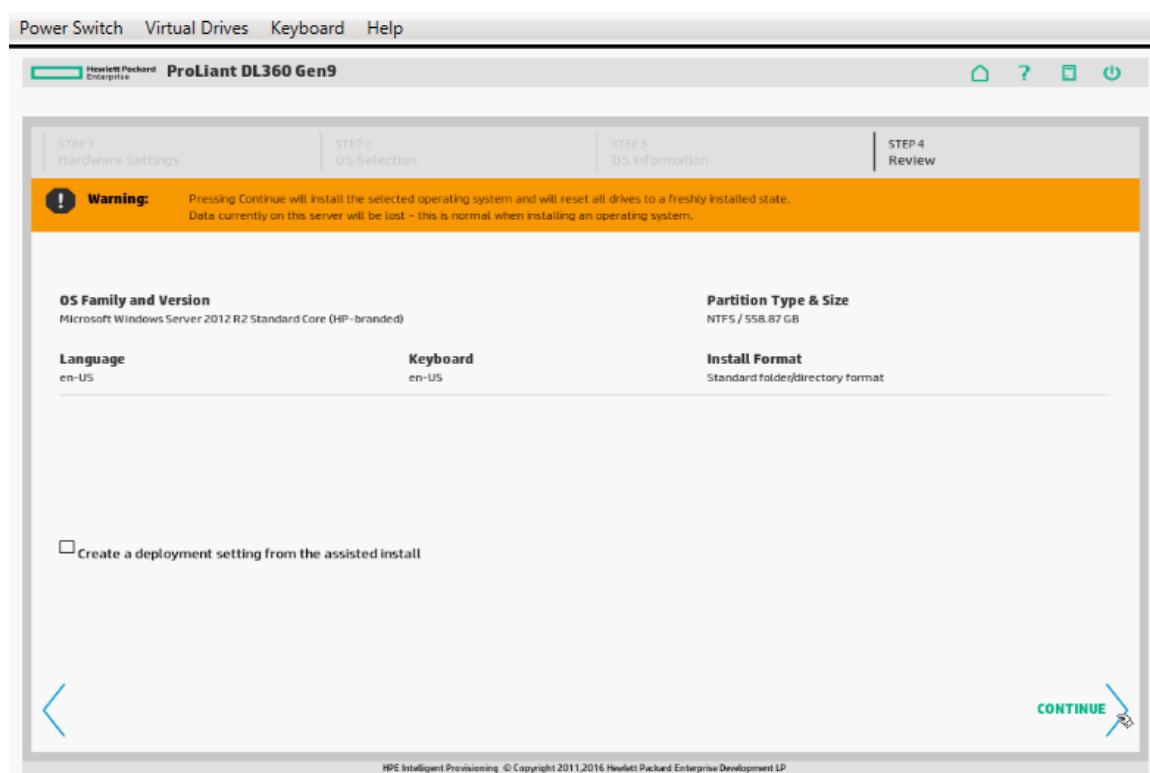
⚠ **CAUTION:** Continuing past this screen resets the drives to a newly installed state and installs the selected OS. Any existing information on the server is erased. This does not affect a first-time setup, because there is no data present on the server.

1. Review the information on the screen and confirm its accuracy.
2. Select **Create a deployment setting from the assisted install** to use these same settings at a later time to install and configure a different server.

    NOTE: Because Deployment Settings profiles support only the settings provided in the Recommended installation methods, if this is a Customized installation, settings that are unique to the Customized installation method are not captured.

3. Click the **Continue** right arrow to begin the automated installation and configuration process. Depending on the Deployment Settings, a variety of screens are displayed, providing progress information about the installation.

More information

Checking installation parameters

During the installation and configuration process, consider the following:

- A EULA might be displayed for Windows installations.

- The **Firmware Update** screen might be displayed at this time, depending on the following two system settings:

  - In the **Step 1: Set Preferences** screen, **System Software Update** must have been enabled.

  - In the **Step 1: Hardware Settings** screen, **Update before OS Install** must have been selected.

  If the **Firmware Update** screen is displayed, follow the on-screen prompts to obtain and install the latest firmware on server components. When the updates are complete, the Installing OS page is displayed, ready to begin the OS installation.

- If you attempt to deploy an OS on a server with no installed drives, the server reboots and, after POST, a page is displayed indicating that the settings are being applied. The deployment does not proceed, but messages are written to the IML.

- For Windows installations, messages about an untested Windows version and hpkeyclick messages might be displayed while the drivers are installed. This is expected behavior. No action is required.

More information

Enabling the VID

1. Reboot the server and press **F9** during POST to access the UEFI System Utilities.
2. Select **System Configuration→BIOS/Platform Configuration (RBSU)→System Options→USB Options→Virtual Install Disk**.

☼ **TIP:** You can use the same procedure to disable the VID if necessary.

---

4 Performing maintenance

The **Perform Maintenance** window contains the following maintenance-related tasks:

Downloading Active Health System data

HPE Support uses the Active Health System log file for problem resolution. To download Active Health System data:

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Active Health System download** from the maintenance options.

   The Active Health System download window is displayed.
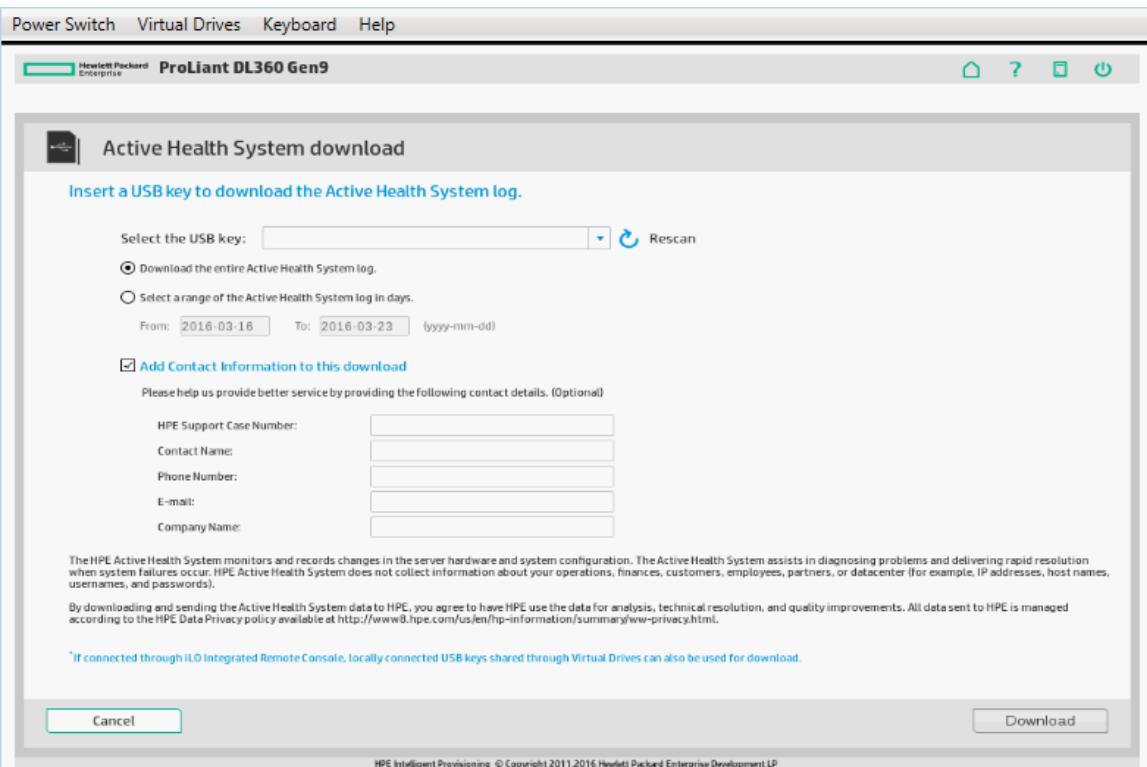
Use the **Active Health System download** screen to download Active Health System telemetry data from the server onto a USB key in the form of an Active Health System log file (`hp_serial#_date.ahs`). Use this screen to select the duration for which data needs to be extracted and the USB key as destination media. You can select a specific start and end date to limit the duration of data extraction. A sample of the Active Health System telemetry is displayed on the Active Health System download screen.

If connected through iLO, locally connected USB keys shared through virtual devices can also be used for saving Active Health System log information.

Using Active Health System download

To download Active Health System telemetry data using the Active Health System download feature:

1. Insert a USB key into the server.
2. Press the **F10** key to boot to Intelligent Provisioning during server boot.
3. Click **Active Health System download** from the Intelligent Provisioning Maintenance screen.
4. In the **Active Health System download** screen, select the USB key from the drop down list.

   NOTE: If you inserted the USB key after launching Active Health System Download, click **Rescan**.

5. Select the duration of data retrieval from the menu. Hewlett Packard Enterprise recommends retrieving seven days of data, which creates a 10 to 15 MB file.
6. Enter contact information (optional) in the form provided. The contact information helps customer services to provide better assistance.
7. Click **Download** to save the data to the USB key.

Submit the file to HPE Support

1. Compress the AHS log to facilitate emailing the file. Compressing the AHS log manually might reduce the file size by 50% or more.

2. Contact HPE Support, with the log file available for email submission.
3. After getting a Case ID from HPE Support, email the log file to `HPSupport_Global@hpe.com`, with the case ID in the subject. For example, **<CASE:123456789>**.
4. Be sure to attach your AHS log file to your open support case.

More information

http://www.hpe.com/info/AHSlog

Updating firmware

ProLiant Gen9 servers and their installed hardware options are pre-loaded with the latest firmware, but updated firmware might be available. For ProLiant Gen9 servers, use the Firmware Update utility to find and apply the latest firmware. Intelligent Provisioning updates can be performed when an SPP update is available.

To update firmware on a ProLiant Gen9 Server:
1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Firmware Update** from the maintenance options.

    The Firmware Update window is displayed.

Determining the installed Intelligent Provisioning version

To check the Intelligent Provisioning version, click the **System Information** icon in the Intelligent Provisioning window. The **Intelligent Provisioning Image** version is listed.

Updating Intelligent Provisioning and component firmware

NOTE: Firmware Update reflects the latest updates available as per the baseline defined in the latest SPP. Newer updates that were added outside of the latest SPP baseline do not appear on the updates list. The FTP site is migrating, and individual firmware updates will not appear until the migration to the new site is complete.

To update Intelligent Provisioning and component firmware:
1. Select **Firmware Update** in the **Perform Maintenance** window.

    Immediately after selecting this option, the system searches for firmware on the source configured in the System Software Update settings ("Setting Intelligent Provisioning Preferences" (page 39)). This might take a few minutes; wait for the display to generate the results.

    While the system is retrieving the data, click **More** or **Less** to show or hide search details.

    If preferred, download and copy the SPP ISO to a DVD or USB key. To download SPP, see the website (**http://www.hpe.com/servers/spp/download**). For instructions on using the ISO, see the SPP quick start guide on the website (**http://www.hpe.com/support/ SPP_UG_en**).

2. After the system retrieves the firmware data, it checks the installed hardware components to suggest items to update. Depending on the search, you might be prompted to click **Continue** to begin the hardware components check.

    This might take a few minutes; wait for the display to generate the results.
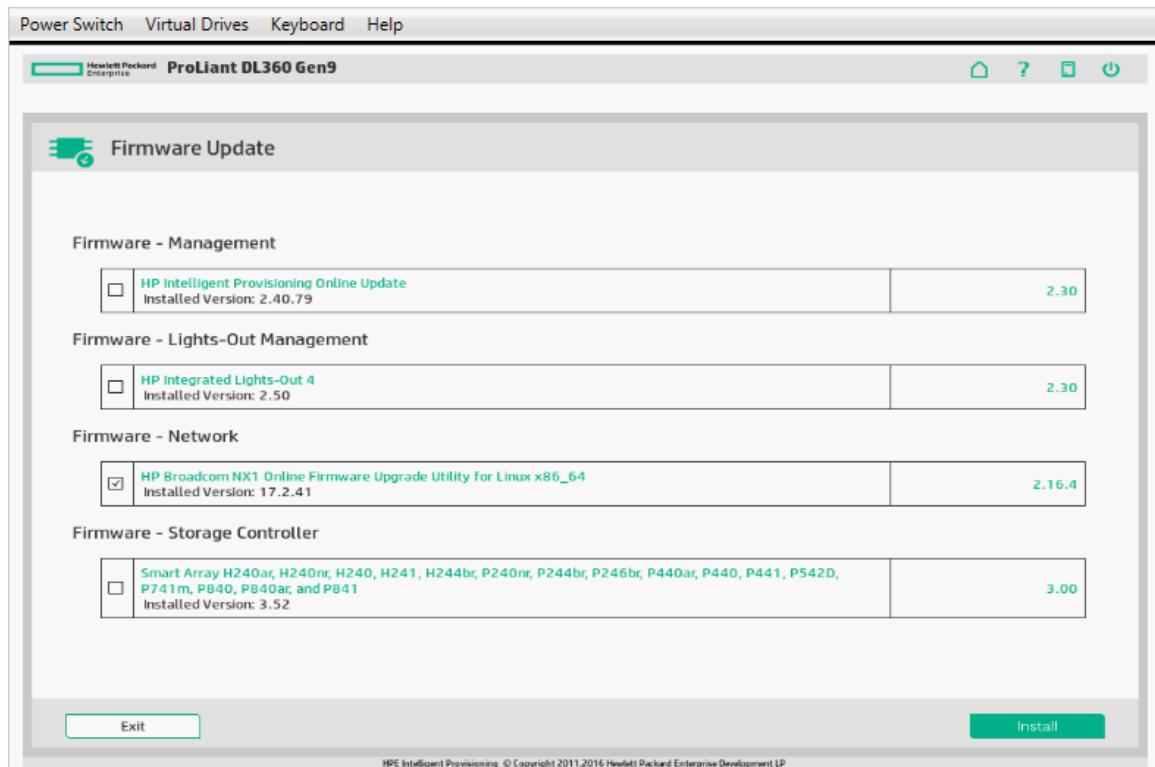
NOTE: If no new firmware is available, the current version is displayed in the Firmware Update screen.

3. Select the items to update, and then click **Install**.

   The table is redisplayed, with only the selected items listed.

4. To install all of the listed components, click **Continue**.

5. If you are ready to perform the installation, click **Continue** at the warning.

   After each component is installed, a green check automatically appears in the left column next to the component name.

6. After all components are installed, click **Exit** to return to the Perform Maintenance screen.

   Restart the OS.

Setting Intelligent Provisioning Preferences

Use Intelligent Provisioning Preferences to change basic preferences, including the interface and keyboard languages, network and share setting, system date and time, and software update settings. In addition, the EULA is accessible from this screen.

To set Intelligent Provisioning Preferences:

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.

2. Select **Intelligent Provisioning Preferences** from the maintenance options.

   The Intelligent Provisioning Preferences window is displayed.
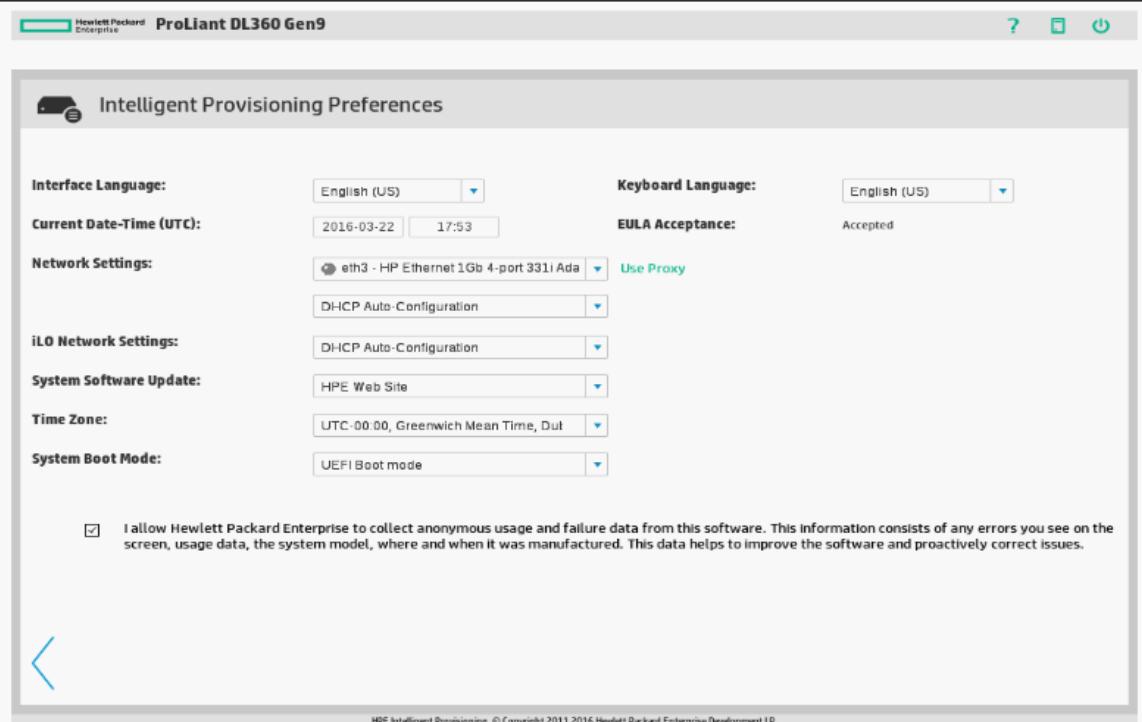
When Intelligent Provisioning is run for the first time on a server, this is the first screen that is displayed within Intelligent Provisioning. For more information about the fields in this screen, see "Step 1: Set Intelligent Provisioning preferences" (page 10).

Using Deployment Settings

Deployment Settings enable you to create a server configuration package that you can deploy to one or more ProLiant Gen9 servers using a USB key and iLO Scripting. Using Deployment Settings is an alternative to using the Scripting Toolkit.

To use Deployment Settings:

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Deployment Settings** from the maintenance options.

   The Deployment Settings window is displayed.
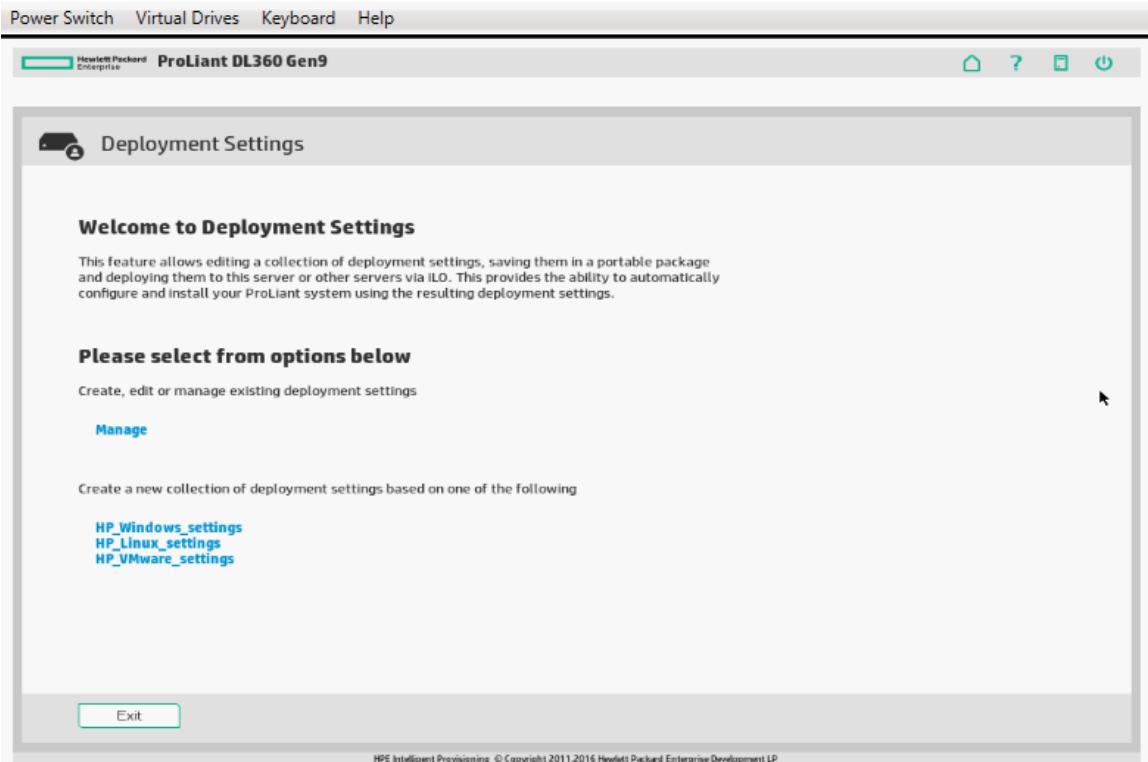
NOTE: Creating a deployment setting from the Assisted Installation option is only supported for Windows installs.

When you open Deployment Settings, you can choose to manage an existing Deployment Settings profile or create a new one.

