



Hewlett Packard
Enterprise

Intelligent Provisioning User Guide for HPE ProLiant Gen10 Servers and HPE Synergy

Abstract

This document details how to access and use the Intelligent Provisioning and HPE Rapid Setup Software, including tasks such as installing an OS, updating firmware, software, and drivers, and performing some diagnostic tests. Intelligent Provisioning is included in the optimized server support software from the Service Pack for ProLiant (SPP). This document is intended for administrators experienced in using ProLiant Gen10 servers and HPE Synergy compute modules.

Part Number: 881706-005
Published: August 2019
Edition: 1

Notices

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

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

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

Acknowledgments

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

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

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

Contents

Introduction.....	6
Intelligent Provisioning.....	6
F10/Remote console features.....	6
Always On Intelligent Provisioning	7
Intelligent Provisioning operation.....	7
Navigating Intelligent Provisioning	8
About HPE Rapid Setup Software.....	9
Software installed with Intelligent Provisioning.....	9
Accessing Intelligent Provisioning.....	10
Accessing Intelligent Provisioning from the iLO web interface	10
Accessing Intelligent Provisioning using an iLO remote console session.....	10
F10 mode options.....	11
Selecting F10 mode to use.....	11
Initial configuration in Intelligent Provisioning.....	11
Using the First Time Setup wizard.....	11
Entering First Time Wizard settings.....	11
Re-enabling Intelligent Provisioning.....	12
Reinstalling Intelligent Provisioning	12
Reinstalling from an ISO image.....	13
Reinstalling from an RPM package (Linux only).....	13
Initial configuration in HPE Rapid Setup Software.....	14
Configuring a RAID with HPE Rapid Setup Software overview.....	14
Creating an advanced RAID array manually.....	15
Using the HPE Rapid Setup Software main menu.....	15
About RAID arrays.....	17
RAID 0	17
RAID 1 and RAID 1+0 (RAID 10).....	18
RAID 5.....	19
RAID 50.....	19
RAID 6.....	20
RAID 60.....	21
Dedicated spare.....	22
Failure spare activation.....	22
Configuring the server and installing an operating system	23
Configuring the server and installing an OS with Intelligent Provisioning.....	23
Server support and special characters.....	23
Source media types and installation methods supported for each OS.....	23
Selecting hardware settings.....	23
Selecting the OS.....	26
Reviewing your settings.....	28
Checking installation parameters.....	28

Performing maintenance	29
Updating firmware	29
Determining the installed Intelligent Provisioning version.....	30
Setting Intelligent Provisioning Preferences	30
Downloading Active Health System data	31
Downloading an Active Health System log.....	31
Uploading an AHS log to AHSV.....	32
Using Deployment Settings	32
Creating a Deployment Settings package.....	33
Using Deployment Settings package to configure a single server.....	34
Deployment Settings package-level actions.....	35
Deployment Settings package individual settings.....	36
Version Information.....	36
Array Configuration settings.....	36
Entering operating system information.....	36
Entering ROM settings.....	37
Entering Intelligent Provisioning Preferences	37
Using the BIOS Configuration (RBSU) utility.....	38
About iLO Configuration.....	39
Running an iLO self-test.....	40
Management Settings.....	40
Configuring Manager iLO Management Settings.....	40
Configuring iLO Management Manager Network Service and Virtual Network Service Settings.....	41
Configuring iLO Management SNMP Settings.....	42
Network Interfaces.....	43
Configuring iLO Manager Dedicated Network Interface.....	43
Configuring iLO Manager Shared Network Interface.....	44
User Accounts.....	46
Configuring iLO Account Services.....	46
Editing User Account settings.....	46
Adding a user account.....	47
Resetting the iLO.....	47
Configuring Intelligent Storage.....	47
Creating a new array or logical drive.....	48
Configuring an array or logical drive.....	48
About Hardware Validation Tool.....	49
Using the hardware validation tool.....	49
Erasing server data.....	50
About erasing data in Intelligent Provisioning.....	50
Using One-button secure erase.....	51
Impacts to the system after One-button secure erase completes.....	52
One-button secure erase FAQ.....	54
Using System Erase and Reset.....	57
System Erase and Reset options.....	57
Creating a RAID configuration with HPE SSA.....	58
Using HPE Smart Storage Administrator (HPE SSA).....	58
HPE SSA features.....	58
Accessing HPE SSA.....	58
Diagnostics/SmartSSD.....	59
 Using the USB Key Utility	 60

Troubleshooting.....	62
Basic troubleshooting techniques.....	62
Troubleshooting general issues	62
iLO log on required during Intelligent Provisioning F10 boot.....	62
Intelligent Provisioning does not launch when F10 is pressed.....	62
Intelligent Provisioning PXE flashing doesn't re-image Always On Intelligent Provisioning.....	63
OS Host name field missing.....	63
Accessing version information in deployment settings.....	64
A browser does not import a deployment profile correctly.....	64
Some Legacy BIOS Mode installs need specific instructions.....	64
Always On Intelligent Provisioning does not display status of NICs.....	64
Cannot create a custom partition size.....	65
Intelligent Provisioning cannot launch One-Button secure erase.....	65
One-Button secure erase is unsuccessful or reports errors.....	66
One-Button secure erase succeeds but some drives are not erased.....	66
One-Button secure erase reports errors, but no specific details.....	67
Troubleshooting Windows-specific issues	67
Windows Essentials does not install from USB source.....	67
Windows does not install on AMD servers.....	68
Troubleshooting Linux-specific issues	68
Unable to proceed with Assisted installation of Red Hat Enterprise Linux 7.....	68
Assisted installation of Red Hat OS hangs.....	68
Troubleshooting VMware-specific issues	69
Server reboots during VMware Assisted installation.....	69
 Websites.....	 70
 Support and other resources.....	 71
Accessing Hewlett Packard Enterprise Support.....	71
Accessing updates.....	71
Customer self repair.....	72
Remote support.....	72
Warranty information.....	72
Regulatory information.....	73
Documentation feedback.....	73

Introduction



TIP: The information in this guide is for using Intelligent Provisioning with ProLiant Gen10 servers and HPE Synergy compute modules. It includes information on using Intelligent Provisioning and HPE Rapid Setup Software. For information on using Intelligent Provisioning with ProLiant Gen8 and Gen9 Servers, see the Intelligent Provisioning user guides available on the Information Library at (<http://www.hpe.com/info/intelligentprovisioning/docs>).

Intelligent Provisioning

Intelligent Provisioning is a single-server deployment tool embedded in ProLiant servers and HPE Synergy compute modules. Intelligent Provisioning simplifies server setup, providing a reliable and consistent way to deploy servers.

Intelligent Provisioning 3.30 and later includes HPE Rapid Setup Software. When you launch F10 mode from the POST screen, you are prompted to select whether you want to enter the Intelligent Provisioning or HPE Rapid Setup Software mode.

NOTE: After you have selected a mode, you must reprovision the server to change the mode that launches when you boot to F10.

Intelligent Provisioning prepares the system for installing original, licensed vendor media and Hewlett Packard Enterprise-branded versions of OS software. Intelligent Provisioning also prepares the system to integrate optimized server support software from the Service Pack for ProLiant (SPP). SPP is a comprehensive systems software and firmware solution for ProLiant servers, server blades, their enclosures, and HPE Synergy compute modules. These components are preloaded with a basic set of firmware and OS components that are installed along with Intelligent Provisioning.

! **IMPORTANT:** HPE ProLiant XL servers do not support operating system installation with Intelligent Provisioning, but they do support the maintenance features. For more information, see "Performing Maintenance" in the Intelligent Provisioning user guide and online help.

After the server is running, you can update the firmware to install additional components. You can also update any components that have been outdated since the server was manufactured.

To access Intelligent Provisioning:

- Press **F10** from the POST screen and enter either Intelligent Provisioning or HPE Rapid Setup Software.
- From the iLO web interface using **Always On**. **Always On** allows you to access Intelligent Provisioning without rebooting your server.

More information

[About HPE Rapid Setup Software on page 9](#)

F10/Remote console features

F10/Remote console allows you to:

- Access HPE Smart Storage Administrator for disk configuration.
- Perform a full set-up of Intelligent Provisioning.

F10/Remote console includes options that are not available in Always On Intelligent Provisioning.