Creating a Deployment Settings package

To create a Deployment Settings package:

1. From the Deployment Settings window, select one of the following:

    - To create a new, custom Deployment Settings profile or modify an existing Deployment Settings profile, click **Manage**.

    - To create a new Deployment Settings profile based on one of the provided default profiles, select one of the templates at the bottom of the page.

2. Navigate through the options in the Deployment Settings windows, entering the appropriate information.

3. Click **Save**. When prompted, enter a name and navigate to a USB key on which to save the Deployment Settings.

ⓘ **IMPORTANT:** Deployment Settings package names cannot include spaces.

Using a Deployment Settings package to configure a single server

ⓘ **IMPORTANT:**

- Before using a deployment to install an OS, be sure that the drives and arrays are configured.

- Do not interrupt the configuration process.

- Deployment Settings are not compatible with an SD card OS installation.

To use a Deployment Settings package to configure a single server:

1. If you want to use the deployment you just created on the server, click **Deploy**.

    If you want to use a previously created deployment, insert the USB key containing the deployment:

    a. Save the deployment from the USB key to the local server.

    b. In the **Select a Deployment** window, select the deployment from the list and click **Deploy.** If the USB key and their stored deployments are not displayed, click **Rescan**.

2. As the deployment runs, a validation screen applies settings for the following elements:

    - ROM Settings

    - Array Settings

    - System Options

    - Firmware Update

    - ERS Settings
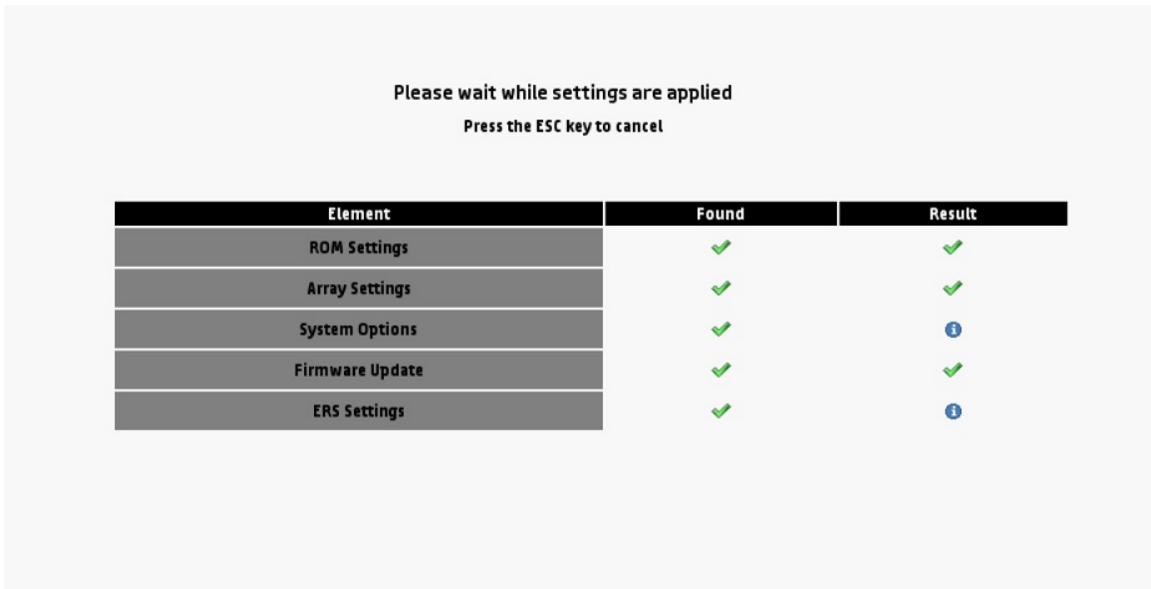
The validation screen indicates the results of the settings, using icons described in the following table.

Icon	Result
Question mark	Status unknown
Red box	Error
Gray box	Element not needed
Green check	Element successfully applied
Information icon	Click for additional information

Performing Deployment Settings package-level actions

Package-level actions manipulate the Deployment Settings package, not individual settings within a deployment.

After making a selection in the initial page, the **Select a Deployment** window opens.

In **Select a Deployment** window, existing Deployment Settings packages that are stored on the server are displayed in the left pane, existing Deployment Settings packages that are stored on

an installed USB drive are displayed in the right pane, and package-level action icons are displayed in the center of the window. If a USB drive is installed, its name is displayed near the top of the window in the **Target USB Key** field.

- To perform a package-level action on a Deployment Settings package, select one of the displayed packages, and then select an action icon in the middle pane.
- To open a specific Deployment Settings package to change individual settings, double-click one of the displayed packages.
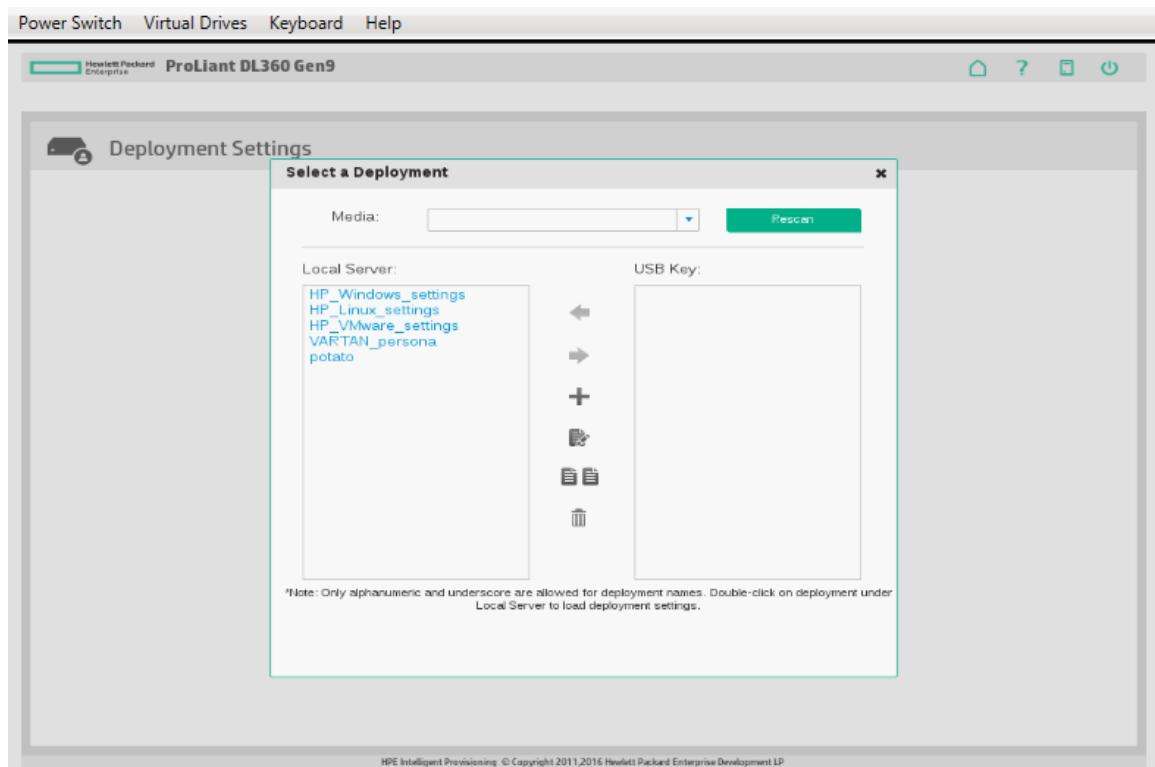
The following table defines the available actions.

Task	Description
Copy a deployment to a local server	Click the **Copy to local server** icon to copy a selected deployment from the attached USB key to a local server.
Copy a deployment to a USB key	Click the **Copy to USB key** icon to copy a selected deployment from the server to the attached USB key.
Create a new deployment	Click the **Create new deployment** icon to create a new deployment on the local server.
Rename a deployment	Click the **Rename** icon to rename the selected deployment. Use only alphanumeric characters and underscores in the deployment name. Do not include spaces in the name.
Duplicate a deployment	Click the **Duplicate** icon to duplicate the selected deployment or template.
Delete a deployment	Click the **Delete** icon to delete the selected deployment.

Entering or changing individual settings for a Deployment Settings package

After double-clicking a displayed Deployment Settings package, the **Deployment Settings** page is redisplayed, with setting categories listed on the left side of the page, and the Deployment

Settings package you are modifying near the top of the page. To switch to a different Deployment Settings package, expand the drop-down menu.

Clicking a category displays the associated data fields. The fields are optional and can be left blank or unchanged.
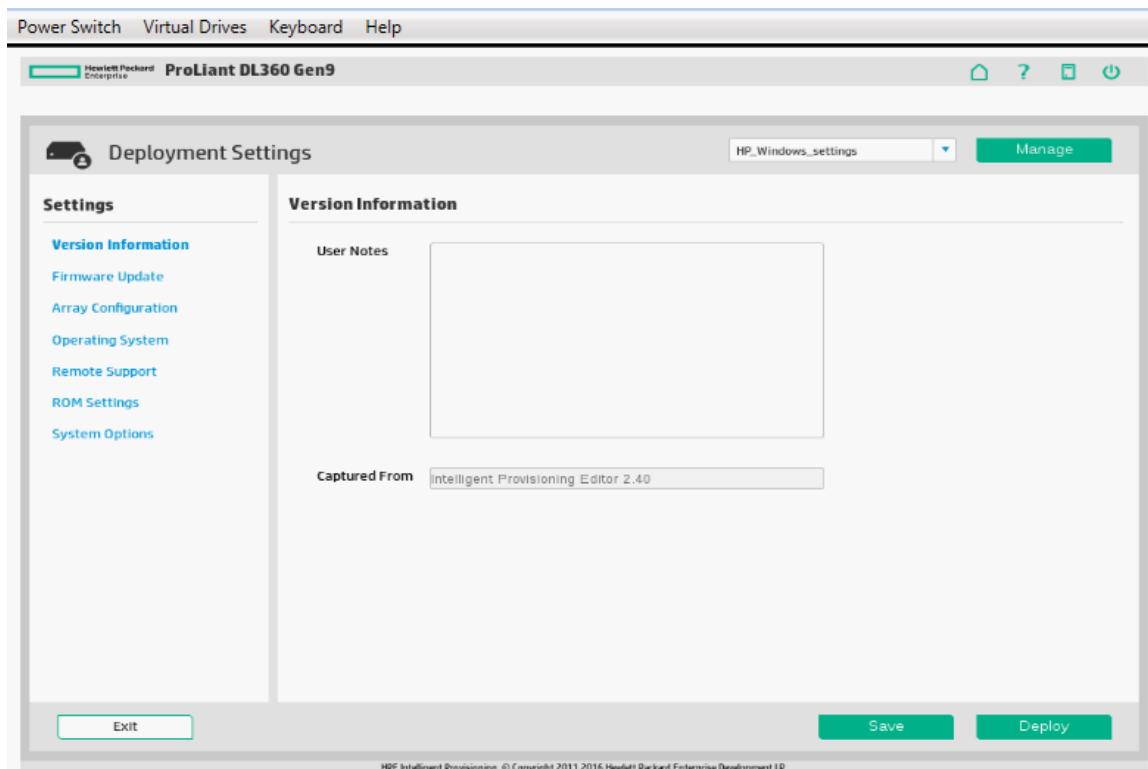
- To record new values, click **Save**.

- To execute the Deployment Settings package on the server, click **Deploy**.

- To go back to the previous page, click **Manage**.

- To exit Deployment Settings screens, click **Exit**.

The following sections define the available Deployment Settings categories.

Entering version information

Use the **Version Information** screen to enter any type of user-defined identifying information that you want to assign to the deployment.

Entering firmware update settings

Use the **Firmware Update** screen to enter information about performing firmware updates as part of the deployment installation process.

Options include:

- **No Update**—System firmware is not updated during the deployment installation process.

- **hpe.com**—During the deployment installation process, the system uses the server's Internet connections to obtain the latest firmware from the Hewlett Packard Enterprise website and install it on the server.

- **Local Repository**—The URL of the local repository where the firmware has previously been uploaded.

Entering array configuration settings

Use the **Array Configuration** screen to enter RAID settings.

1. Select a RAID Level.
2. Select a Stripe Size.
3. Select Read and Write Cache ratios. Make sure that these values total 100%.

Entering operating system information

Use the **Operating System** screens to enter OS information and installation settings. The included fields are the same as those in the Recommended installation method.

Not all source media types are supported for every OS.

1. Select an OS family.
2. Enter the OS media path, which can be a Windows Share or an FTP site on the local network. Installation of Windows from an FTP site is not supported.

   Based on this setting, the system automatically pulls the ISO from the specified location to install it.

   - For a Windows share location, enter the following network connection settings:

     ○ **Server Name or IP Address**—Server name or IP address of the server that hosts the OS contents. If a server name is specified, a DNS entry is also required.

     ○ **Share Name**—The name of the network share using Server Message Block (SMB) protocol that hosts the OS contents.

     ○ **Network Share User**—User name used to access the network share.

     ○ **Network Share Password**—Password for the user name used to access the network share.

   - For an FTP site, enter the following network connection settings:

     ○ **Server Name or IP Address**—FTP server name or IP address of the server that hosts the OS contents. FTP support requires anonymous access to the FTP server and does not support connecting to an FTP server through a proxy.

   ① **IMPORTANT:**

     ○ When entering an FTP path, do not include spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).

     ○ Installation of Windows from an FTP site is not supported.

3. Enter the user name and password for the Deployment Settings package to use to access the network share.

   This password is not encrypted. For a more secure access method, use FTP.

4. Select the OS and the keyboard language.
5. Enter the product key.

   If you do not enter a product key and one is required, the OS installation pauses indefinitely, prompting you to enter the key. The installation resumes after you enter the product key.

6. After clicking **Deploy**, verify that you are ready to create the new OS. Click **Apply** to install the OS.

   NOTE: When the command is sent to iLO, the system will reboot. Disc drives that you had previously deployed may be erased.

Entering Remote Support information

Use the **Remote Support** screen to enable or disable Insight Remote Support central connect. Insight Online direct connect is not supported with the Deployment Settings feature.

If you enable Remote Support, enter the following settings:

- **Local Remote Support Server**—The hostname or IP address of the Insight RS host server.
- **Local Remote Support Server Port**—The port number to use. The default port number for Insight RS is 7906.

For more information about the Insight Remote Support central connect requirements, see "Step 3: Registering for HPE remote support" (page 13).

Entering ROM settings

Use the **ROM Settings** screen to enter ROM-level settings.

1. If this Deployment Settings package might be used to reprovision a server already in use, consider whether to reset the server to its default settings before applying the settings in the Deployment Settings package. For stability reasons, the Standard Boot Order and the PCI Device enable/disable settings are not cleared.

   If you choose to keep the existing settings, the settings in the Deployment Settings package that differ from the existing settings are used to modify the existing settings.

2. Select the power management package to use. These packages set a basic policy for performance versus power usage without having to configure individual settings through the UEFI System Utilities menus.

   A recommended package is displayed, but to change the settings, the options include:

   - **Balanced Power and Performance**
   - **Minimum Power Usage**
   - **Maximum Performance**

   For more information about these options, see "Using Quick Configs" (page 51).

3. Select the boot order.
4. Choose whether to enable SATA devices when they are available.
5. Choose whether to install a Virtual Install Disk (VID) that contains drivers from Hewlett Packard Enterprise.

   When VID is enabled, during the OS installation process, a USB mass-storage device appears with the name of VID. This drive contains a limited set of storage and networking drivers, so any required SAS/iSCSI/FCoE adapter can be loaded, in the event that the OS disc does not have the appropriate drivers. For more information about how to load additional drivers, see the OS installation guide.

   To disable VID at a later time,
   a. Reboot the server and press **F9** during POST to access the UEFI System Utilities.
   b. Select **System Configuration→BIOS/Platform Configuration (RBSU)→Advanced Options→Advanced System ROM Options→Virtual Install Disk**.

Entering system options

Use the **System Options** screen to enter basic system settings.

1. Select the user interface and keyboard language.
2. Accept the Intelligent Provisioning EULA.

3. Choose whether to enable or disable Intelligent Provisioning on the server being configured with the Deployment Settings package.

If Intelligent Provisioning is disabled, it cannot be accessed on the server. During POST, **F10** is in red text on the screen, indicating that the **F10** key is disabled and Intelligent Provisioning is no longer accessible. For information on re-enabling Intelligent Provisioning, see "Step 2: Activate Intelligent Provisioning" (page 12).

Using HPE Smart Storage Administrator (HPE SSA)

These utilities provide high-availability configuration, management, and diagnostic capabilities for all Smart Array products.

HPE SSA features

HPE SSA is a browser-based utility that runs in either offline or online mode. HPE SSA:

- Supports online array capacity expansion, logical drive extension, assignment of online spares, and RAID or stripe size migration
- Suggests the optimum configuration for an unconfigured system
- Provides different operating modes, enabling faster configuration or greater control over the configuration options
- Displays on-screen tips for individual steps of a configuration procedure

In HPE SSA, you can select a controller from the menu at the top left-hand side of the screen, or you can choose to configure or diagnose an available controller from the same menu.
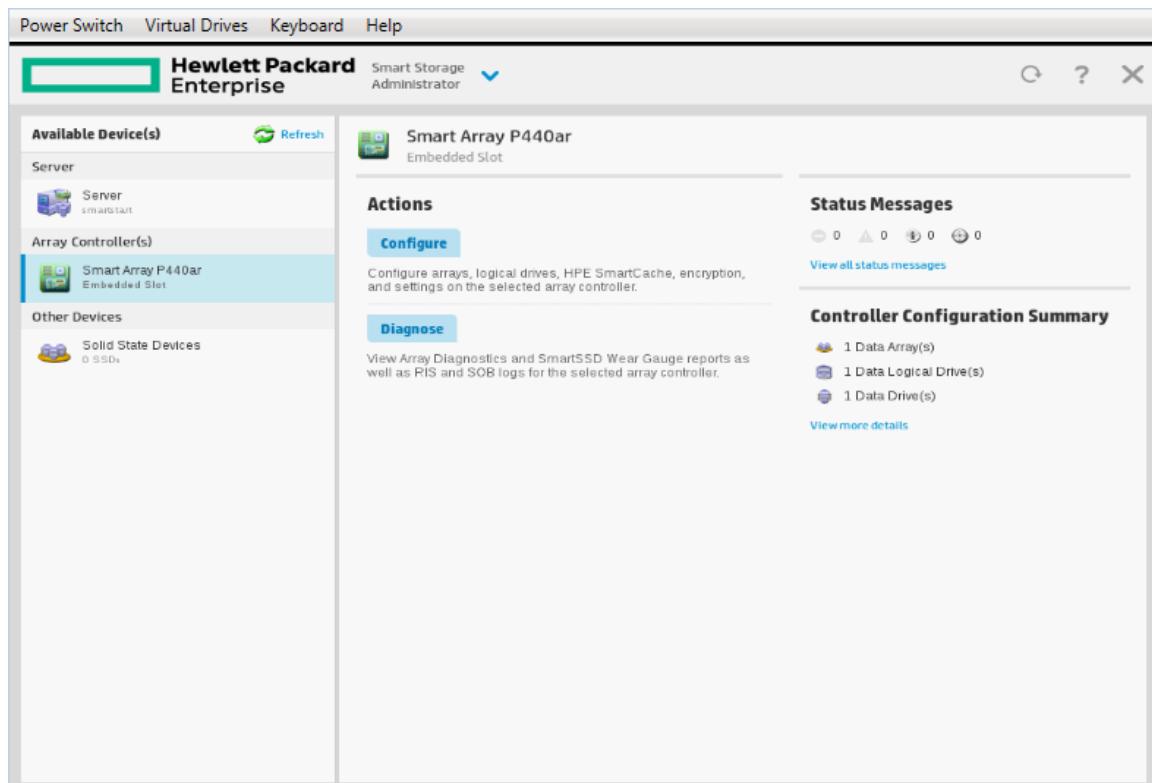
Accessing HPE SSA

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **HPE Smart Storage Administrator (HPE SSA)** from the maintenance options.

The Smart Storage Administrator window is displayed.

Configuration

Under **Actions** click **Configure** to access the configuration tasks which include the following:

- **Controller settings**—Configures the supported controller settings. Depending on the controller, these can include setting the array accelerator cache ratio, transform and rebuild priorities, and surface scan delay.

- **Caching settings**—Configures the supported caching settings which can help increase performance by taking advantage of cache memory. Caching also helps protect data integrity when used with a battery or capacitor.

- **Clear configuration**—Resets the controller's configuration to its default state. Existing arrays or logical drives are deleted, and data on the logical drives is lost. Confirm this is the preferred action before proceeding.

- **Physical drive write cache settings**—Enables or disables the write cache on physical drives attached to a controller. This feature can improve performance but precautions must be taken to ensure data integrity.