Always On Intelligent Provisioning

Always On Intelligent Provisioning allows you to:

- Perform functions when the server is off.
- Perform tasks when running an operating system without powering off the server.

In the Always On Intelligent Provisioning version, the **Perform Maintenance** screen contains utilities that are not available in iLO. For more information, see the iLO user guide.

NOTE: To install an OS in Always On mode, extract the installation ISO on the FTP server.

Intelligent Provisioning operation

Intelligent Provisioning includes the following components:

- Critical boot drivers
- Active Health System (AHS)
- Erase Utility
- Deployment Settings

⚠ **IMPORTANT:**

- Although your server is preloaded with firmware and drivers, Hewlett Packard Enterprise recommends updating the firmware upon initial setup. Also, downloading and updating the latest version of Intelligent Provisioning ensures the latest supported features are available.
- 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 Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware ESXi/vSphere Custom Image
- ClearOS

Not all versions of an OS are supported. For information about specific versions of a supported operating system, see the OS Support Matrix on the Hewlett Packard Enterprise website (<http://www.hpe.com/info/ossupport>).

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
	Enables you to select the language to use.
	Returns to the Intelligent Provisioning home page, with the Express OS Install and Perform Maintenance menus. This icon is available only after completing the initial configuration and registration tasks.
	Displays the job configuration viewer screen, which displays the status of jobs in the queue. You can use this screen to monitor configuration tasks and jobs as they are processed.
	Opens the online help to the section about the current screen.
	Displays system information, including the Intelligent Provisioning version.
	Powers down or reboots the server.
	Logs the current user out of Intelligent Provisioning. NOTE: This icon is only displayed in Always On mode.
	Returns you to the previous screen after validating and saving your choices.
	Takes you forward to the next screen after validating and saving your choices.

About HPE Rapid Setup Software

HPE Rapid Setup Software is a simple, fast, and easy way to:

- Manage BIOS settings.
- Configure a RAID on your system.
- Install ClearOS from the Internet or USB.
- Install supported versions of Windows or VMware from USB or network share.
- Use Hardware Validation Tools.

NOTE: HPE Rapid Setup Software does not support installing a Red Hat or SUSE Linux operating system.

Software installed with Intelligent Provisioning

When a Windows system is installed using Intelligent Provisioning with Internet access, all the software applications are automatically downloaded and installed. On other operating systems or on a Windows system without Internet access, the following applications are not automatically installed with Intelligent Provisioning. To install the following applications, run SPP.

- ProLiant Agentless Management Service (AMS)
- Network Configuration Utility for Windows
- HPE Smart Storage Administrator (HPE SSA)
- Lights-Out Online Configuration Utility
- HPE Rapid Setup Software

Accessing Intelligent Provisioning

Accessing Intelligent Provisioning from the iLO web interface

Procedure

1. Open a browser and enter `https://<iLO host name or IP address>` to log in to the iLO web interface.
2. Enter a user account name and password, and click **Log In**.
3. Click **Intelligent Provisioning** in the navigation tree.
4. Click **Always On**.

The Intelligent Provisioning web interface opens in a new browser window.

Accessing Intelligent Provisioning using an iLO remote console session

Procedure

1. Open a browser and enter `https://<iLO host name or IP address>` to log in to the iLO web interface.
2. From the iLO web interface, navigate to the **Remote Console & Media** page.
3. Verify that your system meets the requirements for using the remote console application you want to use.
4. Click the launch button for your selected application.
Alternatively, you can click an Integrated Remote Console link on the **Information - iLO Overview** page.
5. Restart or power on the server.
The server restarts and the POST screen appears.
6. Press **F10** when prompted during the server POST.
7. Select **Intelligent Provisioning**.

When accessing Intelligent Provisioning, one of the following happens:

If you are using Intelligent Provisioning for the first time, the First Time Setup wizard will guide you through initial configuration and registration tasks. For more information, see [Using the First Time Setup wizard](#) on page 11.

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

F10 mode options

When you launch F10 mode from the POST screen, you are prompted to use Intelligent Provisioning or HPE Rapid Setup Software.

Both Intelligent Provisioning and HPE Rapid Setup Software offer tools to provision and maintain servers.

Intelligent Provisioning	HPE Rapid Setup Software
Provisioning multiple servers.	Provisioning one server at a time.
Configuring multiple RAID arrays.	Configuring RAID arrays.
Users who have servers provisioned and deployed.	Users provisioning new servers.

Selecting F10 mode to use

Procedure

1. Boot the server.
2. On the POST screen, press **F10**.
3. Select **Intelligent Provisioning** or **HPE Rapid Setup Software**.

Initial configuration in Intelligent Provisioning

Using the First Time Setup wizard

The first time Intelligent Provisioning runs on a server, the First Time Setup wizard guides you through selecting preferences for your system.

The first time you launch Intelligent Provisioning you get the option to select Intelligent Provisioning or the HPE Rapid Setup Software interface.

Entering First Time Wizard settings

If you don't want to use the First Time Wizard, click the **Skip** button.

Procedure

1. Enter the following, or select the defaults:
 - **Interface Language**
 - **Keyboard Language**
 - **Time Zone**
 - **Boot BIOS Mode**
 - **System Date**
 - **System Time**
 - **Choose network interface for updates and installs**

- **Use Proxy**
 - **DHCP Auto-Configuration**—Deselect this option to manually enter DHCP settings, including using IPv6 protocol.
 - **Accept EULA**
 - **Provide anonymous usage and error feedback to help improve this product**
2. Click **Next**.
 3. Read the EULA, and then select **Accept Intelligent Provisioning EULA**.
 4. Click **Next**.
 5. Enter the following information:
 - **Automatically optimize your server**

NOTE: Required fields differ if you do not select **Automatically optimize your server**.

 - **What will this server be used for?**
 - **Enable F10 functionality**

Provide anonymous usage and error feedback

 - **Enable automatic application of software and firmware updates to this system**
 6. Click **Next**.
 7. Enter the following information:
 - **Choose network interface for updates and installs**
 - **System Software Update**—The source where the server gets updates.
 8. To save the changes, click **Submit**.

Re-enabling Intelligent Provisioning

Procedure

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 then press **Enter**.
3. Select **Enabled**.

Reinstalling Intelligent Provisioning

NOTE: Changes to the HPE website and the firmware update process will cause firmware updates to time out for versions below 1.63 (for Gen8) and below 2.50 (for Gen9). The older web sites associated with hp.com have been retired and Intelligent Provisioning will be unable to find updates.

Older installations can be updated with the Intelligent Provisioning Recovery DVD.

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 an ISO image

Procedure

1. Download the ISO image file for the latest Intelligent Provisioning recovery media by clicking **Download** from the Intelligent Provisioning website (<http://www.hpe.com/info/intelligentprovisioning>).

NOTE: The following servers and Intelligent Provisioning versions are supported:

- Gen8 supports Intelligent Provisioning 1.x.
 - Gen9 supports Intelligent Provisioning 2.x.
 - Gen10 supports Intelligent Provisioning 3.x.
-
2. To download the ISO image file, complete the onscreen instructions.
 3. Mount the ISO file in one of the following ways:
 - Using iLO virtual media.
 - Burn the Intelligent Provisioning recovery media ISO file to a DVD and place it in the CD/DVD drive of the server.
 4. To power up the server Press ON.
 5. To display the boot menu, press **F11** during server POST.
 6. Press **1** on the keyboard to boot from the CD/DVD.
 7. To update or reinstall Intelligent Provisioning, select the interactive method. The server continues booting from the Intelligent Provisioning recovery media.
 8. Select Reinstall Intelligent Provisioning when the window opens.
 9. Reboot the server when the installation is complete by pressing **F10**.

Reinstalling from an RPM package (Linux only)

Procedure

1. Download the RPM package file for the latest Intelligent Provisioning recovery RPM package from the SDR website (<https://downloads.linux.hpe.com/SDR/ipo/>).

2. Execute the command:

```
rpm -i firmware-intelligentprovisioning-<version>.x86_64.rpm
```

3. Execute the command:

```
cd /usr/lib/x86_64-linux-gnu/firmware-intelligentprovisioning-ip-<version>/
```

4. Execute the command:

```
#!/setup
```

5. Execute the command:

```
#reboot
```

Example

As an alternative to steps 2-4:

1. Execute the command:

```
export FIRMWARE_FLASH_NOW=1
```

2. Execute the command:

```
rpm -i firmware-intelligentprovisioning-ip-<version>.x86_64.rpm
```

Initial configuration in HPE Rapid Setup Software

Configuring a RAID with HPE Rapid Setup Software overview

When you boot the server and enter F10 mode, HPE Rapid Setup Software allows you to configure a RAID, select an OS installation target, or install an OS.