- **Modify spare activation mode**—Switches the spare activation mode from the default behavior (activate on failure only) to predictive spare activation and back.

- **Set Bootable Logical Drive/Volume**—Sets the primary and secondary boot logical drives and volumes. Local logical drives as well as remote logical drives and volumes are listed for selection.

- **Manage License Keys**—Enables the user to add or remove license keys. Depending on the keys entered or removed, various features can be enabled or disabled.

- **More information** — Provides an in-depth display of available information for the currently selected device and all of its child devices, when applicable.

Diagnostics/SmartSSD

Under **Actions** click **Diagnose** to access the diagnostic reporting tools.
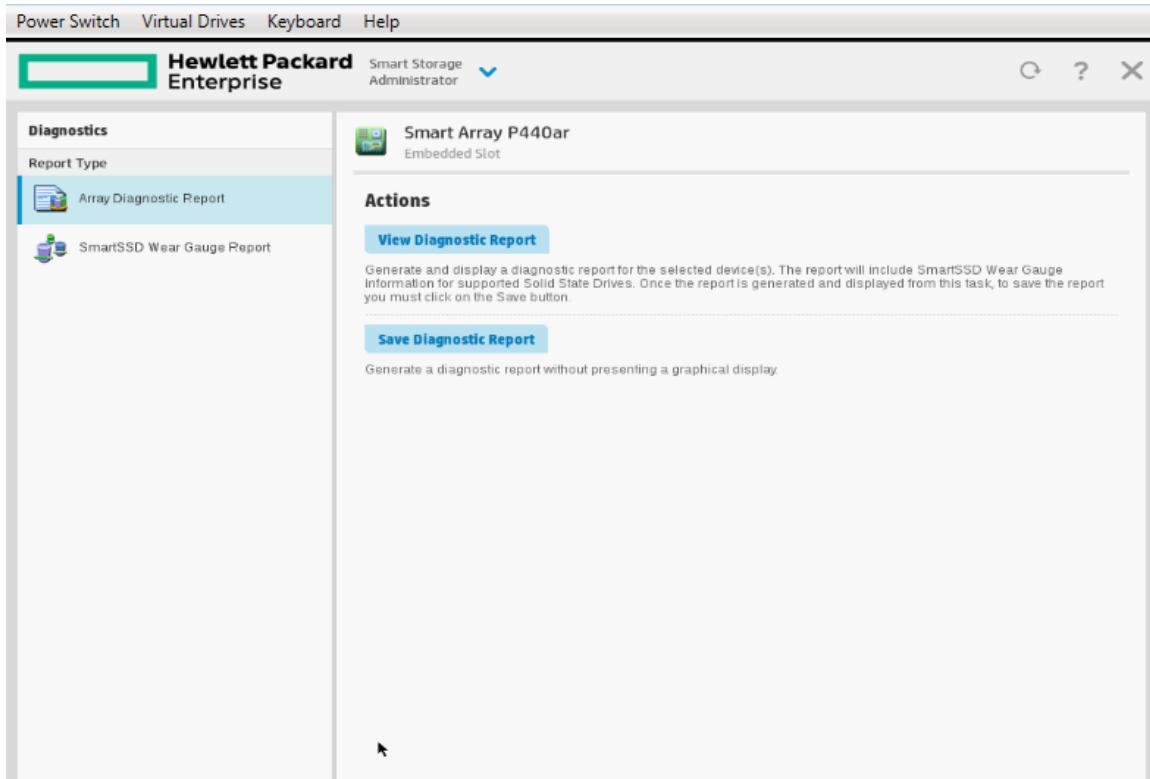
- **Array Diagnostics Report**—Run reports on selected controllers to display available diagnostic tasks. Reports include SmartSSD Wear Gauge information for supported solid state drives.

  ○ **View Diagnostic Report**—Generate and display a diagnostic report for the selected devices. The report includes SmartSSD Wear Gauge information for supported Solid State Drives, and usage and estimated lifetime information.

  ○ **Save Diagnostic Report** —Generate a diagnostic report for the selected devices for export without presenting a graphical display.

- **SmartSSD Wear Gauge Report**—View or generate a report:

  ○ **View SmartSSD Wear Gauge Report**—Display SSD usage and estimated lifetime information.

  ○ **Save SmartSSD Wear Gauge Report**—Generate a report for export, without presenting a graphical display.

Using HPE Insight Diagnostics

HPE Insight Diagnostics

Insight Diagnostics provides a comprehensive suite of offline system and component tests, providing in-depth testing of critical hardware components for devices such as processors, memory, and hard drives. Insight Diagnostics captures system configuration information and provides detailed diagnostic testing capabilities.

Insight Diagnostics simplifies the process of effectively identifying, diagnosing, and isolating hardware issues. System availability is maintained through the following key features:

- Surveying the current configuration, with various levels and categories
- Testing and diagnosing apparent hardware failures

- Documenting system configurations for upgrade planning, standardization, inventory tracking, disaster recovery, and maintenance

- Sending configuration information to another location for more in-depth analysis

- Managing the Integrated Management Log (IML)

In addition to system management tools, service tools can resolve system problems quickly. To streamline the service process and resolve problems quickly, you must have the right information available at the time that a service call is placed. This combination of features simplifies the service process and minimizes downtime.

Accessing Insight Diagnostics

NOTE: If you accidentally double-click the Insight Diagnostics icon, a message is displayed, notifying you that you attempted to have two sessions of Insight Diagnostics open at the same time. To correct the situation, follow the instructions provided in the message.

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Insight Diagnostics** from the maintenance options.

   The Insight Diagnostics window is displayed.
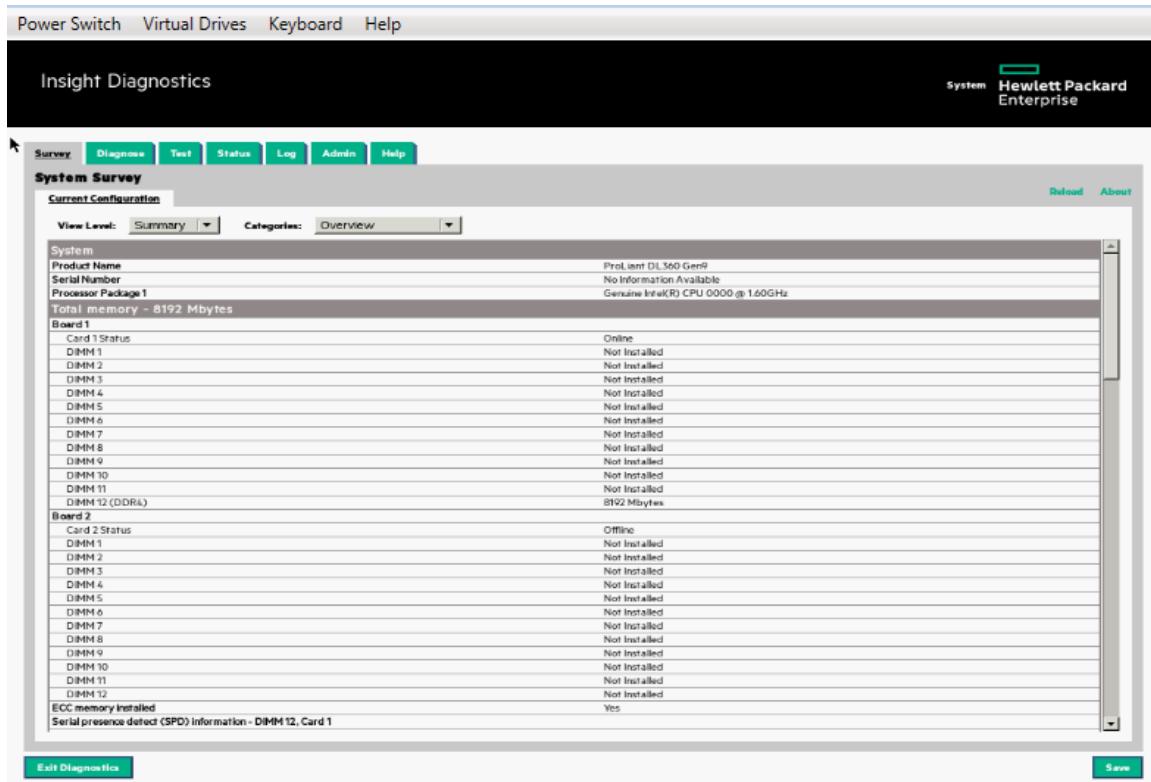
During offline testing, the user-installed OS is not running. Therefore, software information from the system is not reported. Insight Diagnostics (Offline Edition) runs when the computer is started with one of the following products:

- Intelligent Provisioning on ProLiant Gen9 servers

- SPP

Clicking **Exit Diagnostics** exits the Insight Diagnostics application and returns to Intelligent Provisioning. Insight Diagnostics is also available online as a web-based application. For more information, see the Insight Diagnostics user guide on the website (**http://www.hpe.com/info/intelligentprovisioning/docs**).

Using Quick Configs

Use this feature to set a power management policy through Intelligent Provisioning without having to configure individual settings through the UEFI System Utilities.

To use Quick Configs:

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Quick Configs** from the maintenance options.

    The Quick Configs window is displayed.
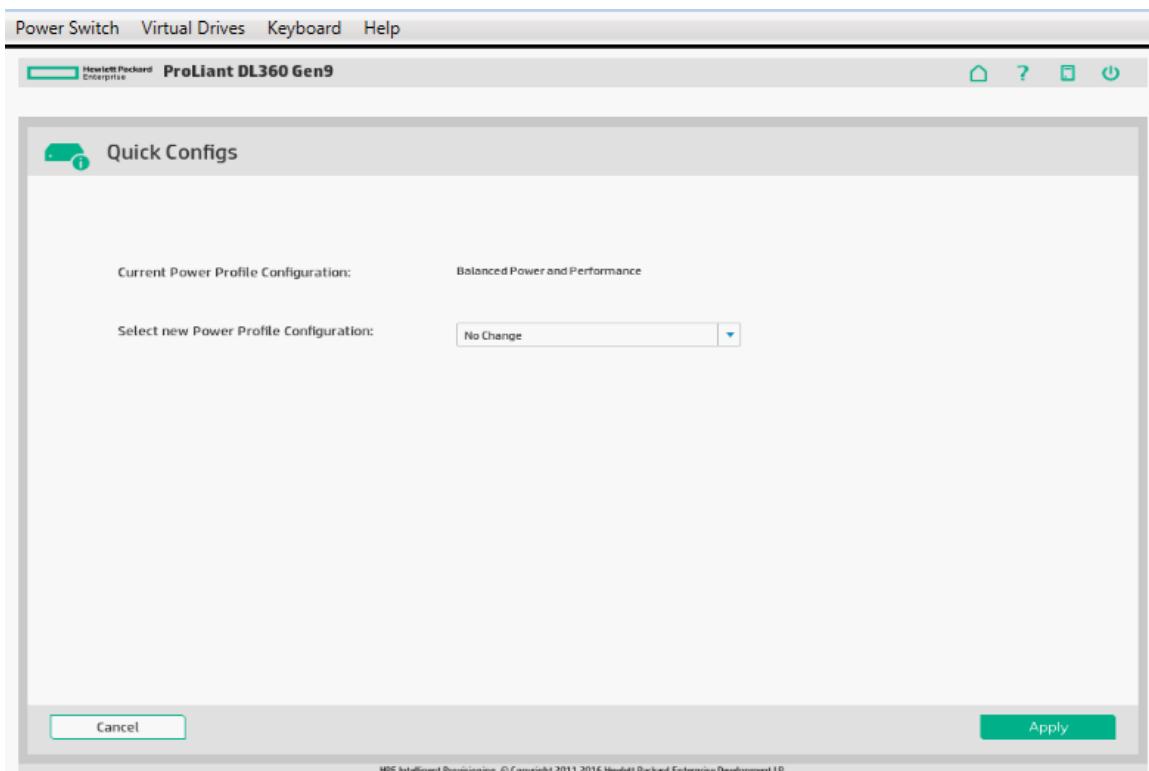
When initially configuring and provisioning a server through Intelligent Provisioning, this Quick Configs screen is presented in the "Step 1: Selecting hardware settings" (page 24) screen.

If the server does not have HPE DIMMs installed, the following Power Profiles might not all be available:

- **Balanced Power and Performance**—Optimum settings to maximize power savings with minimal impact to performance for most OSs and applications.

- **Minimum Power Usage**—Enables power reduction mechanisms that might negatively affect performance. This mode guarantees a lower maximum power usage by the system.

- **Maximum Performance**—Disables all power management options that might negatively affect performance.

After selecting and applying a profile, a confirmation message appears.

To customize the individual settings, press the **F9** key during server reboot to go to the UEFI System Utilities.

Intelligent Provisioning Quick Configs settings and corresponding UEFI System Utilities settings

The Quick Configs options provide the capability to select a basic policy for performance versus power usage, without having to configure individual settings through the UEFI System Utilities menus.

The following table shows the three Intelligent Provisioning Quick Configs profiles and their corresponding UEFI System Utilities settings.

NOTE: Not all of the options in this table are adjustable on all servers. However, even if you do not have the option of adjusting some of these settings, they will default to the values shown here.

Power management options	Quick Configs settings (Intel-based servers)		
	Balanced power and performance	Minimum power usage	Maximum performance
HPE Power Profile	Balanced Power and Performance	Minimum Power Usage	Maximum Performance
HPE Power Regulator	HPE Dynamic Power Savings Mode	HPE Static Low Power Mode	HPE Static High Performance Mode
Intel QPI Link Power Management	Enabled	Enabled	Disabled
Minimum Processor Idle Power Core State	C6 State	C6 State	No C-states
Minimum Processor Idle Power Package State	Package C6 (retention) State	Package C6 (retention) State	No Package State
Energy/Performance Bias	Balanced Performance	Power Savings Mode	Maximum Performance
Maximum Memory Bus Frequency	Auto	1333 MHz	Auto
Channel Interleaving	Enabled	Disabled	Enabled
Maximum PCI Express Speed	Maximum Supported	PCIe Generation 1	Maximum Supported
Intel QPI Frequency	Auto	Minimum QPI Speed	Auto

Using iLO Configuration Utility

Use the iLO Configuration Utility to view and change iLO settings through Intelligent Provisioning, instead of through the iLO web interface. For more information about iLO, see the iLO 4 user guide.

You must configure iLO network settings to register the server with the remote support registration process.

When changing iLO settings, if the display is not as expected or an undefined error message is displayed, press **F5** to refresh the screen display. It is possible that the change was being made at the same time through the iLO web interface.

To use iLO Configuration Utility:

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **iLO Configuration** from the maintenance options.

   The iLO Configuration Utility window is displayed.

Viewing iLO summary information

To view iLO summary information:

1. In the **Maintenance** window, click **iLO**.

   The iLO Configuration Utility window appears.
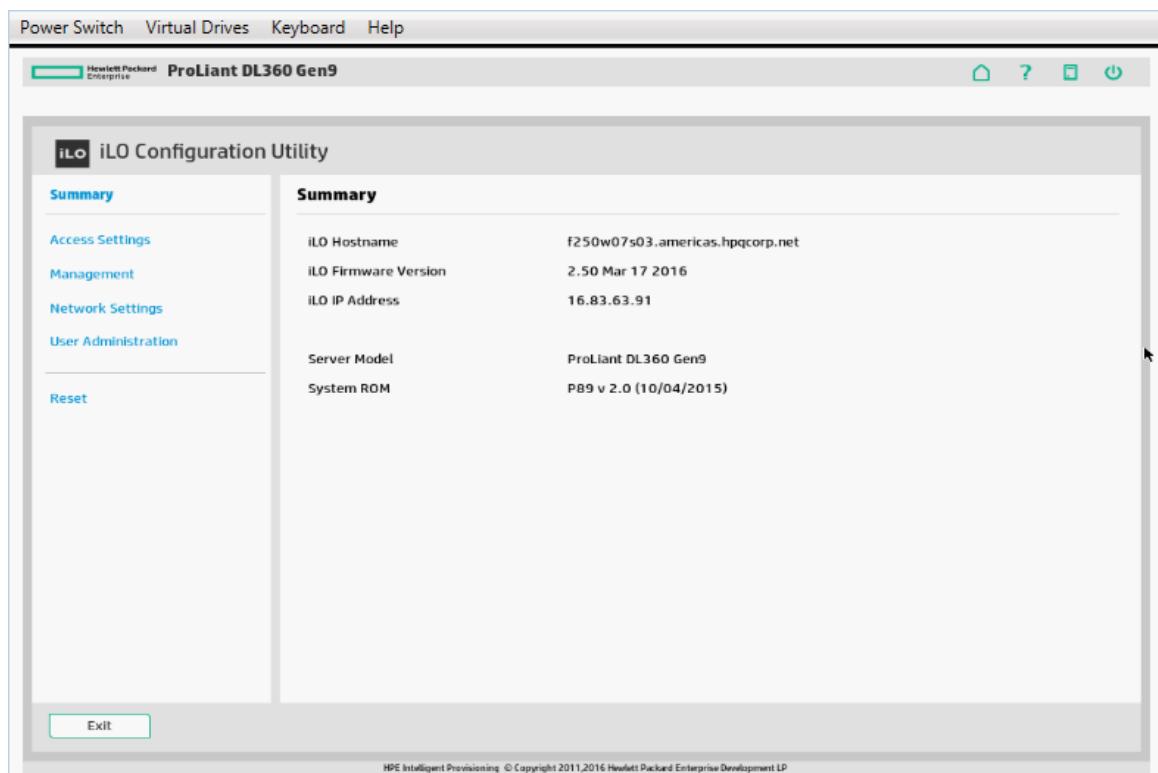
2. Click **Summary**. The following information is displayed:

- **iLO Hostname**—The DNS name of the iLO subsystem, for example, `ilo` instead of `ilo.example.com`. This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

- **iLO Firmware Version**—The version and date of the installed iLO firmware.

- **iLO IP Address**—The network IP address of the iLO subsystem

- **Server Model**—The type of system in which this iLO processor is integrated

- **System ROM**—The family and version of the active system ROM

You can also view this information on the Overview screen in the iLO web interface. For more information, see the iLO 4 user guide on the website (**http://www.hpe.com/info/ilo/docs**).

NOTE: The rest of the procedures in this section are written with the assumption that you have selected **iLO** from the Maintenance window.

Editing iLO Access Settings

Various iLO access settings can be edited from the three tabs on the Access Settings window: Access Options, Service and IPMI/DCMI.

To edit access settings on the Access Options tab:

1. In the **iLO Configuration Utility** window, click **Access Settings**.

   The **Access Options** tab data appears:
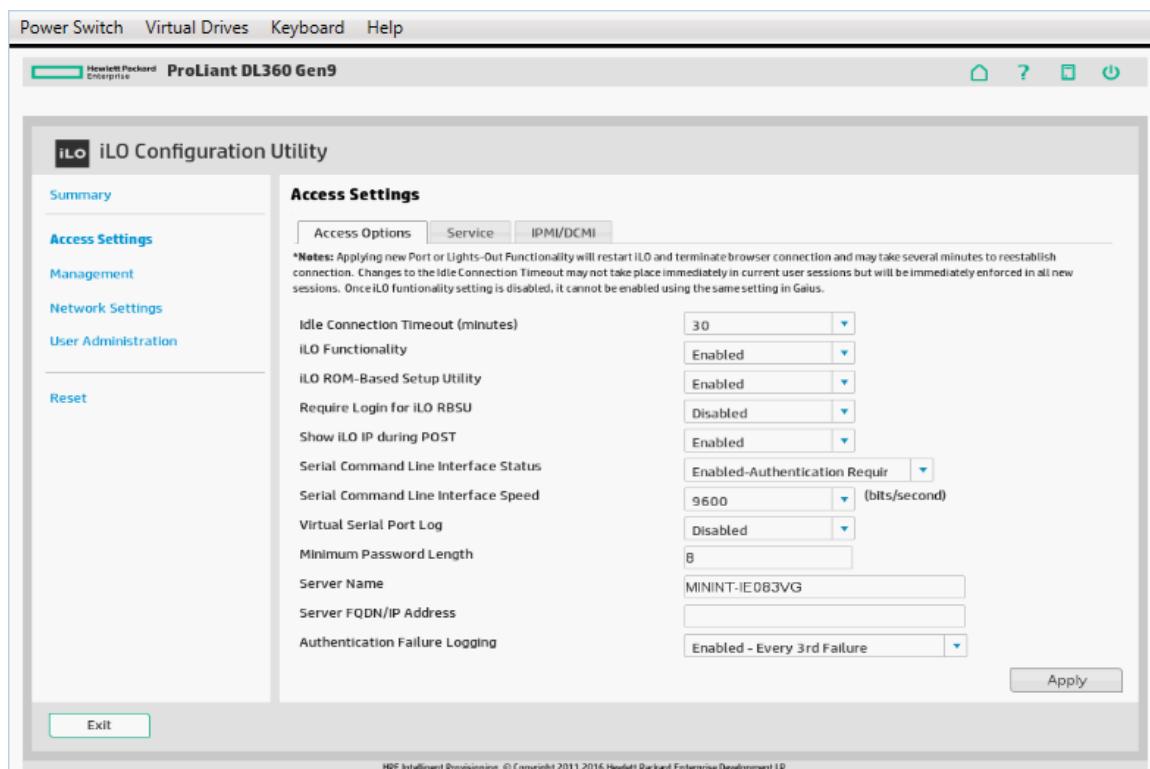
2. Edit the option(s) as necessary. Click **Apply**.

Access Settings–Access Options

- **Idle Connection Timeout (minutes)**—Specifies how long a user can be inactive before the iLO web interface or Remote Console session ends automatically. The iLO web interface and the Remote Console track idle time separately because each connection is a separate session. Remote Console sessions are not affected by this value if a virtual media device is connected.

  The following settings are valid:

  - **15**, **30**, **60**, or **120** minutes—The default value is 30 minutes.

  - **Infinite**—Inactive users are not logged out.

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

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

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

- **iLO Functionality**—Specifies whether iLO functionality is available. The following settings are valid:

  ○ **Enabled** (default)—The iLO network is available and communications with operating system drivers are active.

  ○ **Disabled**—The iLO network and communications with operating system drivers are terminated when **iLO Functionality** is disabled.

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

  iLO functionality cannot be disabled on server blades.

- **iLO ROM-Based Setup Utility**—Enables or disables the iLO 4 Configuration Utility. The following settings are valid:

  ○ **Enabled** (default)—On servers that support UEFI, the iLO 4 Configuration Utility is available when you access the UEFI System Utilities.

  ○ **Disabled**—On servers that support UEFI, the iLO 4 Configuration Utility is not available when you access the UEFI System Utilities.

- **Require Login for iLO RBSU**—Determines whether a user-credential prompt is displayed when accessing the iLO 4 Configuration Utility. The following settings are valid:

  ○ **Enabled**—A login dialog box opens when a accessing the iLO 4 Configuration Utility.

  ○ **Disabled** (default)—No login is required when accessing the iLO 4 Configuration Utility.

- **Show iLO IP during POST**—This setting enables the display of the iLO network IP address during host server POST.

- **Serial Command Line Interface Status**—Enables you to change the login model of the CLI feature through the serial port. The following settings are valid:

  ○ **Enabled-Authentication Required** (default)—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. Valid iLO user credentials are required.

  ○ **Enabled-No Authentication**—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. iLO user credentials are not required.

  ○ **Disabled**—Disables access to the SMASH CLP command line from the host serial port. Use this option if you are planning to use physical serial devices.

- **Serial Command Line Interface Speed**—Enables you to change the speed of the serial port for the CLI feature. The following speeds (in bits per second) are valid:

  ○ **9600** (default)

  ○ **19200**

  ○ **38400**—This value is not supported by the iLO 4 Configuration Utility.

  ○ **57600**

  ○ **115200**

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

The serial port speed set by this option should match the serial port speed configured in the iLO 4 Configuration Utility.

- **Virtual Serial Port Log**—Enables or disables logging of the Virtual Serial Port.

  The following settings are valid:

  ○ **Enabled**—When enabled, Virtual Serial Port activity is logged to a 150-page circular buffer in the iLO memory, and can be viewed using the CLI command `vsp log`. The Virtual Serial Port buffer size is 128 KB.

  ○ **Disabled** (default)—Virtual Serial Port activity is not logged.

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

- **Minimum Password Length**—Specifies the minimum number of characters allowed when a user password is set or changed. The character length must be a value from 0 to 39 characters long. The default value is 8.

- **Server Name**—Enables you to specify the host server name. You can assign this value manually, but it might be overwritten by the host software when the operating system loads.

  ○ You can enter a server name that is up to 49 bytes.

  ○ To force the browser to refresh and display the new value, save this setting, and then press **F5**.

- **Server FQDN/IP Address**—Enables you to specify the server FQDN or IP address. You can assign this value manually, but it might be overwritten by the host software when the operating system loads.

  ○ You can enter an FQDN or IP address that is up to 255 bytes.

  ○ To force the browser to refresh and display the new value, save this setting, and then press **F5**.

- **Authentication Failure Logging**—Enables you to configure logging criteria for failed authentications. All login types are supported; each login type works independently. The following are valid settings:

  ○ **Enabled-Every Failure**—A failed login log entry is recorded after every failed login attempt.

  ○ **Enabled-Every 2nd Failure**—A failed login log entry is recorded after every second failed login attempt.

  ○ **Enabled-Every 3rd Failure** (default)—A failed login log entry is recorded after every third failed login attempt.

  ○ **Enabled-Every 5th Failure**—A failed login log entry is recorded after every fifth failed login attempt.

  ○ **Disabled**—No failed login log entry is recorded.

Access Settings–Service

- **Secure Shell (SSH) Access**—Allows you to enable or disable the SSH feature. SSH provides encrypted access to the iLO CLP. The default value is **Enabled**.

- **Secure Shell (SSH) Port**—The default value is 22.

- **Remote Console Port**—The default value is 17990.

- **Web Server Non-SSL Port** (HTTP)—The default value is 80.

- **Web Server SSL Port** (HTTPS)—The default value is 443.

- **Virtual Media Port**—The default value is 17988.

- **SNMP Access**—Specifies whether iLO should respond to external SNMP requests. The default value is **Enabled**.

  If you set **SNMP Access** to **Disabled**, iLO continues to operate, and the information displayed in the iLO web interface is updated, but no alerts are generated and SNMP access is not permitted. When **SNMP Access** is set to **Disabled**, most of the boxes on the **Administration→Management→SNMP Settings** page are unavailable and will not accept input.

- **SNMP Port**—The industry-standard (default) SNMP port is **161** for SNMP access.

  If you customize the **SNMP Port** value, some SNMP clients might not work correctly with iLO unless those clients support the use of a nonstandard SNMP port.

- **SNMP Trap Port**—The industry-standard (default) SNMP trap port is **162** for SNMP alerts (or traps).

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

To edit access settings on the Service tab:

1. In the **iLO Configuration Utility** window, click **Access Settings**.

   The **Access Options** tab data appears:
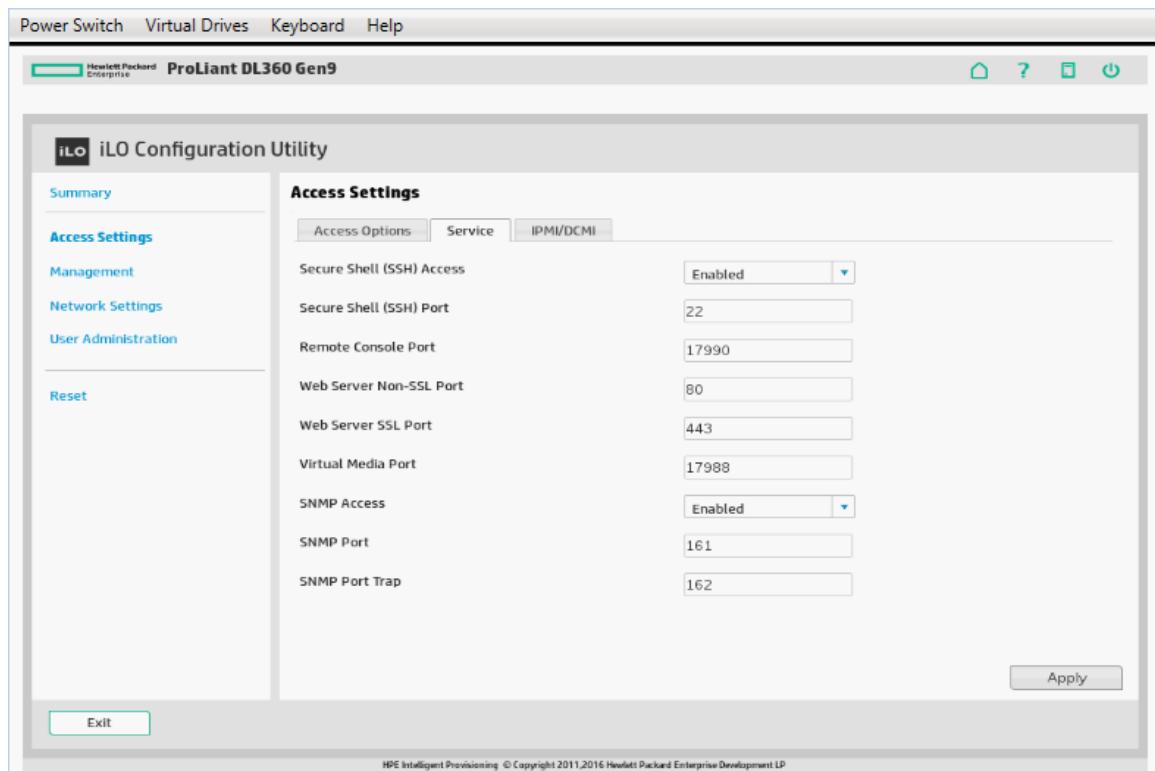
2. Click the **Service** tab. The Service tab data appears.
3. Edit the option(s) as necessary. Click **Apply**.

Access Settings–IPMI/DCMI

iLO enables you to send industry-standard IPMI and DCMI commands over the LAN. The IPMI/DCMI port is set to 623 and is not configurable.

To edit access settings on the IPMI/DCMI tab:

1. In the **iLO Configuration Utility** window, click **Access Settings**. The Access Options tab data is displayed.
2. Click the **IPMI/DCMI** tab.

   The IPMI/DCMI tab data appears:
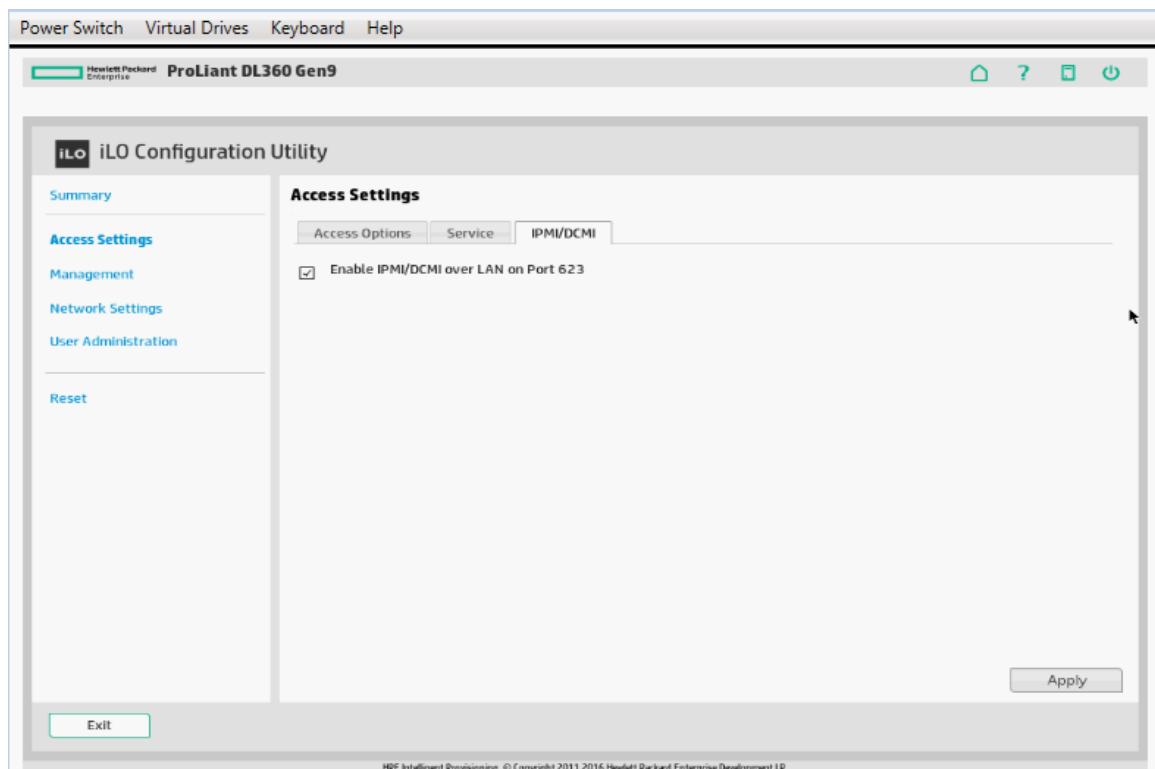
3. Select the check box to enable IPMI/DCMI, or clear the box to disable it. Click **Apply**.

Editing iLO Management Settings

Management–SNMP Settings

NOTE: Read Community supports the following formats: A community string (for example, public). A community string followed by an IP address or fully qualified domain name (for example, public 192.168.0.1). Use this option to specify that SNMP access will be allowed from the specified IP address or fully qualified domain name. For iLO 4 1.10 or later, you can enter an IPv4 address or a fully qualified domain name.

- **System Location** (Agentless Management only)—A string of up to 49 characters that specifies the physical location of the server.

- **System Contact** (Agentless Management only)—A string of up to 49 characters that specifies the system administrator or server owner. The string can include a name, email address, or phone number.

- **System Role** (Agentless Management only)—A string of up to 64 characters that describes the server role or function.

- **System Role Detail** (Agentless Management only)—A string of up to 512 characters that describes specific tasks that the server might perform.

- **Read Community** (Agentless Management only)—The configured SNMP read-only community string.

- **Trap Community**—The configured SNMP trap community string.

- **SNMP Alert Destination(s)**—The IP addresses or fully qualified domain names of up to three remote management systems that will receive SNMP alerts from iLO.

- **SNMP Port**—The port used for SNMP communications. This value is read-only, but can be modified on the Access Settings→ Service page. Navigate to the Access Settings→ Service

page in the iLO Management utility to edit the SNMP port. For more information, see "Editing iLO Access Settings" (page 53).

Various iLO management settings can be edited from the three tabs on the Management window: SNMP Settings, SNMP Alerts and Insight Management Integration.

To edit management settings on the SNMP Settings tab:

1. In the **iLO Configuration Utility** window, click **Management**.

   The SNMP Settings tab data appears:
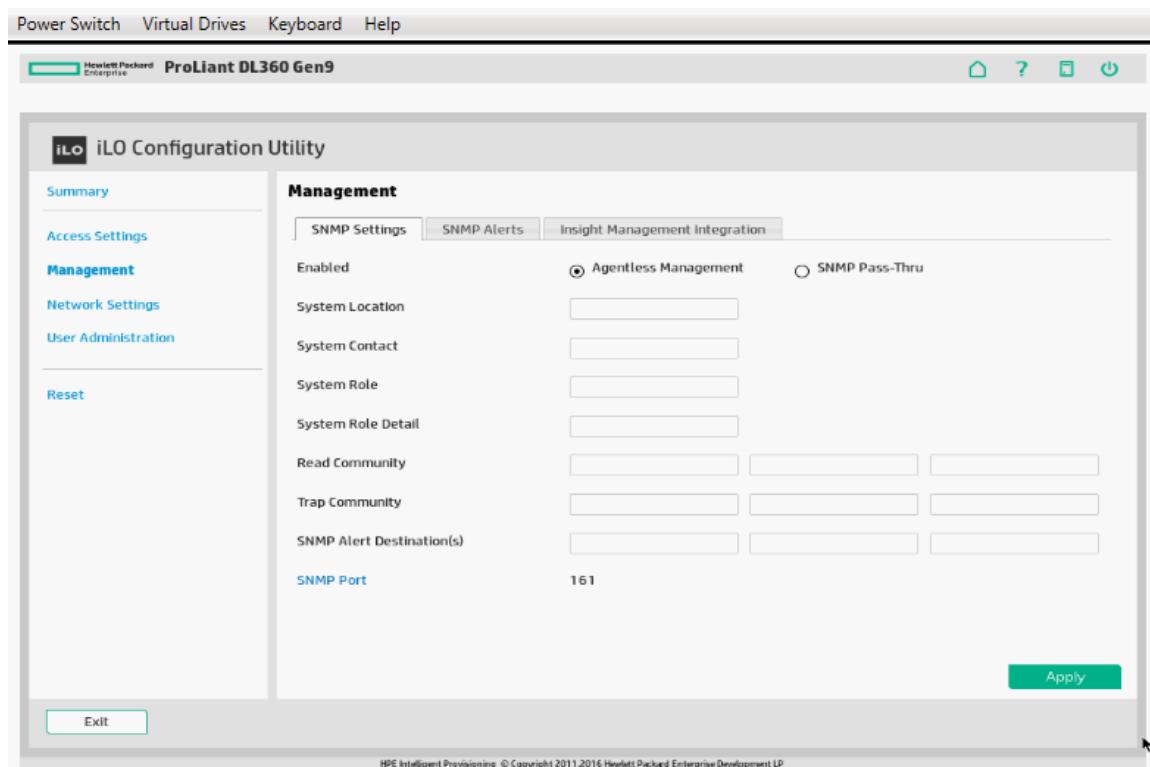
2. Click **Agentless Management** or **SNMP Pass-Thru**.
3. Enter data in the fields as necessary. Click **Apply**.

Management — SNMP Alerts

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

- **iLO SNMP Alerts**—Alert conditions that iLO detects independently of the host OS can be sent to specified SNMP alert destinations, such as SIM.

- **Forward Insight Management Agent SNMP Alerts**—Alert conditions detected by the host management agents can be forwarded to SNMP alert destinations through iLO. These alerts are generated by the Insight Management Agents, which are available for each supported OS. Insight Management Agents must be installed on the host server to receive these alerts.

- **Cold Start Trap Broadcast**—Cold Start Trap is broadcast to a subnet broadcast address if there are no trap destinations configured in the SNMP Alert Destination(s) boxes. The subnet broadcast address for an IPv4 host is obtained by performing a bitwise logical OR operation between the bit complement of the subnet mask and the host IP address. For

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

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

To edit the settings on the SNMP Alerts tab:

1. In the **iLO Configuration Utility** window, click **Management**. The SNMP Settings tab data appears.
2. Click the **SNMP Alerts** tab.

   The SNMP Alerts data appears.
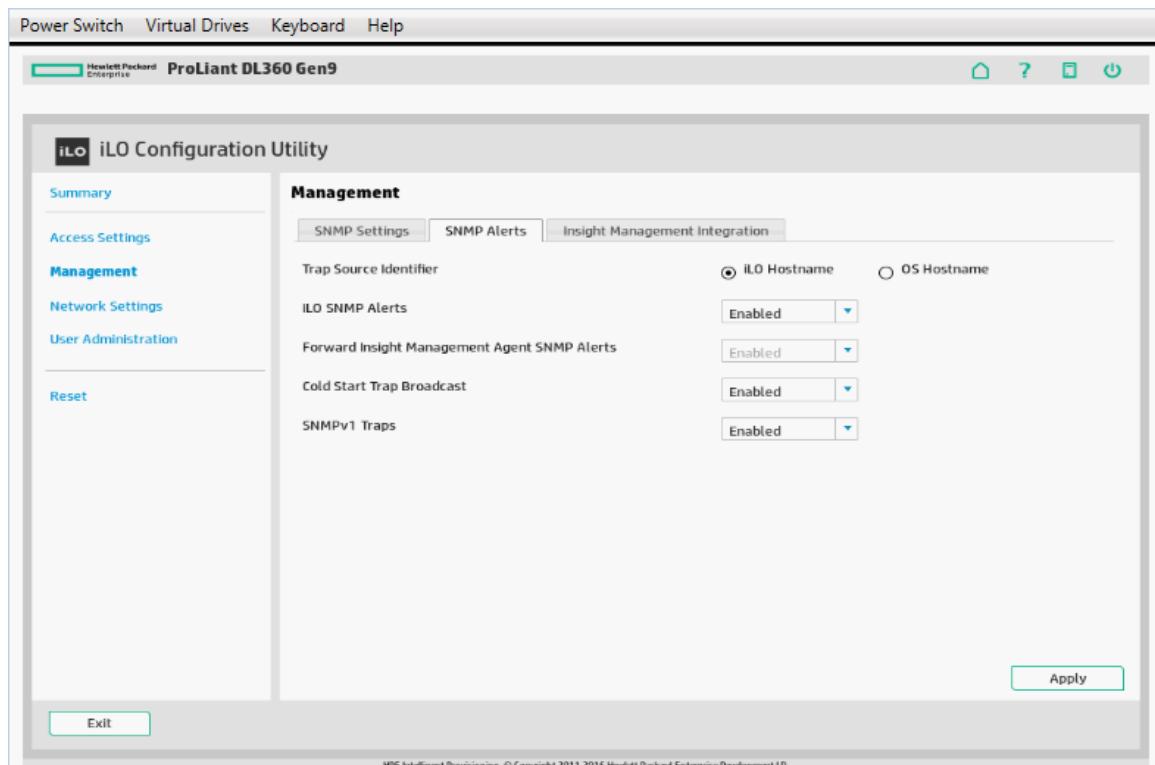
3. Click the radio button to select the **Trap Source Identifier**.
4. Click the drop-down list by each setting to select to enable or disable the setting.
5. If you choose to send an alert, click **Send Test Alert**.
6. Click **Apply**.