Procedure

1. Power on the server, and then select **F10** from the POST screen.
2. Select HPE Rapid Setup Software.
3. If prompted, read and accept the EULA to continue.
4. Select one of these options to view more information about the task:
 - **Setup RAID:** If you want to set up a RAID, select this option. Creating a RAID erases all data off connected drives.
 - **Select OS Target:** Select the target drive where you want to install an OS.
 - **Install OS:** Allows you to skip creating a RAID and selecting an OS target.
5. Click **Continue**.
6. HPE Rapid Setup Software displays the network information on the **Update Web Proxy Settings screen**. If the environment requires a web proxy, select **Yes**, and then enter the web proxy settings.
7. Click **Continue**.

The software scans your system for RAID array information and hardware and provides a recommended RAID configuration.

8. Select whether you want to split the RAID across multiple drives. By default, HPE Rapid Setup Software creates a single RAID volume from all installed drives.

NOTE: This option is only available if your system meets requirements.

Splitting the RAID across the drives uses two drives as a mirrored set, and the remaining drives for a second RAID volume.

9. Select one of the following:
 - Click **Continue** to use the recommendation RAID configuration.

NOTE: You can only continue to the next step if HPE Rapid Setup Software detects a valid hardware configuration.

- Click **Manually Configure** to configure the RAID. For more information, see [Creating an advanced RAID array manually](#).

Creating an advanced RAID array manually

You can use these steps to create multiple RAID arrays.

Procedure

1. From the main page of Intelligent Storage Configuration screen, click **+ Create Array**.
2. Select the drives you want to include in the RAID array, and select the drive usage. If you want a spare drive, select it here.
3. Click **Next**.
4. Enter a **Logical Name**.
5. Select a **RAID Mode**. For example, RAID 1 or RAID 5.
6. (Optional) Select a stripe size.
7. Select an **Accelerator**. For example, cache.
8. (Optional) Select a **RAID size**.
9. Select a **Spare Rebuild Mode**.
10. Click **Submit**.
11. Reboot the system.

More information

[About RAID arrays](#) on page 17

Using the HPE Rapid Setup Software main menu

After the RAID configuration options, the HPE Rapid Setup Software takes you to the main menu. On this screen, you can:

- Configure BIOS/RBSU settings, for example:
 - System Options
 - Processor Options
 - Memory Options
 - Virtualization Options
 - Boot Options
 - Network Options
 - Storage options
 - Power and performance options

- Embedded UEFI shell
- Server Security
- PCIe device configuration
- Advanced options
- Date and Time
- System default options
- Language settings
- Configure RAID settings.
- Perform hardware validation tests.
- Install a supported operating system.

More information

[About Hardware Validation Tool](#) on page 49

[Configuring the server and installing an OS with Intelligent Provisioning](#) on page 23

[Using the BIOS Configuration \(RBSU\) utility](#) on page 38

Installing an operating system with HPE Rapid Setup Software

HPE Rapid Setup Software allows you to install the supported versions of Windows, ClearOS, and VMware. If you want to install a Linux operating system that is supported on your server, use Intelligent Provisioning to install the operating system.

Prerequisites

- HPE Rapid Setup Software supports installing ClearOS from a USB key or the Internet.
- HPE Rapid Setup Software supports installing supported Windows or VMware operating system from a USB key or network location.
- When installing from a USB key, plug the media into the server.
- When installing from a network drive, make sure that the files are available.
- Complete the RAID setup instructions. For more information, see [Configuring a RAID with HPE Rapid Setup Software overview](#).

NOTE: If HPE Rapid Setup Software displays a message that firmware updates are available, you can click **Go** to view the available updates. When you install the OS, HPE Rapid Setup Software also updates the firmware.

Procedure

1. From the main menu, select the operating system that you want to install.
2. Select the network location where the operating system files are saved, or navigate to the operating system installation files.
3. Follow the onscreen prompts.

NOTE: Hewlett Packard Enterprise recommends updating firmware, software, and drivers after installing an operating system.

Once all HPE Rapid Setup Software settings are recorded, the software reboots the server. The software might reboot the server multiple times as it applies the configuration settings. After the OS is installed, you can configure the OS.

More information

[Updating firmware on page 29](#)

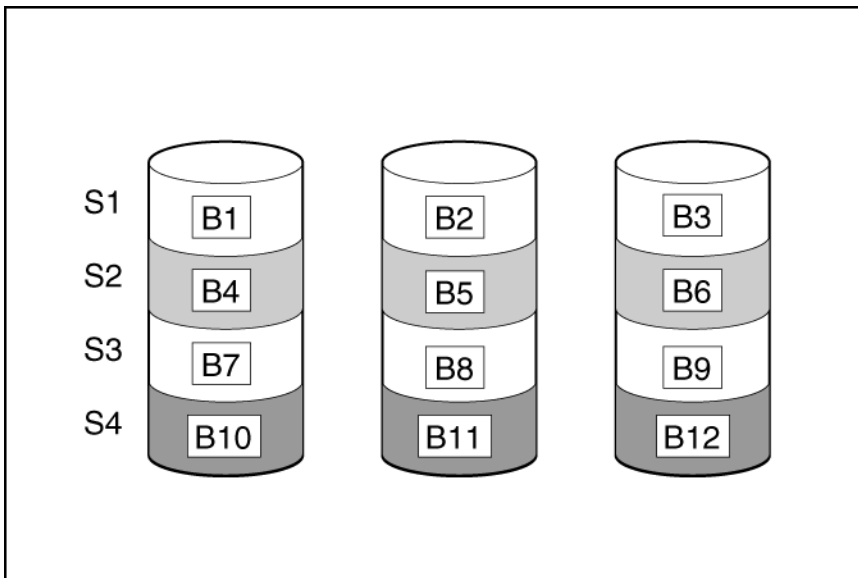
[Configuring a RAID with HPE Rapid Setup Software overview on page 14](#)

About RAID arrays

RAID arrays can help increase system performance and reduce the risk of drive failure. You can create RAID arrays with drives with different specifications, but performance will be based on the smallest drive or lowest speed. For example, if you create an array with a 1 TB drive and a 2 TB drive, then the array can store a maximum 1 TB of data. The extra storage on the larger drive is not available until you reformat the drive.

RAID 0

A RAID 0 configuration provides data striping, but there is no protection against data loss when a drive fails. However, it is useful for rapid storage of large amounts of noncritical data (for printing or image editing, for example) or when cost is the most important consideration. The minimum number of drives required is one.



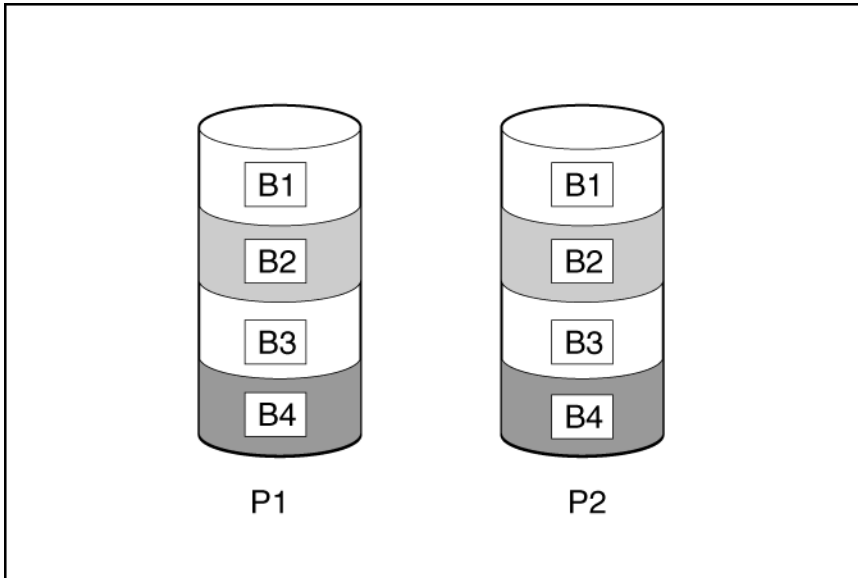
This method has the following benefits:

- Useful when performance and low cost are more important than data protection.
- Has the highest write performance of all RAID methods.
- Has the lowest cost per unit of stored data of all RAID methods.
- All drive capacity is used to store data (none allocated for fault tolerance).