Management — Insight Management Integration

- **Hewlett Packard Enterprise System Management Homepage (HPE SMH) FQDN/IP Address**—This value sets the browser destination of the Insight Agent link on iLO pages. Enter the fully qualified domain name or IP address of the host server. The protocol (https://) and port number (:2381) are added automatically to the IP address or DNS

name to enable access from iLO. If the URL is set through another method (for example, CPQLOCFG), click the browser refresh button to display the updated URL.

- **Level of Data Returned**—This setting controls the content of an anonymous discovery message received by iLO. The information returned is used for SIM HTTP identification requests. The following options are available:

  ○ **Enabled (iLO+Server Association Data)** (default)—Enables SIM to associate the management processor with the host server, and provides sufficient data to enable integration with SIM.

  ○ **Disabled (No Response to Request)**—Prevents iLO from responding to SIM requests.

To edit the settings on the Insight Management Integration tab:

1. In the **iLO Configuration Utility** window, click **Management**. The SNMP Settings tab data appears.
2. Click the **Insight Management Integration** tab.

   The Insight Management Integration tab data appears.
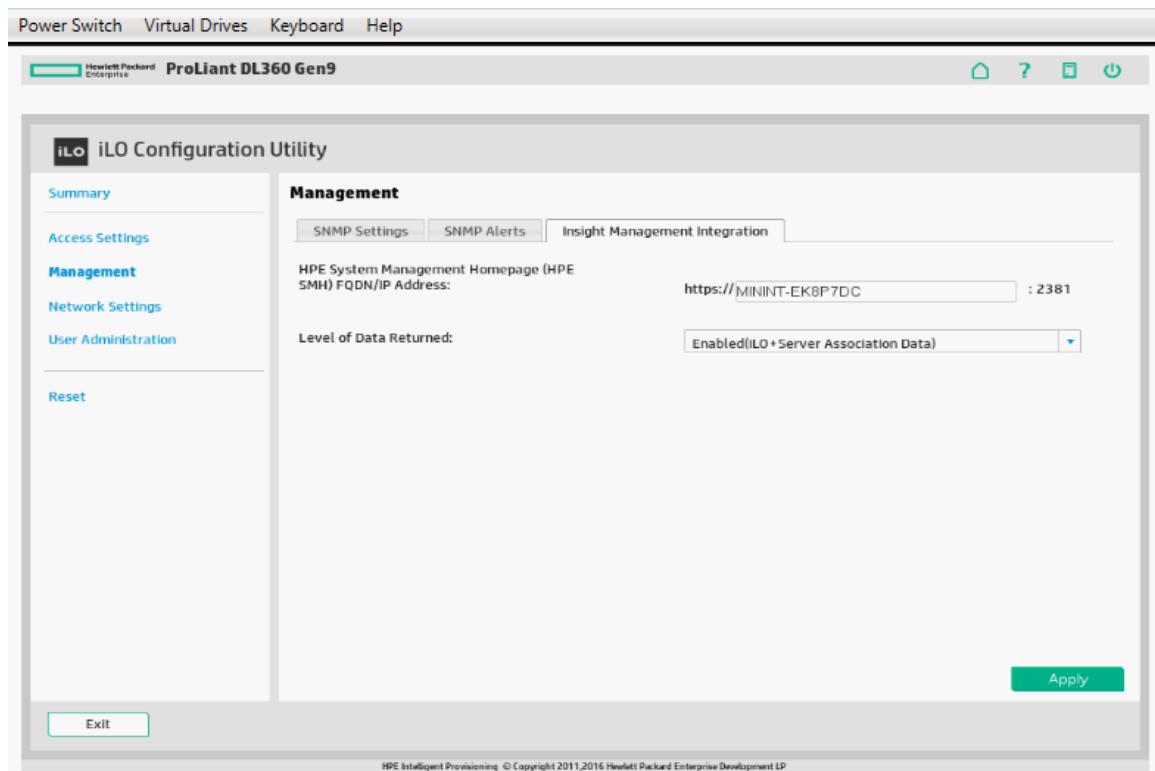
3. Edit the setting(s) that you want. Click **Apply**.

Modifying Network Settings

Network Settings — Summary

- **NIC in use**—The current NIC configuration you are using (for example, iLO Dedicated Network Port, or Shared Network Port.

- **iLO Host Name**—The DNS name of the iLO subsystem (for example, iLO instead of ilo.example.com). This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address. For more information, see the iLO 4 user guide.

- **MAC Address**—The NIC MAC address.

- **Link State**—The current link state (iLO Dedicated Network Port only).

- **Duplex Option**—The current duplex option (Full Duplex or Half Duplex).

- **DHCPv4 Status**—Enabled or Disabled.

- **IPv6 Stateless Address Auto-Configuration (SLAAC)**—Enabled or Disabled.

- **SLAAC Address**—Physical address of IPv6 created by iLO.
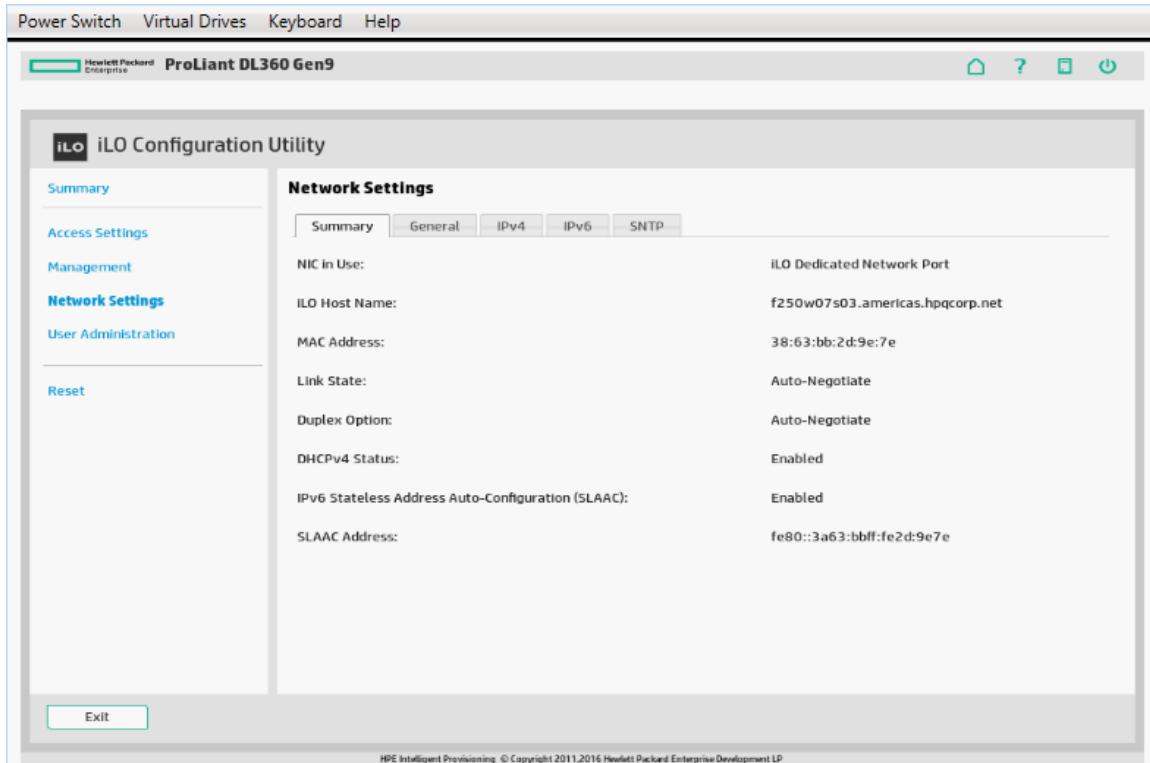
Network Settings–General

- iLO Hostname Settings

  ○ **iLO Hostname**—The DNS name of the iLO subsystem (for example, ilo instead of ilo.example.com). This name can be used only if DHCP and DNS are configured to

connect to the iLO subsystem name instead of the IP address. For more information, see the iLO 4 user guide.

- ○ **Domain Name**—The iLO domain name. If DHCP is not used, enter a domain name.
- NIC Settings
  - ○ **Use iLO Dedicated Network Port**—If the check box is selected, you are indicating that your system uses a NIC with a connector on the back of the server. The NIC handles iLO traffic only.

    If you leave the check box blank, you are indicating that your system is using a shared network port. There are two types of shared network ports:
    - – LOM—Uses a NIC that is built into the server. The NIC handles server network traffic and can, if iLO is configured to do so, handle iLO traffic at the same time.
    - – FlexibleLOM—Uses an optional NIC that connects to a special connector on the server. The NIC handles server network traffic and can, if iLO is configured to do so, handle iLO traffic at the same time. Not all servers support a FlexibleLOM. For the list of servers that support the Shared Network Port–FlexibleLOM option, see the iLO 4 user guide.

- Link State (iLO Dedicated Network Port only).
  - ○ **Automatic** (Default)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network.
  - ○ **1000Base T, Full-duplex**—Forces a 1 Gb connection that uses full duplex (not supported for BL c-Class servers).
  - ○ **1000Base T, Half-duplex**—Forces a 1 Gb connection that uses half duplex (not supported for BL c-Class servers).
  - ○ **100BaseT, Full-duplex**—Forces a 100 Mb connection using full duplex.
  - ○ **100BaseT, Half-duplex**—Forces a 100 Mb connection using half duplex.
  - ○ **10Base T, Full-duplex**—Forces a 10 Mb connection using full duplex
  - ○ **10Base T, Half-duplex**—Forces a 10 Mb connection using half duplex.

To edit the settings on the General tab:

1. In the **iLO Configuration Utility** window, click **Network Settings**. The General tab data appears.
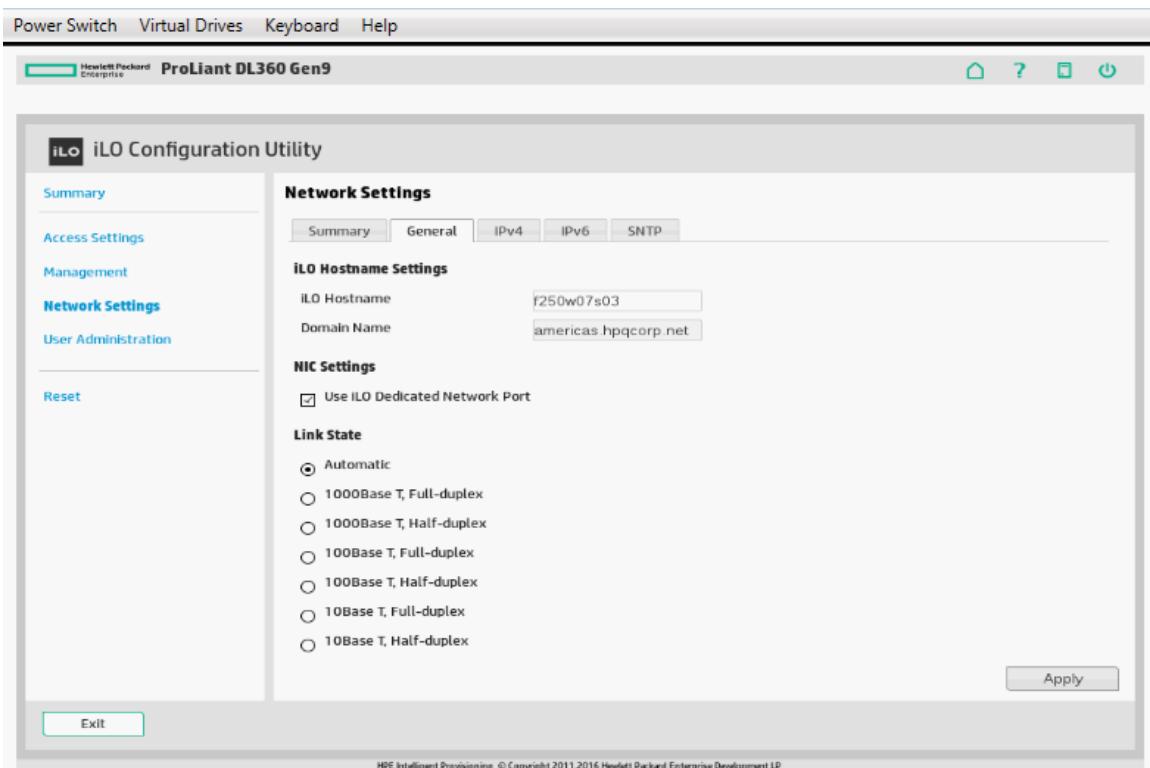
2. Edit the setting(s) as required. Click **Apply**.

Network Settings–IPv4

*   **Enable DHCPv4**—Enables iLO to obtain its IP address (and many other settings) from a DHCP server.

    *   **Use DHCPv4 Supplied Gateway**—Specifies whether iLO uses the DHCP server-supplied gateway. If DHCP is not used, enter a gateway address in the Gateway IPv4 Address box.

    *   **Use DHCPv4 Supplied Static Routes**—Specifies whether iLO uses the DHCP server-supplied static routes. If not, enter the static route destination, mask, and gateway addresses in the Static Route #1, Static Route #2, and Static Route #3 boxes.

    *   **Use DHCPv4 Supplied Domain Name**—Specifies whether iLO uses the DHCP server-supplied domain name. If DHCP is not used, enter a domain name in the Domain Name box on the **Shared Network Port** page.

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

    *   **Use DHCPv4 Supplied Time Settings**—Specifies whether iLO uses the DHCPv4 server-supplied time.

    *   **Use DHCPv4 Supplied WNS Servers**—Specifies whether iLO uses the DHCP server-supplied WINS server list. If not, enter the WINS server addresses in the Primary WINS Server and Secondary WINS Server boxes.

*   **IPv4 Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.

- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.

- **Gateway IPv4 Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.

- **Static Route #1**, **Static Route #2**, and **Static Route #3**—The iLO static route destination, mask, and gateway addresses. If **Use DHCPv4 Supplied Static Routes** is used, these values are supplied automatically. If not, enter the static route values.

- **Primary DNS Server**—Enter the IPv4 address for the primary DNS service.

- **Secondary DNS Server**—Enter the IPv4 address for the secondary DNS service.

- **Tertiary DNS Server**—Enter the IPv4 address for the tertiary DNS service.

NOTE: When DNS server locations are configured in both IPv4 and IPv6, both sources are used, with preference given according to the iLO Client Applications use IPv6 first configuration option, primary sources, then secondary, and then tertiary.

- **Enable DNS Server Registration**—Select this option to enable iLO to register its IPv4 address and name with a DNS server.

- **Primary WINS Server**—Enter the IPv4 address for the primary WINS server.

- **Secondary WINS Server**—Enter the IPv4 address for the secondary WINS server.

- **Enable WINS Server Registration**—Select this check box to enable iLO to register the IPv4 address for the WINS server(s).

- **Ping Gateway on Startup**—Select this check box to have iLO send request packets to the gateway when iLO initializes.

To edit the settings on the IPv4 tab:

1. In the **iLO Configuration Utility** window, click **Network Settings**. The General tab data appears.
2. Click the **IPv4** tab. The IPv4 tab data appears.
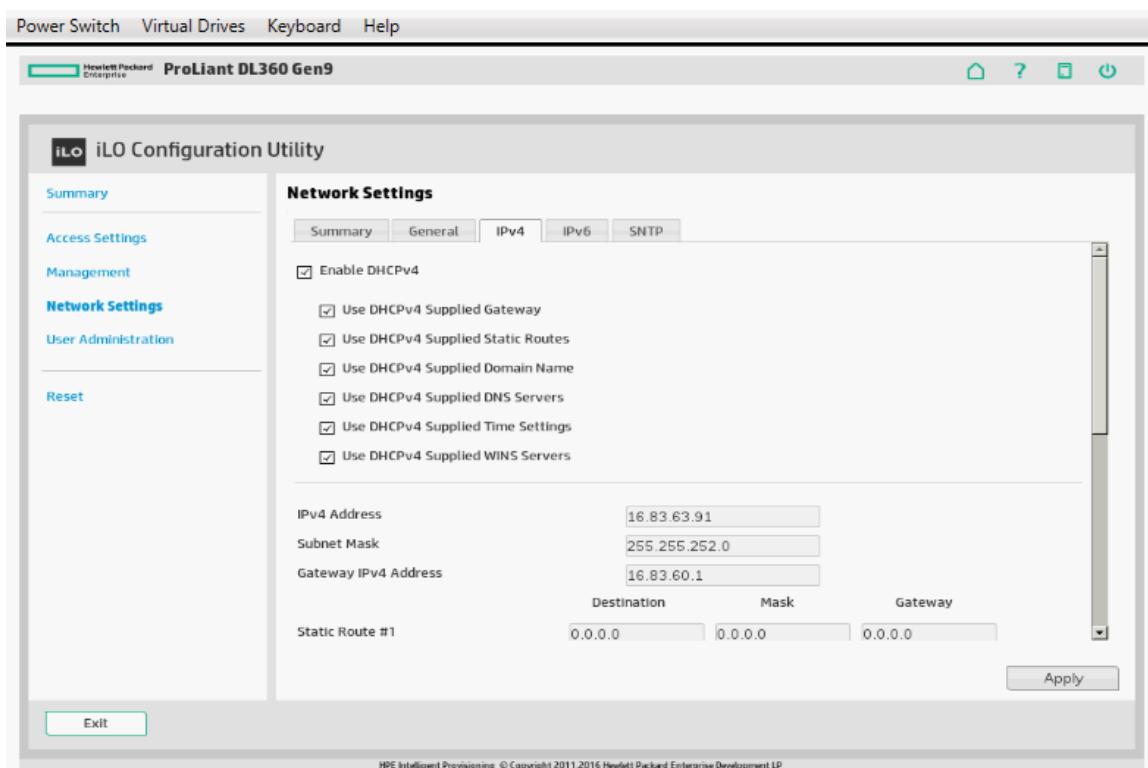
3. If you have enabled DHCPv4, clear the check box.
4. Edit the setting(s) as necessary. Click **Apply**.

Network Settings–IPv6

- **iLO Client Applications use IPv6 first**—When both IPv4 and IPv6 service addresses are configured for iLO client applications, this option specifies which protocol iLO tries first when accessing a client application. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.

  ○ Select this check box if you want iLO to use IPv6 first.

  ○ Clear this check box if you want iLO to use IPv4 first.

  If communication fails using the first protocol, iLO automatically tries the second protocol.

- **Enable Stateless Address Auto Configuration (SLAAC)**—Select this check box to enable iLO to create IPv6 addresses for itself from router advertisement messages.

  NOTE: iLO will create its own link-local address even when this option is not selected.

- **Primary DNS Server**, **Secondary DNS Server**, **Tertiary DNS Server**—Enter the IPv6 addresses for the DNS service.

  When DNS server locations are configured in both IPv4 and IPv6, both sources are used, with preference given according to the iLO Client Applications use IPv6 first configuration option, primary sources, then secondary, and then tertiary.

- **Use DHCPv6 Supplied NTP Servers**—This option determines whether iLO uses the DHCPv6 server-supplied time.

- **Enable DDNS Server Registration**—This option determines whether iLO registers its IPv6 address and name with a DNS server.

- **Static IPv6 Address 1–4**—Enter up to four static IP addresses if they are not automatically assigned. You must specify the prefix length for the addresses.

- **Static Default Gateway**—Enter a default IPv6 gateway address for cases in which no router advertisement messages are present in the network.

- **Static Route #1** (Destination/Gateway), **Static Route #2** (Destination), **Static Route #3**—Enter static IPv6 route destination prefix and gateway address pairs. You must specify the prefix length for the destination. Link-local addresses are not allowed for the destination, but are allowed for the gateway.