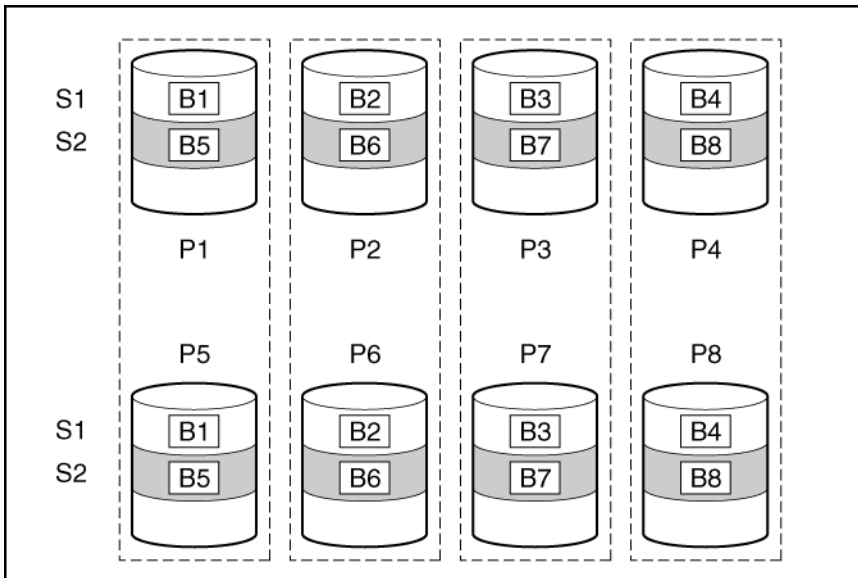
RAID 1 and RAID 1+0 (RAID 10)

In RAID 1 and RAID 1+0 (RAID 10) configurations, data is duplicated to a second drive. The usable capacity is $C \times (n / 2)$ where C is the drive capacity with n drives in the array. A minimum of two drives is required.

When the array contains only two physical drives, the fault-tolerance method is known as RAID 1.



When the array has more than two physical drives, drives are mirrored in pairs, and the fault-tolerance method is known as RAID 1+0 or RAID 10. If a physical drive fails, the remaining drive in the mirrored pair can still provide all the necessary data. Several drives in the array can fail without incurring data loss, as long as no two failed drives belong to the same mirrored pair. The total drive count must increment by 2 drives. A minimum of four drives is required.



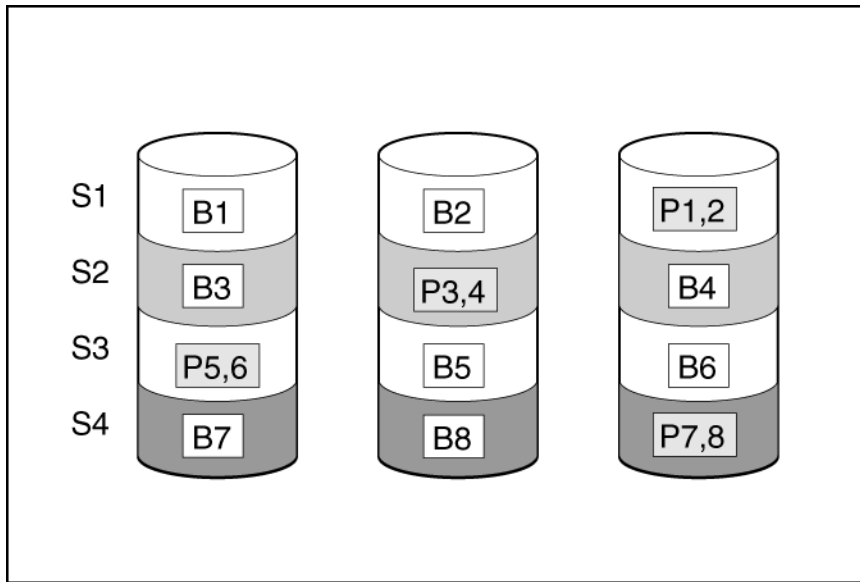
This method has the following benefits:

- It is useful when high performance and data protection are more important than usable capacity.
- This method has the highest write performance of any fault-tolerant configuration.

- No data is lost when a drive fails, as long as no failed drive is mirrored to another failed drive.
- Up to half of the physical drives in the array can fail.

RAID 5

RAID 5 protects data using parity (denoted by $P_{x,y}$ in the figure). Parity data is calculated by summing (XOR) the data from each drive within the stripe. The strips of parity data are distributed evenly over every physical drive within the logical drive. When a physical drive fails, data that was on the failed drive can be recovered from the remaining parity data and user data on the other drives in the array. The usable capacity is $C \times (n - 1)$ where C is the drive capacity with n drives in the array. A minimum of three drives is required.

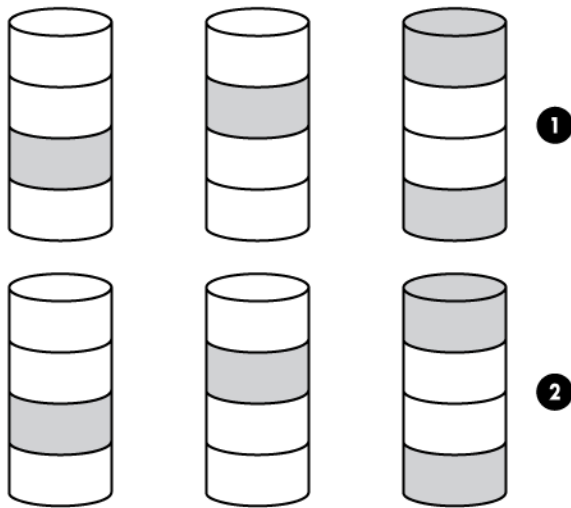


This method has the following benefits:

- It is useful when usable capacity, write performance, and data protection are equally important.
- It has the highest usable capacity of any fault-tolerant configuration.
- Data is not lost if one physical drive fails.

RAID 50

RAID 50 is a nested RAID method in which the constituent drives are organized into several identical RAID 5 logical drive sets (parity groups). The smallest possible RAID 50 configuration has six drives organized into two parity groups of three drives each.



For any given number of drives, data loss is least likely to occur when the drives are arranged into the configuration that has the largest possible number of parity groups. For example, four parity groups of three drives are more secure than three parity groups of four drives. However, less data can be stored on the array with the larger number of parity groups.

All data is lost if a second drive fails in the same parity group before data from the first failed drive has finished rebuilding. A greater percentage of array capacity is used to store redundant or parity data than with non-nested RAID methods (RAID 5, for example). A minimum of six drives is required.

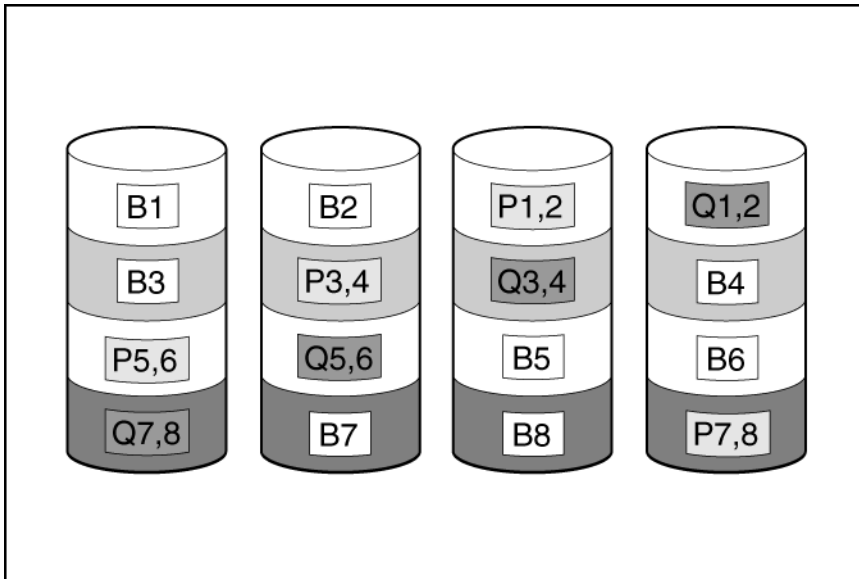
This method has the following benefits:

- Higher performance than for RAID 5, especially during writes.
- Better fault tolerance than either RAID 0 or RAID 5.
- Up to n physical drives can fail (where n is the number of parity groups) without loss of data, as long as the failed drives are in different parity groups.

RAID 6

RAID 6 protects data using double parity. With RAID 6, two different sets of parity data are used (denoted by $P_{x,y}$ and $Q_{x,y}$ in the figure), allowing data to still be preserved if two drives fail. Each set of parity data uses a capacity equivalent to that of one of the constituent drives. The usable capacity is $C \times (n - 2)$ where C is the drive capacity with n drives in the array.

A minimum of 4 drives is required.



This method is most useful when data loss is unacceptable but cost is also an important factor. The probability that data loss will occur when an array is configured with RAID 6 (Advanced Data Guarding (ADG)) is less than it would be if it were configured with RAID 5.

This method has the following benefits:

- It is useful when data protection and usable capacity are more important than write performance.
- It allows any two drives to fail without loss of data.

RAID 60

RAID 60 is a nested RAID method in which the constituent drives are organized into several identical RAID 6 logical drive sets (parity groups). The smallest possible RAID 60 configuration has eight drives organized into two parity groups of four drives each.

For any given number of hard drives, data loss is least likely to occur when the drives are arranged into the configuration that has the largest possible number of parity groups. For example, five parity groups of four drives are more secure than four parity groups of five drives. However, less data can be stored on the array with the larger number of parity groups.

The number of physical drives must be exactly divisible by the number of parity groups. Therefore, the number of parity groups that you can specify is restricted by the number of physical drives. The maximum number of parity groups possible for a particular number of physical drives is the total number of drives divided by the minimum number of drives necessary for that RAID level (three for RAID 50, 4 for RAID 60).

A minimum of 8 drives is required.

All data is lost if a third drive in a parity group fails before one of the other failed drives in the parity group has finished rebuilding. A greater percentage of array capacity is used to store redundant or parity data than with non-nested RAID methods.

This method has the following benefits:

- Higher performance than for RAID 6, especially during writes.
- Better fault tolerance than RAID 0, 5, 50, or 6.
- Up to $2n$ physical drives can fail (where n is the number of parity groups) without loss of data, as long as no more than two failed drives are in the same parity group.

Dedicated spare

The dedicated spare drive activates any time a drive within the array fails.

Failure spare activation

Failure spare activation mode activates a spare drive when a member drive within an array fails using fault tolerance methods to regenerate the data.

Assigning one or more online spare drives to an array enables you to postpone replacement of faulty drives.

Configuring the server and installing an operating system

Follow the instructions to configure the hardware and install an OS on your server.

Configuring the server and installing an OS with Intelligent Provisioning

Follow the onscreen prompts in the Intelligent Provisioning **Express OS Install** menu to complete the following tasks:

Procedure

1. [Selecting hardware settings](#) on page 23
2. [Selecting the OS](#) on page 26
3. [Reviewing your settings](#) on page 28

More information

[Using the HPE Rapid Setup Software main menu](#) on page 15

Server support and special characters

- ProLiant XL Servers do not support operating system installations with Intelligent Provisioning. These servers do support the maintenance features described in [Performing maintenance](#) on page 29, except deploying the operating systems installations.
- You can only use special characters in passwords. Do not use special characters in any other data fields. Special characters, punctuation, and spaces are not supported in any pathname.

Source media types and installation methods supported for each OS

Each Express OS Install screen provides a guided method for configuring the server, installing an OS, and updating the system software.

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

For more information about source media and installation methods supported by each OS, see the *Intelligent Provisioning Release Notes*.

Selecting hardware settings

Procedure

1. Select **Express OS Install** on the Intelligent Provisioning home screen.
The Operating System Installation screen appears.
2. Select a **RAID Configuration** option.

- **Recommended settings**—HPE SSA polls any drives that are present, and builds an appropriate array for those drives. Hewlett Packard Enterprise recommends selecting this option when initially provisioning a server.

⚠ CAUTION: Selecting this option 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*.

- **Keep current settings**—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: Intelligent Provisioning does not support SAN volumes.


⚠ CAUTION: In Legacy BIOS mode, drives that are 2.2 TB or larger will not be detected during OS installation.

- If you want to use Legacy BIOS mode, use HPE SSA to create a logical drive to boot with less than 2.2 TB. To access HPE SSA, select **RAID Configuration** from the Intelligent Provisioning Perform Maintenance home screen.
- If you want to use logical drives of 2.2 TB capacity or more for OS installation, use UEFI mode instead. See the *UEFI System Utilities User Guide* for more information.

3. Select a **Controller** from the list. Controller selections are based on your operating environment.
4. Select a **Disk** from the list. Disk selections are based on your operating environment.
5. Select an **Install Source** from the list. The options and the required information and action for each are described in the following table.

Media type	Required information/action
DVD-ROM Media	Insert the DVD.
File on a USB drive	Insert the USB drive and browse to the location of the OS installation files on the USB drive. Then, double-click the ISO file. NOTE: Only FAT or exFAT-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.

Table Continued

Media type	Required information/action
SMB/CIFS (Windows Share)	<p>Enter network connection information, including:</p> <ul style="list-style-type: none"> • 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 (not encrypted)—Password for the user name used to access the network share.
An anonymous FTP server	<p>Enter network connection information, including:</p> <p>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.</p> <hr/> <p> IMPORTANT: When entering an FTP path, remove spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).</p>

6. Select whether to do a **Firmware Update**.

- **Skip Update**—Default. No firmware updates are performed before the OS installation.
- **Update before OS Install**—Firmware updates available according to the baseline defined in the latest SPP are done before OS installation.

7. Select an **Install Method**.

NOTE: If using Always On (Intelligent Provisioning accessed from the iLO web interface), only the Assisted Install option is listed.

- **Assisted Install**—An 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.

NOTE: The ProLiant iLO 5 Channel Interface Driver is installed automatically if you use the Intelligent Provisioning Assisted Install method for Windows installation. The ProLiant iLO 5 Channel Interface Driver is standard for SUSE Linux Enterprise Server, Red Hat Enterprise Linux, and ClearOS.

- **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. Intelligent Provisioning partitions storage based on OS recommendations.
-

NOTE: The Legacy BIOS boot order cannot be changed by pressing **F10**. If doing an assisted or a manual install in Legacy BIOS mode, you must ensure that:

- On Windows system:
 - Manual install: The system only boots to a DVD.
 - Assisted install: The system boots to a hard drive.
- On Linux/VMware, the system boots to the hard drive.

Do this by changing the boot order or by pressing **F11** to choose at boot.

8. To proceed to **Selecting the OS**, click the **Continue** right arrow.
-

- ⓘ **IMPORTANT:** If an unsupported media device is selected, you will not be able to continue to the next screen. To resolve the issue, remove the unsupported media device, and make sure that you have a supported install source when prompted.
-

Selecting the OS

You can use Always On Intelligent Provisioning mode supports installing an OS from:

- FTP server
- SMB/CIFS (Windows share)
- Virtual media source
 - Local ISO
 - URL
- Install Clear OS from the Internet

Prerequisites

To install an OS in Always On mode from an FTP server, extract the installation ISO. An ISO that is not extracted it too large to install from an FTP source.

Procedure

1. Select an operating system or choose the default. OS Language, OS Keyboard, and Time Zone are automatically filtered.

Supported OS families include:

- Microsoft Windows

NOTE: Microsoft Windows Essentials are supported from an ISO only, not a USB or network source.

- VMware vSphere Custom Image
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux
- ClearOS

NOTE: Certain ProLiant servers require an HPE Customized image for a successful VMware ESXi installation. For more information or to download an image, see the Hewlett Packard Enterprise website at <http://www.hpe.com/info/esxidownload>.

2. Enter information into the following fields (automatically selected in manual installations):

- Organization Name
- Owner Name
- Optional Password
- Confirm Password

NOTE: When creating passwords, refer to the operating system documentation for password requirements. Requirements might include:

- Minimum password length
- Maximum password length
- Upper case letters
- Lower case letters
- Punctuation marks !@#\$%^&* _.
- Special characters

NOTE: Windows Linux only support using the underscore _ special character.