To edit the settings on the IPv6 tab:
1. In the **iLO Configuration Utility** window, click **Network Settings**. The General tab data appears.
2. Click the **IPv6** tab. The IPv6 tab data appears.
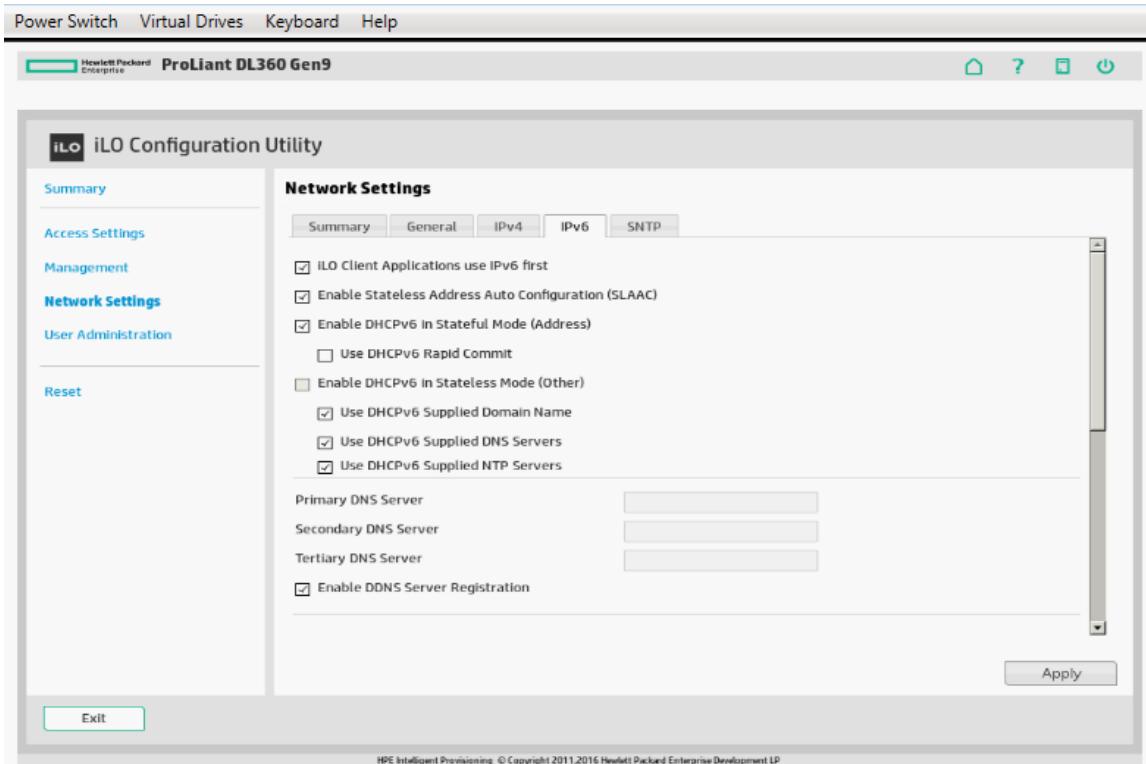
3.   Edit the setting(s) as necessary. Click **Apply**.

Network Settings–SNTP

*   **Use DHCPv4 Supplied Time Settings**—Specifies whether iLO uses the DHCP server-supplied time.

*   **Use DHCPv6 Supplied Time Settings**—Specifies whether iLO uses version 6 of the DHCP server-supplied time.

*   **Propagate NTP Time to Host**—Specifies whether ILO uses NTP time instead of the DHCP server-supplied time.

*   **Primary Time Server**—If DHCPv4 or DHCPv6 SNTP is not used, enter a time server address in the Primary Time Server box.

*   **Secondary Time Server**—If DHCPv4 or DHCPv6 SNTP is not used, enter a secondary time server address in the Secondary Time Server box.

*   **Time Zone**—A drop-down list of worldwide time zones.

To edit the settings on the SNTP tab:

1.   In the **iLO Configuration Utility** window, click **Network Settings**. The General tab data appears.
2.   Click the **SNTP** tab. The SNTP tab data appears.

3. If you enabled DHCPv4 or DHCPv6 time settings, clear the appropriate check box.
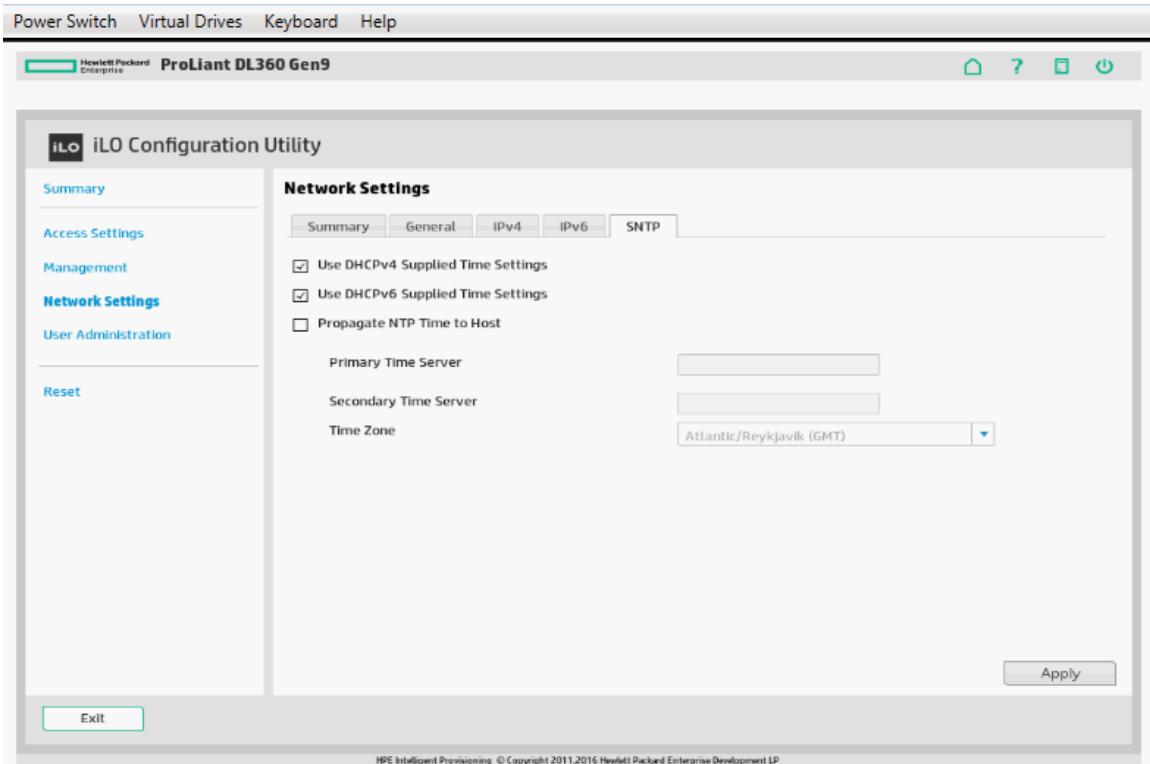4. Edit the setting(s) as necessary. Click **Apply**.

Editing User Administration

- **User Accounts**—Displays available users.

  - **User Name**—Appears in the user list on the User Administration page and on the iLO Overview page. It does not have to be the same as the Login Name. The maximum length for a user name is 39 characters. The user name must use printable characters.

  - **Login Name**—Is the name that you must use when logging in to iLO. The maximum length for a login name is 39 characters. The login name must use printable characters.

  ⓘ **IMPORTANT:** The Login Name cannot be modified, once it is set.

- **Privileges**—Select from the following permissions:

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

  - **Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration.

  - **Remote Console Access**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.

  - **Virtual Media** —Enables a user to use the Virtual Media feature on the host system.

  - **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the button.

To add a new user:

1. In the iLO Configuration Utility window, click **User Administration**. The User Administration window appears.
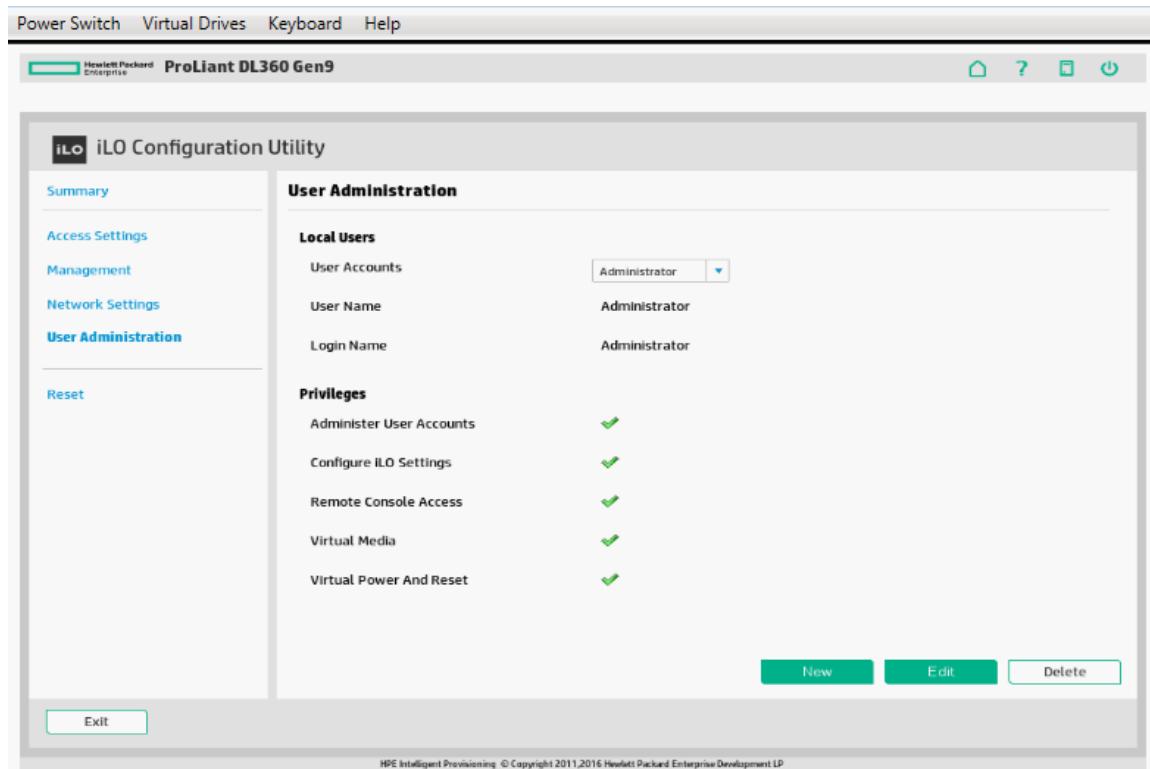
2. Click **New**. The Add User window appears.
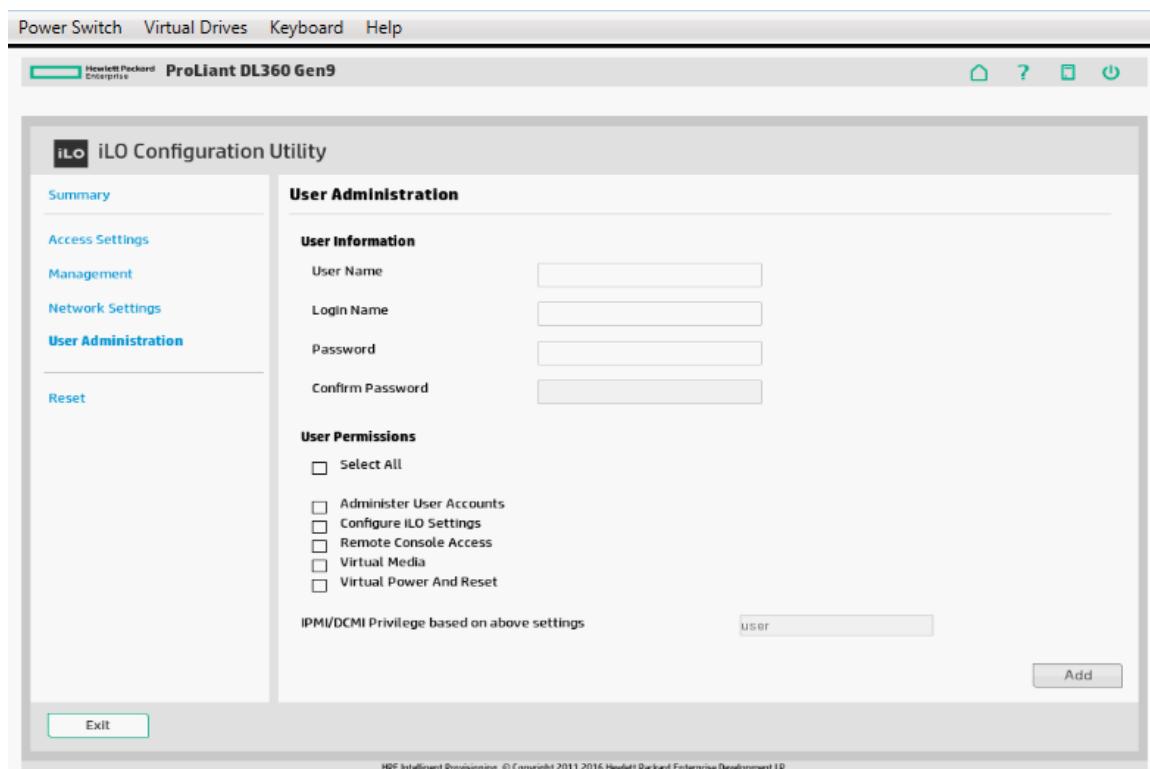
3. Enter the user name. The maximum length for a user name is 39 characters. The user name must use printable characters.

4. Enter the login name. The maximum length for a login name is 39 characters. The login name must use printable characters.

ⓘ **IMPORTANT:** The Login Name cannot be modified, once it is set.

5. Enter the password. The minimum length for a password is set on the **Access Settings** page. The maximum length for a password is 39 characters.
6. Re-enter the password to confirm it.
7. Select the appropriate user permission(s) for the user you are adding.
8. Click **Add**.

To edit an existing user's account:

1. In the iLO Configuration Utility window, click **User Administration**. The User Administration window appears.
2. Click **Edit**. The Edit User window appears.
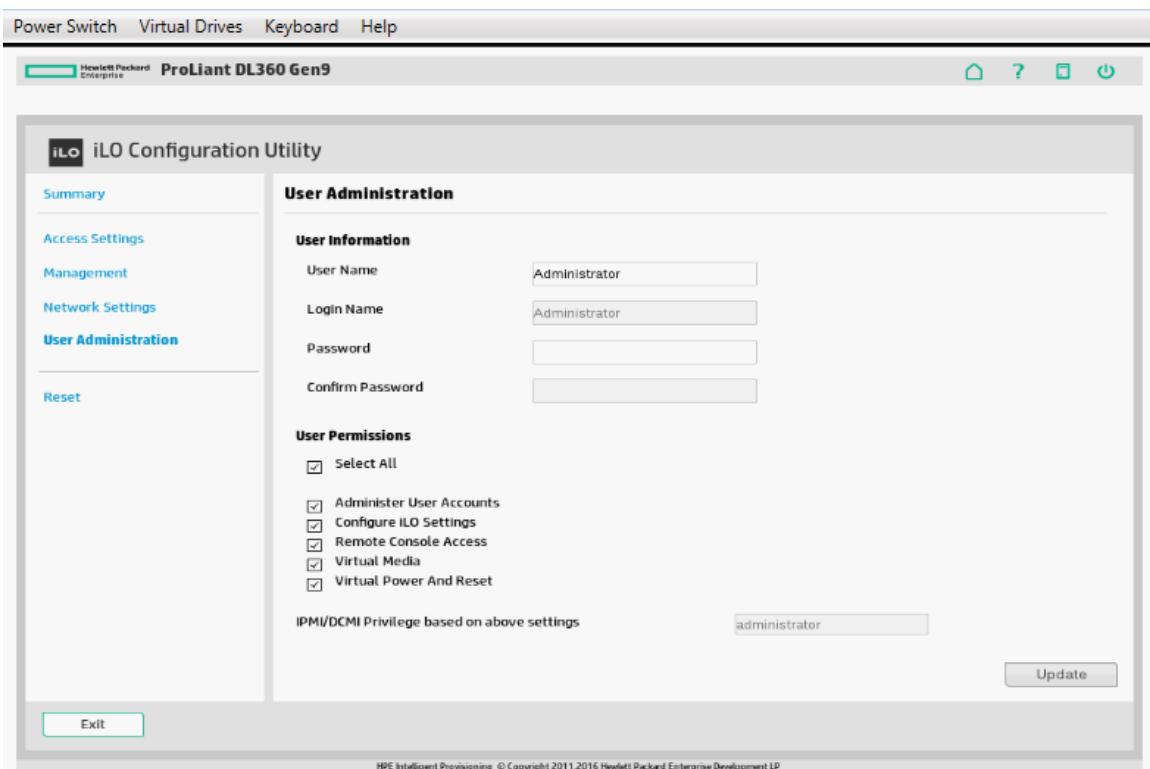
3. Enter the User Name for the user's account you are editing.
4. Enter the user's password. Re-enter the password to confirm it.
5. Select the check boxes to modify the user's permissions.
6. Click **Update**.

To delete a user account:

1. In the iLO Configuration Utility window, click **User Administration**. The User Administration window appears.
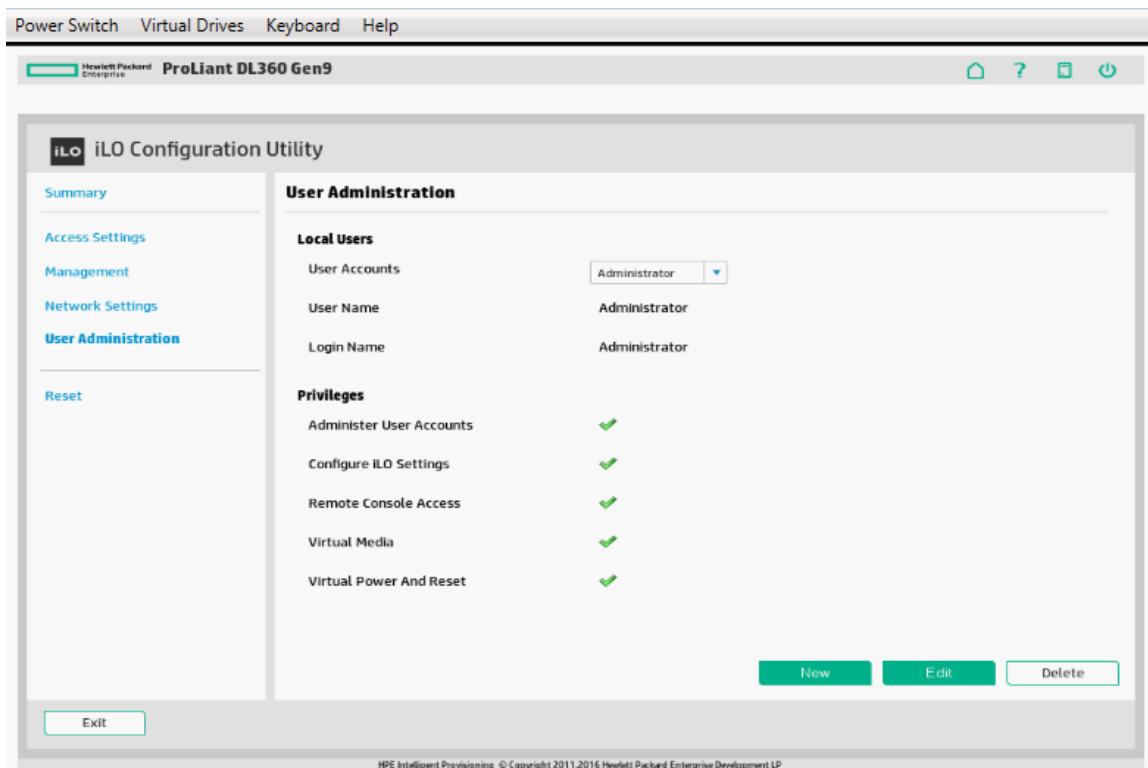
2. In the **User Accounts** drop-down list, select the user account you want to delete.
3. Click **Delete**. Click **OK** to delete the user account, or click **Cancel**.

Resetting iLO

Use this screen to reset iLO, or to restore iLO to factory default settings.

- **Reset iLO**—Click to reset iLO.

- **Reset to Factory Default Settings**—Click to restore factory default settings.