If you do not provide a password, Windows prompts for a password on first boot. Linux and VMware ESXi 6.5 and earlier use the default password **password**. VMware ESXi 6.5U and later use the password **Passw0rd_**.

- a. For manual installations, select the operating system again after entering the product key.
3. Enter Hyper-V role for the system.
 4. Enable Windows Firewall.
 5. To proceed to **Reviewing your settings**, click the **Continue** right arrow.

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.
-

Procedure

1. Review and confirm your deployment settings.
2. 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.

Checking installation parameters

During the installation and configuration process, consider the following:

- A EULA might be displayed.
- The **Firmware Update** screen might be displayed at this time, depending on the following two system settings:
 - In the **Preferences** screen, **System Software Update** must have been enabled. See **Setting preferences** for more information.
 - In the **Operating System Installation** screen, **Update before OS Install** must have been selected. See **Selecting hardware settings** for more information.

If the **Firmware Update** screen is displayed, follow the onscreen 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. After POST completes, 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.

Performing maintenance

NOTE: The following maintenance tasks are not supported on an HPE Synergy compute module:

- Downloading Active Health System data
- Updating firmware
- Using iLO Configuration Utility

To perform these tasks on an HPE Synergy compute module, you must use HPE OneView.

Updating firmware

HPE servers and their installed hardware options are preloaded with the latest firmware. However, updated firmware might be available. You can use Intelligent Provisioning to find and deploy available updates.

- For ProLiant servers, use the Intelligent Provisioning Firmware Update utility to find and apply the latest firmware.
- For HPE Synergy compute modules, use HPE OneView to update the firmware. Intelligent Provisioning updates can be performed when an SPP update is available.

NOTE: The Intelligent Provisioning Firmware Update utility reflects the latest updates available in the baseline defined in the latest SPP. Updates that are not in the SPP baseline do not appear on the updates list.

You can use the Firmware Update utility to roll back to older versions of components.

Prerequisites

To update firmware, make sure that port 443 is open for SSL communication.

Procedure

1. Boot the system, and then press **F10** at the POST screen.
2. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
3. Select **Firmware Update** from the maintenance options.

The system searches for firmware on the source configured in the System Software Update settings. This process might take a few minutes; wait for the display to generate the results. If no new firmware is available, the current version is displayed in the Firmware Update screen.

NOTE: Alternatively, you can 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 *Service Pack for ProLiant Quick Start Guide* on the website (http://www.hpe.com/support/SPP_UG_en).

4. Select one of the following:

- **Newest firmware available**


Updates create versions that you can use to undo an update.

- **Rollback to previous**

NOTE: This feature allows you to return to a previous firmware version. You can choose specific firmware versions you can roll back.

5. Select the items to update, and then click **Submit**.
6. The **Job Configuration Viewer** screen displays the selected items.
7. Do one of the following:
 - **Launch Now**
 - **Add another job**
8. Click **Reboot** at the completion of the firmware update process.

Determining the installed Intelligent Provisioning version

To check the Intelligent Provisioning version, click the **System Information**  **Intelligent Provisioning Image** version is listed.

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.

Procedure

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Intelligent Provisioning Preferences** from the maintenance options.
3. Select settings for the following options:
 - **Interface Language**
 - **Keyboard Language**
 - **Boot BIOS Mode**
 - **System Software Update**—Select a source updates.
 - **Time Zone**
 - **System Date**
 - **System Time**
 - **Choose network interface for updates and installs**
 - **Use Proxy**, and provide proxy details.
 - **DHCP Auto-Configuration**, and provide the configuration details.

- **Accept EULA**, or click **Read EULA**.
- **Provide anonymous usage and error feedback to help improve this product. No personal data is collected and it will not be shared with third parties.**

4. Click **Submit**.

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 on this screen, see **Using the First Time Setup wizard**.

Downloading Active Health System data

HPE Support uses the Active Health System (AHS) log file for problem resolution.

Use the **Active Health System Log** screen to download AHS telemetry data from the server onto a USB key in the form of an AHS log file case number or a default string with an `.ahs` extension. 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.

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

The high level steps for submitting a case are:

Procedure

1. Download an AHS Log from the server experiencing a support issue. See **Downloading an Active Health System log**.
2. Upload the AHS Log to the Active Health System Viewer at <http://www.hpe.com/servers/AHSV>. See **Uploading an AHS log to AHSV**.
3. Review the Fault Detection Analytics for any self-repair actions/recommendations. See the *AHSV User Guide* for more information.
4. Create a support case using the AHSV Navigation menu. See the *AHSV User Guide* for more information.

Downloading an Active Health System log

Procedure

1. Insert a USB key into the server.
2. To go directly to Intelligent Provisioning, press the **F10** during the boot.
3. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
4. From the maintenance options, select **Active Health System Log** from the maintenance options.
The Active Health System Log screen appears.
5. Enter a start date and an end date, and then click **Download logs**.
6. Select the USB key from the **Removable Device to Save Log to** list.
7. Define the period for which to retrieve data by selecting the **From** and **To** dates. Hewlett Packard Enterprise recommends retrieving seven days of data, which creates a 10 MB to 15 MB file.

8. If there is an associated **HPE Support Case Number**, enter it. You can also enter a **Contact Name** and **email** address. The contact information helps HPE Support assist with the issue.
9. Click **Download Logs** to save the data to the USB key.

NOTE: Do not remove the USB key until the download has completed and the media lights clear.


Once the data has been downloaded, upload it to the Active Health System Viewer at <http://www.hpe.com/servers/AHSV>.

Uploading an AHS log to AHSV

The maximum file size limit is 250 MB. For logs that are larger than 250 MB, contact the HPE Support Center for assistance.

Perform this task in AHSV.

Prerequisites


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

- Buy more licenses.
- Find partner for license purchase.
- Contact HPE Support.

Procedure

1. Select **Upload AHS Log**.
2. Navigate to your log file, and then click **Open**.

A window is displayed that shows parsing and log loading states. As the AHS log loads, the screen displays the estimated time of completion.

 **TIP:** This window also displays videos for different platforms. You can search and play different videos while you are waiting for the log file to load.

To cancel the load process, click **Cancel**

Using Deployment Settings

The Intelligent Provisioning **Deployment Settings** page enables you to create server configuration packages. You can deploy the packages using a USB key or iLO Scripting to one or more ProLiant servers or HPE Synergy compute modules. Using **Deployment Settings** is an alternative to using the Scripting Toolkit or iLO RESTful Interface Tool.

For more information about iLO RESTful Interface Tool, see <http://www.hpe.com/info/resttool>.

NOTE: Some browsers do not import Deployment Profiles correctly. Use the extension `.txt` to ensure browser compatibility.

Procedure

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

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

More information

[About Hardware Validation Tool](#) on page 49

[Creating a Deployment Settings package](#) on page 33

Creating a Deployment Settings package

Procedure

1. On the Deployment Settings screen, do one of the following:
 - a. Create a profile based on an existing profile. Import the existing profile, click **Import** and use one of the following options:
 - **From Network Share** enter:
 - **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.
 - **Domain Name**—Name of the domain that hosts the network share.
 - **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.
 - **From USB Drive**—Insert the USB key containing the deployment:
 - I. Save the deployment from the USB key to the local server.
 - II. On the Select a Deployment screen, select the deployment from the list, and click **Deploy**. If the USB key and their stored deployments are not displayed, click **Rescan**.
Specify a file path, and then go to Step 8.
 - b. Create a new, custom profile, click **Create New Deployment**, and navigate the deployment settings screens to complete the settings in the following steps.
2. Enter a **Deployment Name**—Enter a name for this deployment package. Do not include spaces.
3. Enter the **Version Information**—Enter **User Notes** and **Captured From** details, and click **Done**. See [Entering version information](#).
4. Enter an **Operating System**—Do one of the following:

- To leave the OS details as shown, click **Done**.
 - To add an operating system, click **Edit**. On the Operating System Installation screen, select an **Install Source**, complete the fields required on the resulting screens, and click **Done**. See [Entering operating system information](#).
5. Enter the **ROM Settings**—Do one of the following:
 - To leave the ROM configuration as shown, click **Done**.
 - To edit ROM settings, click **Edit**. On the RBSU Profile Editing screen, complete your edits, and click **Done**. See [Entering ROM settings](#).
 6. Enter the **Array Configuration**—Review or select new settings. See Entering array configuration settings.
 7. Enter **Intelligent Provisioning Preferences**—See [Setting Intelligent Provisioning Preferences](#).
 8. Click **Save**. When prompted, enter a name and navigate to a network share or a USB key to save the Deployment Settings.

Using 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.
-

Procedure

1. Do one of the following:
 - a. To use the deployment you created on the server, click **Deploy**.
 - b. To use a previously created deployment:

Select **Deployment Settings > Import**.

 - **From Network Share** enter:
 - **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.
 - **Domain Name**—Name of the domain that hosts the network share.
 - **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.
 - **From USB Drive**—Insert the USB key containing the deployment:

- I. Save the deployment from the USB key to the local server.
- II. On the Select a Deployment screen, 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
- Hardware Validation Tool

Deployment Settings package-level actions

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

After making a selection on the initial page, the Select a Deployment screen opens.

On the Select a Deployment screen, 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 screen. If a USB drive is installed, its name is displayed near the top of the screen 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.





Icon	Description
	Click the Deploy icon to launch the automatic configuration utility.
	Click the Edit icon to change the following options: <ul style="list-style-type: none"> • Version Information • Operating System parameters • Intelligent Provisioning Preferences • Array Configuration information • ROM Settings

Table Continued

Icon	Description
	Click the Delete icon to delete the selected deployment.
	Click Download to download the performance package to a network share or a USB drive.

Deployment Settings package individual settings

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.

Select from one of the following deployment options:

- Create New Deployment. See the following topics:
 - [Version Information](#)
 - [Entering operating system information](#)
 - [Entering Intelligent Provisioning Preferences](#)
 - [Array Configuration settings](#)
 - [Entering ROM settings](#)
 - [About Hardware Validation Tool](#)
- Importing through Always On Intelligent Provisioning has two options:
 - Select **Choose File**, and then browse to the import file.
 - Drag and drop the import file into the browser.

Version Information

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

Array Configuration settings

Selecting the Array Configuration button takes you to the Configuring Intelligent Storage page. For more information, see [Configuring Intelligent Storage](#).

Entering operating system information

Use the **Operating System** screens to enter OS information and installation settings. The included fields match the Assisted installation method.

- ❗ **IMPORTANT:** The operating system settings you apply are sent to iLO, and the system reboots. Disc drives that you previously deployed might be erased.

Procedure

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.
 - a. 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.
 - b. For an FTP site, enter:
 - **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, do not include spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).
 - Windows and SLES FTP installation, and RHEL network share installation are not supported.
-

- c. For ClearOS, click **Install ClearOS from the Internet**.

The system automatically pulls the ISO from the specified location to install it.

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. Click **Deploy**, and verify that you are ready to create the OS.
7. Click **Apply** to install the OS.

Entering ROM settings

For information on ROM settings, see [Using the BIOS Configuration \(RBSU\) utility](#).

Entering Intelligent Provisioning Preferences

To enter basic system settings, click **Create New Deployment > Intelligent Provisioning Preferences > Edit**.

Procedure

1. Select the user interface and keyboard language.
2. Enter Boot BIOS Mode.
3. Select a System Software Update option:
 - Update from HPE website
 - Update From Custom URL
4. Select Time Zone, System Date, and System Time.
5. Choose your network interface for updates and installs.
6. In the Choose network interface for updates and installs section, choose the following based on your setup:
 - **Use Proxy**—Configures a network proxy for use with features that communicate across the network. Enter a proxy address and port.
 - **DHCP Auto-Configuration**—(Recommended) DHCP automatically assigns IP addresses to your server.

NOTE: DHCP auto-configuration does not support IPv6 networks.

 - **IPv4/IPv6**—Works as a mask field for the IP address.
7. Accept the Intelligent Provisioning EULA.
8. Click **Update**.

Using the BIOS Configuration (RBSU) utility

The BIOS configuration page allows you to change some system configurations from Intelligent Provisioning. The options available differ based on the system components. For a description of RBSU options, see the *UEFI System Utilities User Guide* at <https://www.hpe.com/info/uefi/docs>.

For example, you can update:

- Jitter Smoothing
- Workload Matching
- Core Boosting
- Workload profiles
- Boot options
- Storage options
- Network options
- Virtualization options

NOTE: If a lock icon is shown next to a BIOS option, you cannot change that option. The option might be restricted to the F9 screen, or you might have to change another setting, for example the Workload Profile.

NOTE: Intelligent Provisioning does not support the HPE Smart Array P824i-p MR Gen10 controller.

Procedure

1. Select **BIOS configuration (RBSU)** from the maintenance options. The BIOS configuration (RBSU) screen displays the following information:
 - ROM version
 - If a pending update follows valid RBSU dependency rules
 - Number of pending changes
 - Number of items changes automatically due to dependency rules
 - Resetting the BIOS
 - Workload profile
2. To reset the BIOS for this server, click **Reset BIOS**.
3. To update the workload profile, click **Workload Profile**.
4. To change RBSU configurations, select from the menu on the left, and then select the section that contains the configuration you want to change.
5. To save changes, click **Update**.
6. To return to the Perform Maintenance home screen, click the **Previous** left arrow.

About iLO Configuration

The iLO Configuration screen provides the following options for configuring iLO:

- Summary: Provides a summary of the iLO configuration.
- iLO Self-Test: Displays items tested during the self test.
- Management Settings
 - Manager
 - Manager Network services
 - SNMP Service
- Network Interfaces
 - Manager Dedicated Network Interface
 - Manager Shared Network Interface
 - Manage Virtual Network Interface
- User Accounts

- Account Service
- Administer User Accounts
- Add User Account
- Reset Options

Running an iLO self-test

Running an iLO self-test checks the status of certain server hardware components.

Procedure

1. On the iLO Configuration Utility screen, click **iLO Self-Test**.

The self-tests are run, and the results screen appears.

- Tests that ran successfully are followed by a green checkmark.
- Tests that failed are followed by a red "X".

For more information about iLO self-tests and about how to interpret and troubleshoot the results, see the *HPE iLO 5 User Guide*.

Management Settings

Configuring Manager iLO Management Settings

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > Management Settings > Manager**.

2. Configure the following settings:

- IPv6 Multicast Scope
- Multicast Announcement Interval
- Multicast Discovery
- Multicast Time to Live
- iLO Federation Management
- Trusted Certificate Required
- Mass Storage Authentication Required
- USB Ethernet Adapters Enabled
- USB Flash Drive Enabled
- iLO Service Port Enabled
- Video Presence Detect Enabled
- Clear Rest API Status

- Configuration Settings
- Idle Connection Timeout Minutes
- RIBCL Enabled
- Persistent Mouse Keyboard Enabled
- Required Login for iLO RBSU
- Serial CLI Speed
- Serial CLI status
- Enabled Auth Required
- VSP DI Logging Enabled
- Web GUI Enabled
- iLO RBSU Enabled
- VSP Log Download Enabled
- iLO Functionality Required
- iLO Functionality Enabled
- Video presence Detect Override Supported
- Video presence detect override
- Physical Monitor health Status Enabled
- Remote Console Thumbnail enabled
- iLO IP during Post Enabled
- Command Shell Max Concurrent Sessions

3. Click **Save Settings** to save the changes.

Configuring iLO Management Manager Network Service and Virtual Network Service Settings

Enable this feature and provide the information to send the network manager alerts.