To reset iLO:

1. In the iLO Configuration Utility window, click **Reset**. The Reset iLO window appears.
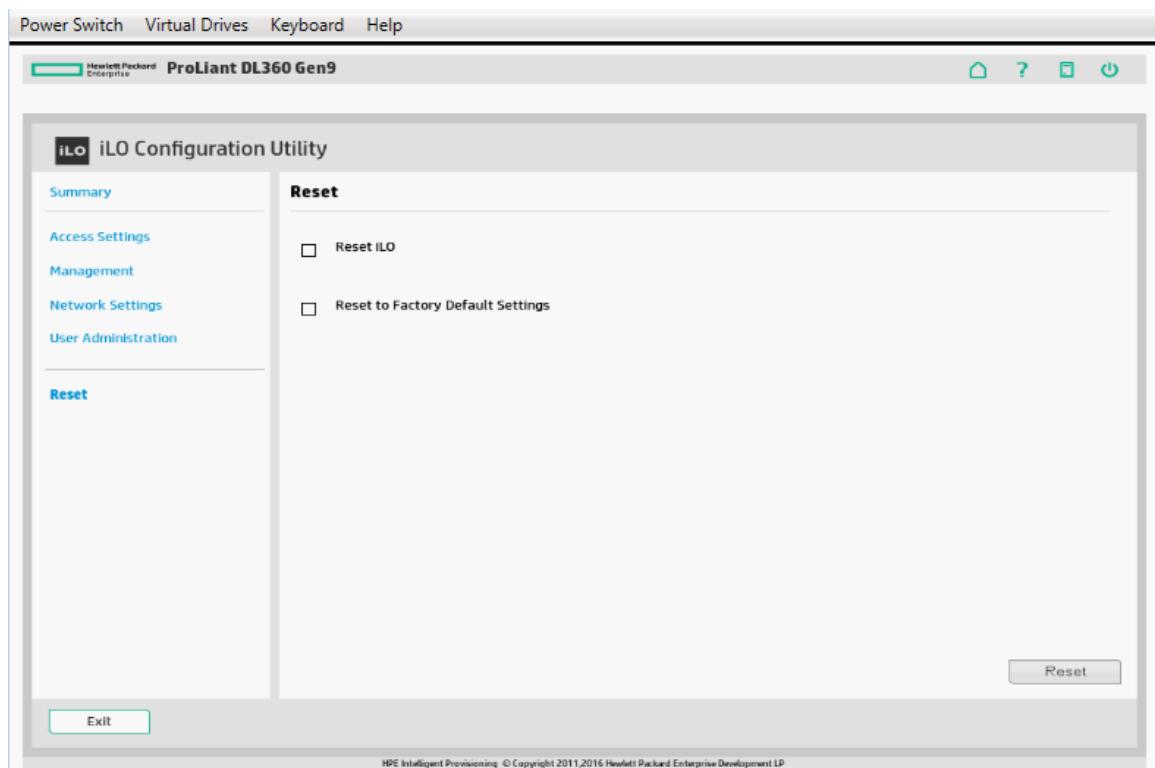
2. Select the check box for the option you want. Click **Reset**. iLO will be reset. You will have to log in again.

Using HPE remote support

You can access the HPE remote support feature from **Perform Maintenance** and tasks you can do include unregistering and updating the proxy settings.

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **HPE Insight Remote Support** from the maintenance options.

When initially configuring Intelligent Provisioning for use, this screen is displayed in "Step 3: Registering for HPE remote support" (page 13).

Unregistering from HPE remote support

The process to unregister from remote support depends on whether you used the Insight Online direct connect or Insight Remote Support central connect registration method.

Unregistering from Insight Online direct connect

1. Navigate to the **Perform Maintenance** page, and then select **HPE Insight Remote Support**.
2. Click **Unregister**.

Intelligent Provisioning notifies you that the server is no longer registered.

Unregistering from Insight Remote Support central connect

1. Log in to the Insight RS Console.

2. Do one of the following:

- To stop monitoring a server temporarily, select the server on the **Devices→Device Summary** tab in the Insight RS Console, and then select **ACTIONS→DISABLE SELECTED**.

  Unregistering the server directly from Intelligent Provisioning is the same as temporarily disabling the server in the Insight RS Console.

- To stop monitoring a server permanently, delete the server from the Insight RS Console. To delete the server, select it on the **Device Summary** tab, and then select **ACTIONS→DELETE SELECTED**.

3. Navigate to the **Perform Maintenance→HPE Insight Remote Support** page in Intelligent Provisioning.
4. Verify that the server is not registered.

Editing the web proxy settings (Insight Online direct connect only)

If the web proxy settings change after a server is registered for remote support, update the settings to enable the server to continue to send remote support data to Hewlett Packard Enterprise.

1. Navigate to the **Perform Maintenance** page and select **HPE Insight Remote Support**.
2. Click **Update Proxy**.
3. Update the following settings, as needed:

- **Web Proxy Server**—Enter the hostname or IP address.
- **Web Proxy Port**
- **Web Proxy Username**
- **Web Proxy Password**

4. Click **Update Proxy**.

Using License Management

Use the License Management feature to activate the iLO Advanced License Pack and the HPE SmartCache License Pack.

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **License Management** from the maintenance options.

   The License Management window is displayed which includes a list of licenses appropriate for your server.

3. Enter the License Key for the iLO Advanced License Pack and/or the HPE SmartCache License Pack.

- The iLO Advanced License Pack enables remote media access and enhanced diagnostics and runtime functions.
- The HPE SmartCache License Pack enables the Smart Array Controller to make use of solid state devices to accelerate access to data residing on hard drives.

4. Click **Apply** to activate your licenses.

Using the Erase Utility

Use the Erase Utility to clear hard drives and the Active Health System logs, and to reset the RBSU settings in the UEFI System Utilities.

Erase Utility options

Select the erase option you want to use for each device.

Device	Do Not Erase	Reset	Secure Erase Mode
All Hard Drives	Does not erase any hard drive operations	Erases the master boot record of the hard drives, so they are no longer bootable	Performs an overwrite pattern erase, so no data is recoverable. The VID is also erased. For more information, see "Using Secure Erase" (page 76).[1]
Active Health System log	Does not erase AHS logs	Mounts AHS partitions and erases all files in the partition	Not an available option
RBSU	Does not reset RBSU settings	Resets the RBSU settings to default	Not an available option

[1] Hard Drive Secure Erases may take hours, or, for larger drives, days to complete. This is expected behavior for this thorough erase procedure.

Accessing Erase Utility

△ **CAUTION:** Perform a backup before running the Erase Utility. The utility sets the system to its original factory state, deletes the current hardware configuration information, including array setup and disk partitioning, and erases all connected hard drives completely. Based on your selections in this utility, the Erase Utility erases data from the specified areas of the system. Existing data and system configuration settings are lost.

To use the Erase Utility:
1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Erase Utility** from the maintenance options.
3. Select the desired erase option for each device.
4. Click **Erase**. A **Confirm Erase** window appears, prompting you to click **OK** to initiate the Erase procedure, or click **Cancel** to cancel the Erase.
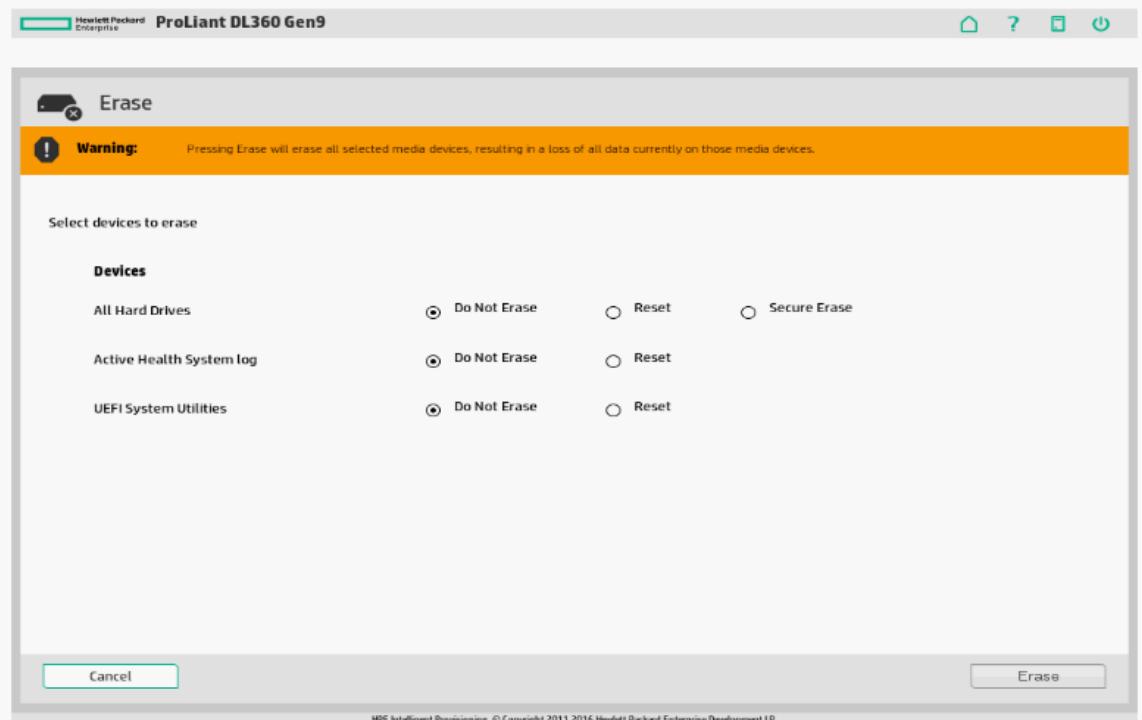
Using Secure Erase

Intelligent Provisioning provides secure erase functionality for the internal system storage and hard disks following the guidelines outlined in DoD 5220.22-M. Secure erase overwrites all block devices attached to the system through applying random patterns in a three-pass process. These block devices include hard disks, storage systems attached to the server, as well as the internal storage used by iLO. Depending on the amount of storage installed on a system, the secure erase process can take many hours or even days to complete.

△ **CAUTION:**

- Secure Erase should be used with extreme caution and only when a system is being decommissioned. The secure erase process will reset iLO and lose all licenses stored there, reset BIOS settings in many cases, and delete all AHS and warranty data stored on the system. iLO will reboot multiple times after the process is complete.

- Disconnect any FCoE, iSCSI, external SAS, and Fibre Channel storage before using secure erase, unless they should also be erased.

5 Advanced topics

Using a provided script to create an Intelligent Provisioning update mirror

For Windows environments, Hewlett Packard Enterprise provides a script that can populate the Intelligent Provisioning update mirror repository for you. When creating this mirror, you upload the software and firmware delivered through SPP to a server within your local network. Then, when updating servers in your network, they can access the firmware and software on the local server instead of the website, and can therefore greatly increase the speed of updates to the servers.

This script uses hp-ipcli to automate the process.

Procedure 1

1. Obtain the script from the FTP site: **ftp://ftp.hp.com/pub/softlib2/software1/pubsw-windows/p1911695011/v118289/ipcli.exe**

2. Run the tool from the command line, pointing it to the directory with which you want to serve the files, and optionally, if a Proxy server is required, enter the second command:

   ```
   >ipcli.exe –dir <path to the directory from which you will serve the files>
   >ipcli.exe –dir <path to the directory from which you will serve the files> -proxy
   http://proxy.yourcompany.com:8080/proxy
   ```

   NOTE: Prompts for input may occur while the tool is running.

3. When the downloads are finished, open the config.xml and change the "replace" to the URL at which you will be serving the files.

Configure a ProLiant server to use the newly created update mirror

1. Select **Intelligent Provisioning Preferences** from the **Perform Maintenance** screen.
2. Change **System Software Update** to **Custom URL**, and enter the URL at which you are serving the files.

Creating an Intelligent Provisioning update mirror

Use an Intelligent Provisioning update mirror to access software and firmware delivered through SPP from a server within your local network, increasing the speed of updates.

The mirror requires a web server running on a server with any OS capable of serving files over FTP or HTTP.

To create an Intelligent Provisioning update mirror for an SPP:

1. Download the SPP and copy the files to your web server:
   a. Download the `.iso` file from the website:

      http://www.hpe.com/servers/spp/download

   b. Mount the SPP ISO and copy the contents to your web server. The following example uses UNIX commands and assumes that the web server is serving the files from `/srv/www/spp-version1`. On Windows, you can use a utility to mount the ISO and then copy the files with Windows Explorer.

      ```
      # mkdir -p sppmount
      # mount -o loop SPP2011.09.0.iso sppmount
      # mkdir -p /srv/www/spp-version1
      # cp -r ./sppmount/. /srv/www/spp-version1
      # umount sppmount
      # rmdir sppmount
      ```

2. If you want to host the Intelligent Provisioning software on the mirror, download the latest version of Intelligent Provisioning and copy the files to your web server:

   a. Navigate to the website:

      ```
      ftp://ftp.hpe.com/pub/softlib2/software1/pubsw-linux/p1048499843
      ```

   b. From the newest folder, download the following files:

      - `Gaius.img.gz`

      - `Vid.img.gz`

      - `Hp_manifest.zip`

   c. Copy the files to your web server.

      ```
      # cp gaius.img.gz /srv/www/ipupdate-1.00
      # cp vid.img.gz /srv/www/ipupdate-1.00
      # unzip -d /srv/www/ipupdate-1.00 hp_manifest.zip
      ```

3. Update the URLs in the SPP configuration files to address your web server:

   a. Create or modify the file `spp-version1/hp_manifest/config.xml`, adding rules to rewrite the URLs to reference your web server. For example,

      ```
      <?xml version="1.0" encoding="UTF-8"?>
      <hp_manifest schema_version="1.0.0.0"><index>
        <config>
          <rewrite_url
            pattern="file://\."
            replace="http://myserver/spp-version1"
          />
        </config>
        </index>
      </hp_manifest>
      ```

      In the previous example, Intelligent Provisioning replaces each URL that starts with `file://` with a URL on your web server. For example, a request for `file://./hp/swpackages/CP0012345.scexe` is converted to `http://myserver/spp-version1/hp/swpackages/CP0012345.scexe`.

   b. Update `spp-version1/hp_manifest/index.xml` to reference `config.xml` if it is not already listed.

      ```
      <?xml version="1.0" encoding="UTF-8"?>
      <hp_manifest schema_version="1.0.0.0">
        <index>
          <include src="meta.xml" type="meta" lang="en" />
          <include src="meta-ja.xml" type="meta" lang="ja" />
          <include src="os.xml" type="operating_systems" />
          <include src="type.xml" type="type" />
          <include src="system.xml" type="systems" />
          <include src="device.xml" type="devices" />
          <include src="category.xml" type="categories" />
          <include src="config.xml" type="config" />
        </index>
      </hp_manifest>
      ```

4. If you are hosting the Intelligent Provisioning software on your mirror, update the URLs in the Intelligent Provisioning configuration files to address your web server:

   a. Create or modify the file `ipupdate-1.00/hp_manifest/config.xml` and add rules to rewrite the URLs to reference your web server.

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <hp_manifest schema_version="1.0.0.0"><index>
     <config>
       <rewrite_url
         pattern="file://\."
         replace="http://myserver/ipupdate-1.00 "
       />
     </config>
   </index>
   </hp_manifest>
   ```

   In the previous example, the Intelligent Provisioning software replaces each URL that starts with `file://` with a URL on your web server. For example, a request for `file://./gaiusw.img.qz` is converted to `http://myserver/ipupdate-1.00/gaius.img.gz`.

   b. Update `ipupdate-1.00/hp_manifest/index.xml` to reference `config.xml` if it is not already listed.

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <hp_manifest schema_version="1.0.0.0">
     <index>
       <include src="meta.xml" type="meta" lang="en" />
       <include src="meta-ja.xml" type="meta" lang="ja" />
       <include src="os.xml" type="operating_systems" />
       <include src="type.xml" type="type" />
       <include src="system.xml" type="systems" />
       <include src="device.xml" type="devices" />
       <include src="category.xml" type="categories" />
       <include src="config.xml" type="config" />
     </index>
   </hp_manifest>
   ```

5. Create an `index.xml` file to redirect FTP or HTTP requests from the URL entered in the Intelligent Provisioning user interface to the locations of the update files.

   For example, to use the URL `http://mywebserver/update-src/hp/proliant` in the Intelligent Provisioning user interface, create the following `index.xml` file and place it in the `update-src/hp/proliant` directory relative to your web server's root directory.

   ```xml
   <?xml version="1.0" encoding="UTF-8"?>
   <hp_manifest schema_version="1.0.0.0">
     <index>
       <include
         src="http://myserver/spp-version1"
         type="redirect"
       />

       <include
         src="http://myserver/ipupdate-1.00"
         type="redirect"
       />
     </index>
   </hp_manifest>
   ```

Mirroring different SPPs to different servers

You can add regular expressions to the `index.xml` file so that the web server serves different SPPs to different servers based on SMBIOS runtime attributes. If the regular expression matches the SMBIOS information, the file is included; otherwise it is ignored.

Table 1 Regular expression attributes

Attribute name	SMBIOS attribute
product_name	SMBIOS product name (dmidecode — string system-product-name)
product_serial	SMBIOS serial number (smidecode — string system-serial-number)
product_uuid	SMBIOS uuid (dmidecode — string system-id)
bios_family	ROM family (dmidecode — string bios-version)

For example, to configure a mirror that serves different SPPs for different types of servers, you can add the `product_name` attribute to the redirect commands in the `index.xml` file. In the following example, the DL380 servers access spp-version1 while the DL580 servers access spp-version2.

```
<?xml version="1.0" encoding="UTF-8"?>
<hp_manifest schema_version="1.0.0.0">
  <index>
    <include
      src="http://myserver/spp-version1"
      type="redirect"
      product_name=".*dl380.*"
    />

    <include
      src="http://myserver/spp-version2"
      type="redirect"
      product_name=".*dl580.*"
    />

    <include
      src="http://myserver/ipupdate-1.00"
      type="redirect"
    />
  </index>
</hp_manifest>
```

Using the HPE USB Key Utility

-

HPE USB Key Utility

The HPE USB Key Utility is a Windows application that copies Intelligent Provisioning or SPP contents, and other CD or DVD images to a USB flash drive. After copying data to the USB flash drive, you can run Intelligent Provisioning or SPP from the USB flash drive instead of from a CD or DVD. This process is beneficial in headless-server operations. It also simplifies the storage, transportation, and usage of the contents by allowing you to retrieve their images from the web and customize them as needed.

Installing the utility adds a shortcut in System Tools in the Programs Start menu folder.

Features

The USB Key Utility supports:

- ISO files larger than 1 GB.

- Quick Formatting on USB flash drives.

- USB flash drives up to a maximum of 32 GB. USB flash drives larger than 32 GB are not displayed in the utility.

USB Key Utility supports multiple images on a single USB flash drive if there is adequate space available on the USB flash drive and you are not loading content that works with a UEFI bootloader, which does not support multiple images due to security reasons.

NOTE: HP SUM 6.2.0, SPP 2014.02.0, and Intelligent Provisioning 1.60 and later do not support multiple-boot environments on a single device. HP SUM, SPP, and Intelligent Provisioning contain signed parts to work with the UEFI bootloader. Use only single-image boot configurations with the USB Key Utility.

Prerequisites

Installing applications onto a USB flash drive requires a supported source CD, DVD, or ISO, and a USB flash drive with adequate storage space for storing the source contents. The USB Key Utility requires a USB 2.0 flash drive with a storage size larger than the media or ISO image (2 GB or greater).

NOTE: Version 2.0 and later of the USB Key Utility does not support a 32-bit operating system. Use version 1.8 of the utility in 32-bit environments.

AutoRun files

AutoRun files do not start automatically from the utility. To start an AutoRun file, double-click the `autorun.exe` file in the appropriate CD or DVD folder on the USB Key.

Creating a bootable USB key

To create a bootable USB key:
1. Double-click the **HPE USB Key Utility** shortcut in the HPE System Tools folder.

2. Complete each step as presented by the application:
   a. Click **Next** at the splash screen.
   b. Read the End-User License Agreement, and then select **Agree** and click **Next**.
   c. Select **Create a bootable USB key from CD/DVD**, and then click **Next**.
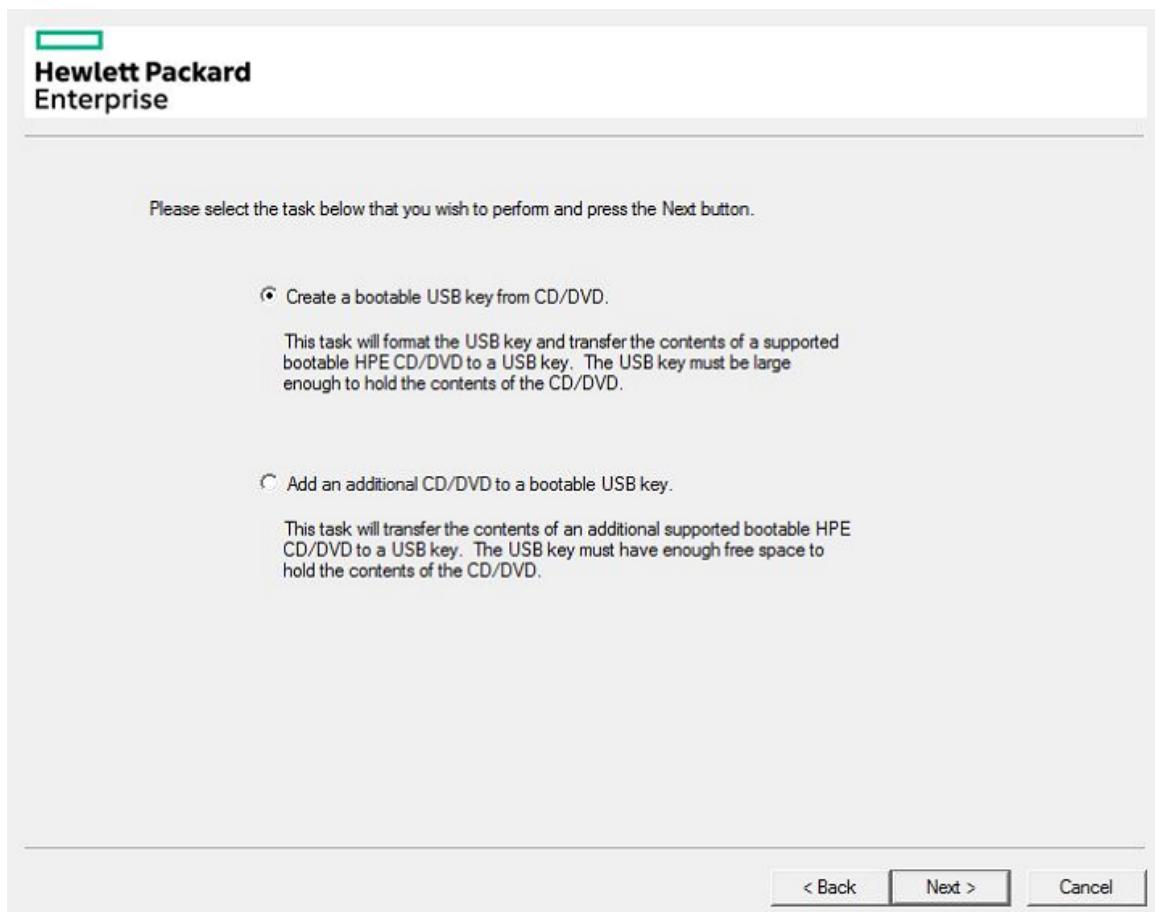
   d. Place the USB flash drive in an available USB port. Insert the media in the optical drive or mount the ISO image, and then click **Next**.
   e. Choose the drive letter of the source, choose the drive letter of the target USB flash drive, and click **Next**.

   ☼ **TIP:** Click **Rescan Target** if you do not see your drive key or just insert a new one.

△ **CAUTION:**   All data on the target USB key will be deleted.

f. Click **Next** on the warning message screen. The USB flash drive is formatted, and the source contents are copied to the USB flash drive.

g. Click **Finish** to display the README.TXT file.

6 Troubleshooting

This chapter includes topics on troubleshooting general issues, Windows-specific issues, Linux-specific issues, and VMware-specific issues. Directions for corrective action are provided where possible.

Troubleshooting general issues

When F10 is pressed a grub error appears

Symptom

Cannot access Intelligent Provisioning and a black screen appears with the following error listing the installed graphics processing unit (GPU):

```
Welcome to GRUB! error: no such device:
```

Cause

All Gen8 and Gen9 ProLiant servers only provide F10 video on the embedded video card and through the iLO remote console. If a GPU is installed in addition to the embedded video card, the software is unable to determine the "right" monitor at boot time, and the F10 video redirects to the iLO virtual video or the onboard video port.

Action

Plug the video cable into the onboard video port, or access Intelligent Provisioning through the iLO remote console.

Installation interrupted when deploying a profile

Symptom

When deploying a profile containing OS settings on a server that does not have disks connected, the OS settings are applied and the installation is interrupted without displaying a `There are no physical disks attached` error message to indicate a problem has occurred.

Cause

No disks are connected to the server.

Action

Attach the disks and retry.

Unable to boot in UEFI Mode

Symptom

You are unable to boot your system in UEFI Mode and complete the OS setup. The screen displays a message that no available boot device can be found and reboots.

Cause

You are using an unsupported option card.

Action

Replace the option card with a supported device that supports UEFI Boot Mode.

The integrated SATA RAID controller (B140i) in ProLiant models is only supported in UEFI Boot Mode. When using Legacy Boot Mode, the B140i controller should be disabled. The B140i controller can only be configured using Intelligent Provisioning and currently cannot be used in

conjunction with other RAID controllers during assisted installation because of driver installation restrictions. To install a system in this configuration, you must manually install the OS by providing the correct driver at install time, and then install the SPP to enable the other devices.

Most supported iSCSI targets are fully supported by Intelligent Provisioning, including many FCoE targets. There are issues involving HPE 3PAR targets using both Broadcom and Emulex-based devices in Microsoft Windows. These devices might require set up in a non-scripted manner using a manual installation or an imaging-based solution.

AHS Download Utility does not download the AHS logs

Symptom

The **Download** button in the AHS Download Utility does not download the AHS logs.

Cause

The system does not recognize the **Download** button the first time it is used.

Action

Retry the operation. The logs should be downloaded when the **Download** button is used a second time.

Cannot access HPE SSA

Symptom

Cannot access HPE SSA from systems supporting SATA RAID operating in Legacy BIOS Boot Mode.

Cause

Dynamic Smart Array (B140i) works only in UEFI Boot Mode.

Action

To access HPE SSA in Legacy BIOS Boot Mode, switch the SATA Controller (in RBSU) to SATA AHCI mode from Dynamic Smart Array mode.

OS-recommended DVD acting as a manual installation

Symptom

The OS-recommended DVD is acting as a manual installation when the server is set up to be password protected.

Cause

The system is password protected and no changes can be applied that will bypass this issue.

Action

None. The Intelligent Provisioning installation process is working as designed.

System Information page not displaying information

Symptom

While performing offline flashing with SPP, information for InfiniBand cards is not displayed on the **System Information** page.

Cause

The **System Information** page does not display information for InfiniBand cards.

Action

You can see system information by booting a full operating system and running Insight Diagnostics, which shows what hardware is connected.

Active Health System (AHS) log option selected for Secure Erase

Symptom

When selecting the **Secure Erase** option for Onboard NAND Flash, the Active Health System (AHS) log option is also selected by default.

Cause

The AHS secure erase process does not initiate with the Onboard NAND Flash option in the Erase Utility.

Action

None. The process is working as designed.

Controllers not accessible in Legacy BIOS Boot Mode

Symptom

Some boot controllers are inaccessible on multicontroller systems set to Legacy BIOS Boot Mode.

Cause

This is normal operation caused by a system restriction.

Action

To target the other controller, remove the unwanted controller and proceed with the installation. Using Manual installation is also an option.

Installation fails with SD card

Symptom

Installation fails with SD card on a system set to Legacy BIOS Boot Mode.

Cause

SD cards are only supported in UEFI Boot Mode. Installations in Legacy BIOS Boot Mode might be unable to boot from the internal device if any other storage (such as a DVD or virtual DVD device) is present in the system.

Action

Use UEFI Boot Mode with SD media.

Intelligent Provisioning does not launch when F10 is pressed

Symptom

Intelligent Provisioning allows service personnel and customers to press the **F10** key during System Power-On Self-Test (POST) to load the latest SPP automatically. If Intelligent Provisioning does not launch as expected, it may be necessary to reinstall Intelligent Provisioning.

Cause

There is an issue with the current Intelligent Provisioning files.

Action

1. Download the firmware ISO image and the USB utility-tool from hpe.com.
2. Create a bootable USB Key and copy the ISO image.
3. Insert the USB Key and power up the unit.
4. To boot from the USB key, press **F11**, and select **Option 3: One Time Boot to USB Drive Key**.
5. The system boots from the USB Key and installs IP Recovery.
6. When the installation is complete, the utility prompts for the USB Key to be removed.
7. Reboot the system and press **F10** (IP Recovery) to verify IP Recovery launches properly.

Troubleshooting Windows-specific issues

Installation of Microsoft Hyper-V Server 2012 R2 fails

Symptom

When installing Microsoft Hyper-V Server 2012 R2 using an SD card, the installation fails.

Cause

The Windows media may not support the high speed USB controllers on some ProLiant servers and be unable to run from SD media.

Action

Install Hyper-V Server 2012 R2 using the Microsoft install tools instead of using Intelligent Provisioning.

Windows installation fails

Symptom

The Windows installation process fails with selected language.

Cause

The Windows installation process fails because an unsupported language has been selected. The installation media must support the OS Language selected.

Action

Ensure the language selected is supported by the Windows installation media.

Integrated Management Log (IML) not generated

Symptom

When viewing the Integrated Management Log (IML) after installing Windows, the log is not generated and the following error message is displayed: `No system management driver is loaded.`

Cause

Need proper access to view the IML log.

Action

Use the **Run as administrator** option to launch the IML Viewer.

Microsoft Hyper-V Server 2012 installation fails

Symptom

When attempting to install Microsoft Hyper-V Server 2012, the installation fails and the following error message is displayed: `Unattended settings error.`

Cause

Windows 2012 OS family and the Hyper-V OS is not selected. These options must be selected when installing Microsoft Hyper-V Server 2012.

Action

Select the Windows 2012 OS family and the Hyper-V OS.

No information on the System Management Homepage

Symptom

No information is displayed on the System Management Homepage after a Recommended installation of Windows.

Cause

This is expected behavior because by default only AMS is installed.

Action

To display the information on the System Management Homepage, install WBEM or SNMP agents.

Troubleshooting Linux-specific issues

Manual installation of SUSE Linux Enterprise Server 12 fails

Symptom

Manual installation of SUSE Linux Enterprise Server 12 fails when the server is in Legacy BIOS Boot Mode.

Cause

SUSE Linux Enterprise Server 12 does not support manual installation in Legacy BIOS Boot Mode.

Action

Switch the server to UEFI Boot Mode instead and retry the installation.

Installation of SUSE Linux Enterprise Server 12 halts

Symptom

When attempting to install SUSE Linux Enterprise Server 12, the installation process stops and the following message is displayed:

```
Please make sure your installation medium is available. This can occur
if the installation involves a file server in a Windows domain. This
can occur when using either Legacy BIOS or UEFI Boot Modes.
```

Cause

The file server is part of a Windows domain.

Action

Make sure the file server is not part of a Windows domain. An alternative is to use disk installation to avoid this problem.

Firmware update fails for Linux x86_64

Symptom

When performing a Firmware Update, the update process fails to update the Broadcom Online Upgrade Utility for Linux x86_64.

Cause

The firmwar update process does not support updating the Broadcom Online Upgrade Utility for Linux x86_64.

Action

Update the firmware under the installed OS.

Unable to browse Red Hat OS

Symptom

When installing Red Hat Enterprise Linux 6, you are unable to browse the Red Hat OS files while saving the **Deployment Setting** profile.

Cause

While selecting Red Hat OS flat files in Deployment Settings, if a `This media does not match the selected OS.` message is displayed, either the wrong OS family is selected, or some of the OS files are missing from the OS flat file folder.

Action

Make sure all required Red Hat OS files are present in the OS Flat file folder.

Unable to proceed with Recommended installation of Red Hat Enterprise Linux 6

Symptom

When installing Red Hat Enterprise Linux 6, you are unable to proceed with the Recommended installation with valid OS images through FTP source media.

Cause

Required Red Hat OS files are missing or incorrectly placed.

Action

While performing Red Hat recommended installation using FTP source media, make sure that all the required Red Hat OS files are present in the OS flat file folder. If files are missing or incorrectly placed, you might not be able to continue with installation. Also make sure that two TRANS.TBL files are present in the Red Hat OS flat files folder. One file should be present in the main OS file folder, and another should be present inside the "Server" folder inside the main OS file folder.

Recommended installation of Red Hat OS hangs

Symptom

When using the Recommended installation method for Red Hat OS installation with FTP source media, one of the following problems might occur:

- The installation hangs during reboot and a `The Red Hat Enterprise Linux Server CD was not found` error is displayed.
- The installation hangs and a `Could not allocate requested partitions` error is displayed.
- The installation does not complete successfully, or
- The installation completes successfully even if there are missing flat files for the OS installation.

Cause

Using the Recommended installation method for Red Hat OS installation with FTP source media might not work reliably.

Action

To resolve any of the problems mentioned, obtain the DUD from the HPE Support Center to perform the installation outside of Intelligent Provisioning.

Manual install of SUSE Linux Enterprise Server 12 in Legacy BIOS Boot Mode fails

Symptom

When attempting to perform a Manual install of SUSE Linux Enterprise Server 12 in Legacy BIOS Boot Mode, the install fails with a boot loader error.

Cause

Manual installation of SUSE Linux Enterprise Server 12 in Legacy BIOS Boot Mode is not supported.

Action

Use UEFI Boot Mode when installing SUSE Linux Enterprise Server 12.

Troubleshooting VMware-specific issues

Continue arrow is visible during ESXi Custom installation

Symptom

On the **OS Information** screen for ESXi Custom installation, the Continue arrow is visible.

Cause

A host name is not entered in the **Host Name** field.

Action

Make sure the **Host Name** field contains at least three characters.

Server reboots during VMware Recommended installation

Symptom

When performing a VMware Recommended installation with DVD as source media, after copying the OS files the server displays the message `Press Enter to reboot`. Pressing **Enter** causes the server to begin loading the ESXi installer again rather than opening the OS.

Cause

VMware OS installed on HDD will continuously reboot if a USB is connected to SUT.

Action

Remove the USB device and the installation will continue.

Installing VMware ESXi Custom Image

Symptom

Cannot install VMware Custom Image.

Cause

VMware ESXi Custom Image requires a custom HPE ISO.

Action

Download the ISO from the VMware website.

VMware ESXi install on a multiple controller system fails

Symptom

When installing VMware ESXi on a multiple controller system, the install process hangs.

Cause

While installing VMware ESXi on a multiple controller system the installation might enter an install loop and continually run the installer depending on which controller is chosen. The VMware installer does not detect the controller boot preferences and may choose a different target disk than that selected in the user interface, resulting in a continuous loop.

Action

Disconnect one controller or perform a Manual installation so the correct disk can be manually selected.

Customer advisories

Additional problem-solving information is available from the following sources:

- How to Install/Reinstall Intelligent Provisioning if It Does Not Launch After Pressing F10 During POST: **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c03693433**

- Windows Installations May Fail on 3 TB Volumes In Some Configurations: **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c03711970**

- Unable to Launch Successfully if More Than 32 Logical Drives Are Created: **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=c03686831**

- Installation of SUSE Linux Enterprise Server 12 Halts When Using Intelligent Provisioning on an ProLiant Server In Legacy Mode: **http://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c04565685**

Intelligent Provisioning Recovery

Download and use the Intelligent Provisioning recovery media when a mass update is required for several servers, a new board has become corrupted, or a NAND error has occurred. Mass update of several systems is available through iLO/RIBCL using recovery media mount and one time boot.

1. Download Intelligent Provisioning at **http://www.hpe.com/info/intelligentprovisioning**.

   NOTE: Gen8 servers supports Intelligent Provisioning 1.x. Gen9 servers supports Intelligent Provisioning 2.x.

2. Select an operating system.
3. Click **Intelligent Provisioning Recovery Media**.
4. Click **Download**.

   NOTE: Once a user downloads the Intelligent Provisioning recovery media file from the Hewlett Packard Enterprise website, it will be a **.ZIP** file. Please extract the **.ZIP** file to a folder and user will find an ISO file. Please use this ISO file to boot the server by using iLO or burn the ISO file to a DVD media and boot the server from DVD

7 Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  www.hpe.com/assistance

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

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)

- Product name, model or version, and serial number

- Operating system name and version

- Firmware version

- Error messages

- Product-specific reports and logs

- Add-on products or components

- Third-party products or components

Accessing updates

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

- To download product updates, go to either of the following:

  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates

  - Software Depot website:

    www.hpe.com/support/softwaredepot

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

  www.hpe.com/support/AccessToSupportMaterials

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

Websites

Website	Link
Intelligent Provisioning	**www.hpe.com/servers/intelligentprovisioning**
HPE iLO 4	**www.hpe.com/info/ilo**

Website	Link
HPE Active Health System	**www.hpe.com/servers/ahs**
HPE Systems Insight Manager	**www.hpe.com/info/hpsim**
Service Pack for ProLiant	**www.hpe.com/servers/spp**
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
Software Depot	**www.hpe.com/support/softwaredepot**
Customer Self Repair	**www.hpe.com/support/selfrepair**
Insight Remote Support	**www.hpe.com/info/insightremotesupport/docs**

Customer self repair

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

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

www.hpe.com/support/selfrepair

Remote support

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

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Glossary

This Glossary provides names and definitions for terms and acronyms commonly used in this document.

Agent
Software on managed servers used to make changes to the servers. Functions supported include software installation and removal, software and hardware configuration, and server status reporting.

AHS
Active Health System is a technology that provides continuous, proactive health monitoring of over 1600 system parameters. It also logs configuration changes for more accurate problem resolution. All information collected by Active Health is logged securely, isolated from the operating system and separate from any customer data.

AMS
Agentless Management Service. AMS is a service that collects OS configuration information about events and provides this information to the iLO Active Health System log.

Captured image
A data store containing all the information from a target server including the files, disk partition information, and anything else needed to completely recreate the target server back to the same server, or perhaps a different one. The captured image does not include partitions, only file system data. See also image installation.

Configuration file
The generic term for Windows and Linux unattended installation files. These files provide all the information required to install the operating system without user intervention. Also applies to hardware configuration utilities such as BIOS configuration and array controller configuration. Customers may create new configurations for their own purposes.

DDNS
Dynamic DNS

DHCP
Dynamic Host Configuration Protocol

Enclosure
A chassis that contains multiple blade servers and interconnect devices.

HP PSP
ProLiant Support Pack. This is product has been replaced by the SPP.

HP SUM
HP Smart Update Manager. HP SUM is a technology that installs and updates firmware and software on ProLiant servers.

HPE SSA
HPE Smart Storage Administrator. HPE SSA consists of utilities that provide high-availability configuration, management, and diagnostic capabilities for all Smart Array products.

HPE USB Key Utility
The HPE USB Key Utility is a Windows application that enables you to copy Intelligent Provisioning contents to a USB flash drive. After being copied to the USB flash drive, Intelligent Provisioning can be started from the USB flash drive instead of from a CD or DVD.

iLO Virtual Media
An Integrated Lights-Out (iLO) feature that enables you to attach a removable storage device or image file from a client machine to the server, and have that appear to the server as a local device. The server can boot from that virtual device or use it with a running operating system.

Image installation
The process of installing a server using a previously captured image of the disk to make a duplicate of the original server. This is in contrast to a scripted installation.

Insight Diagnostics
Insight Diagnostics provides a comprehensive suite of offline system and component tests, providing in-depth testing of critical hardware components for devices such as processors, memory, and hard drives.

Insight Online
Insight Online is a service that automatically aggregates device health, asset, and support information from iLO with contract and warranty information, and then secures it in a single, personalized dashboard that is viewable from anywhere.

Insight Remote Support
Insight Remote Support enables intelligent event diagnosis and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise. These notifications prevent downtime and enable faster issue resolution.

Integrated Lights-Out (iLO)
An independent microprocessor built into ProLiant servers that provides multiple ways to configure, update, and operate servers remotely. iLO can remotely perform most functions that otherwise require a visit to the data center, computer room, or remote location. See **http://www.hpe.com/info/ilo**.

Intelligent Provisioning	Intelligent Provisioning is a single-server deployment tool embedded in ProLiant Gen8, Gen9, that replaces the SmartStart CDs and Smart Update Firmware DVD used with previous generations of ProLiant servers.
Media	Software which can include vendor-supplied OS distribution files, Hewlett Packard Enterprise-provided OS distribution files, captured images, and firmware and driver updates such as the SPP.
Package	A single compressed (zipped) file that can contain executables, configuration information, and script files. An example of a package is a `.zip` file of Windows drivers to be used during unattended installations.
POST	Power on self test. POST is a process performed by firmware or software routines immediately after a device is powered on. The routines are part of a device's pre-boot sequence. Once POST completes successfully, bootstrap loader code is invoked.
Provisioned	A server in this state has an operating system installed.
Provisioning	Installing an operating system on a target server using either scripted installation or captured image deployment.
RBSU	ROM-Based Setup Utility. A configuration utility that is embedded in the system ROM and included with the UEFI System Utilities. This configuration utility performs a wide range of configuration activities that may include: • Configuring system devices and installed options • Displaying system information • Selecting the primary boot controller • Configuring online spare memory
SAN	Storage Area Network. A dedicated network that provides access to consolidated, block-level data storage.
Scripted installation	The OS provisioning method that uses configuration files and OS distribution files to deploy an OS to a target server as an unattended installation. This is the native way the operating system is intended to be installed by the OS vendor but with the interactive installation process automated. This is in contrast to an image installation.
SNTP	Simple Network Time Protocol
SPP	The Service Pack for ProLiant has replaced the Windows and Linux ProLiant Support Pack (PSPs). The SPP is a comprehensive package that includes firmware, drivers, and tools across ProLiant servers, and infrastructure including a broad range of many generations of ProLiant BL/DL/ML/SL 100, 300, 500, 700, and 900 series servers. See **http://www.hpe.com/servers/spp**.
UEFI	The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. UEFI is meant to replace the Basic Input/Output System (BIOS) firmware interface.
Unattended installation	An automatic Windows or Linux OS installation that does not require user intervention.
Unprovisioned	A server waiting to have an operating system installed.
VID	Virtual Install Disk.
WBEM	Web-based Enterprise Management. WBEM is a DMTF (Distributed Management Task Force) standard based on the CIM (Common Information Management) model. WBEM enables customers to manage their systems consistently across multiple platforms and operating systems, providing integrated solutions that optimize your infrastructure for greater operational efficiency. WBEM enables management applications to retrieve system information and request system operations wherever and whenever required.
WMI	Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems.

Index