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > Management Settings > Manager Network Services**.
2. Configure the following settings:
 - Alert Mail Email
 - Alert Mail Enabled
 - Alert Mail SMTP Port
 - Alert Mail SMTP Server
 - Alert Mail Sender Domain

- Configuration Settings
- Federation Enabled
- Remote Syslog Enabled
- Virtual Serial Port Log
- Federation Supported
- Remote Syslog Port
- SNMP Trap Port
- Serial of Lan Logging
- XML Response Enabled
- Port and Protocol Enabled for:
 - HTTP
 - HTTPS
 - IPMI
 - KVMIP
 - SNMP
 - SSH
 - Virtual Media
- SSDP
 - Notify IPV6 Scope
 - Notify Multicast Interval Seconds
 - Notify TTL
 - Port
 - Protocol Enabled
- FQDN
- Host Name

3. Click **Save Settings** to save the changes.

Configuring iLO Management SNMP Settings

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > Management Settings > SNMP**.
2. Configure the following settings:

- Alerts Enabled
- Alert Destination Contacts
- Periodic HSA Trap Config
- Location: Physical location of the server
- Read Communities: You can set up to 3 read-only communities.
- Role: Definition of the server role or function.
- Role Detail: Describes the tasks the server might perform.
- SNMPv3 Engine ID: The unique SNMP ID for this server.
- SNMPv3 Inform Retry Attempt: Number of SNMP retries to perform.
- SMPv3 Inform Retry Interval Seconds
- SNMP Trap Communities: You can provide up to eight trap community strings.
- Trap Source Hostname: The hostname that is used when SNMP traps are generated.
- Users: Create up to eight user profiles for SNMPv3 USM parameters.
- SNMP Cold Start Trap Broadcast

3. Click **Save Settings** to save the changes.

Network Interfaces

Configuring iLO Manager Dedicated Network Interface

Procedure

1. From the main Intelligent Provisioning screen, click **Perform Maintenance > iLO Configuration > Network Interfaces > Manager Dedicated Network Interface**.
2. Configure the following settings:
 - Auto Neg: Select this option and the NIC automatically configures speed and duplex.
 - FQDN
 - Frame Size
 - Full Duplex: Enable full duplex on the NIC. Auto Neg overrides this option.
 - Host Name: Provide the DNS Host name.
 - IPv4 Addresses
 - IPv6 Addresses
 - IPv6 Static Addresses
 - IPv6 Default Gateway
 - Link Status (of this port)
 - MAC address

- Max IPv6 Static Addresses
- Name Servers
- Permanent MAC Address
- Speed Mbps
- UEFI Device Path
- DHCPv4
 - Enabled
 - Use DNS Servers
 - Use Domain Name
 - Use Gateway
 - Use NTP Servers
 - Use Static Routes
- SLAAC Enabled
- Static Default Gateway
- Static Routes
- Shared Network Port Options
 - NIC
 - Port
- Configuration Settings
- Domain Name
- Host Name
- Interface Type
- NIC Enabled
- Ping Gateway On Startup
- NIC supports IPv6
- Supports Flexible LOM

3. Click **Save Settings** to save your changes.

Configuring iLO Manager Shared Network Interface

Procedure

1. From the main Intelligent Provisioning screen, click **Perform Maintenance > iLO Configuration > Network Interfaces > Manager Shared Network Interface**.
2. Configure the following settings:

- Auto Neg: Select this option and the NIC automatically configures speed and duplex.
- FQDN
- Frame Size
- Full Duplex: Enable full duplex on the NIC. Auto Neg overrides this option.
- Host Name: Provide the DNS Host name.
- IPv4 Addresses
- IPv6 Addresses
- IPv6 Static Addresses
- IPv6 Default Gateway
- Link Status (of this port)
- MAC address
- Max IPv6 Static Addresses
- Name Servers
- Permanent MAC Address
- Speed Mbps
- UEFI Device Path
- DHCPv4
 - Enabled
 - Use DNS Servers
 - Use Domain Name
 - Use Gateway
 - Use NTP Servers
 - Use Static Routes
- SLAAC Enabled
- Static Default Gateway
- Static Routes
- Shared Network Port Options
 - NIC
 - Port
- Configuration Settings
- Domain Name
- Host Name
- Interface Type

- NIC Enabled
 - Ping Gateway On Startup
 - NIC supports IPv6
 - Supports Flexible LOM
3. Click **Save Settings** to save your changes.

User Accounts

Configuring iLO Account Services

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > User Accounts > Account Service**.
2. Configure the following settings:
 - Auth Failure Delay Time Seconds
 - Auth Failure Logging Threshold
 - Auth Failures Before Delay
 - Default Password
 - Default User Name
 - Min Password Length
3. Click **Save Settings** to save the changes.

Editing User Account settings

Procedure

1. On the iLO Configuration Utility screen, click **User Accounts**, and then click **Administer User Accounts**.

The User Accounts screen appears.

2. Select a user account.
3. Enter the user's password. Re-enter the password to confirm it.
4. Select the appropriate permissions for the user account:
 - **Login Priv**—Enables a user to log in to iLO.
 - **User Config Priv**—Provides the user account with user configuration privileges.
 - **Virtual Power and Reset Priv**—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.

- **Host BIOS Config Priv**—Enables a user to configure the host BIOS settings by using the UEFI System Utilities.
- **Host Storage Config Priv**—Enables a user to configure to host storage settings.
- **Remote Console Priv**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Media Priv**—Enables a user to use the Virtual Media feature on the host system.
- **iLO Config Priv**—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.
- **Host NIC Config Priv**—Enables a user to configure the host storage settings.

5. Click **Update**.

Adding a user account

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > User Accounts > Add User Account**.
2. Enter the following information:
 - Login Name
 - User Name
 - Password
 - Confirm Password
3. Select **Service Account** if the service user.
4. Click **Add** to create the account.

Resetting the iLO

Procedure

1. From the main Intelligent Provisioning page, click **Perform Maintenance > iLO Configuration > Reset Options**.
2. Select from the following options:
 - Reset iLO
 - Reset to Factory Default Settings
 - Clear RESTful API state

Configuring Intelligent Storage

The Intelligent Storage options allow you to:

- Create arrays
- Create logical drives
- Create logical devices
 - Logical drives
 - Physical drives
 - Storage enclosures
- Change configuration settings
- View system messages

Creating a new array or logical drive

Procedure

1. Click **+ Create Array**.
2. To create a simple array, click **Simple Array**.
3. Select a **Logical Drive Type**.
4. Select the **Number of Drives**.
5. Enter a **Logical Drive Name**.
6. Select a RAID mode.
7. Select a **Minimum Array Size**.
8. Review the array settings.
9. Click **Submit**.

Configuring an array or logical drive

Procedure

1. Make changes to the following options:

NOTE: Changes take place during the next reboot.

- General
 - Transformation Priority
 - Rebuild Priority
 - Surface Scan Analysis Priority

- Surface Scan Analysis Delay (Seconds)
- Current Parallel Surface Scan Count
- Advanced
 - RAID 6/60 Alternate Consistency Repair Policy
 - Maximum Drive Request Queue Depth
 - Monitor and Performance Analysis Delay (Seconds)
 - HDD Flexible Latency Optimization
 - Parity RAID Degraded Mode Performance Optimization
 - Physical Drive Request Elevator Sort
- Cache
 - Read Cache Percentage
 - Write Cache when Battery Not Present
 - Write Cache Bypass Threshold (KiB)
 - Physical Drive Write Cache
- Spare
 - Predictive Spare Activation Mode
- Power
 - Power Mode
 - Survival Mode

About Hardware Validation Tool

The Hardware Validation Tool performs discovery on the components in your system and then displays the results. You can:

- Test the system
- View test results
- Export test results

Using the hardware validation tool

Procedure

1. Click **Hardware Validation Tool**.

The tool performs hardware discovery. This discovery process might take several minutes.

2. After discovery finishes, the tool displays the test results.
3. Select one of the following tabs:

- **Survey:** Displays an overview of the hardware in the system.
- **Test:** Tests the hardware and displays the test results.
- **Export:** Export test results. If there is no network connection, save the files to a USB key.
- **Compare:** Compare the tests to previous test results.

Erasing server data

About erasing data in Intelligent Provisioning

Intelligent Provisioning provides two methods to secure data on a server you want to decommission or prepare for a different use. Both methods follow NIST Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization*.

For more information about the specification, see <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf>.

NOTE: Section 2.5 of the specification describes the level of sanitization. The appendix recommends minimum sanitization levels for media.

One-button secure erase

One-button secure erase implements the NIST SP 800-88 Revision 1 Sanitization Recommendations for **Purging** user data and returns the server and supported components to the default state. This feature automates many of the tasks you follow in the *Statement of Volatility* document for a server.

This feature is supported only on Gen10 servers that have been updated with SPP version 2019.03.0 or later.

To use this feature, the storage drives attached to the affected Gen10 system must support a native sanitize method. Examples include the `SANITIZE` command for SATA and SAS drives and `FORMAT` for NVM Express drives. The NIST publication recommends these commands for purging data on these device types. Using these commands is more secure than using software to overwrite data on storage drives.

When a One-button secure erase is in progress, iLO prevents firmware update and iLO reset operations.

If you want to use the server after you perform the One-button secure erase procedure, you must provision the server.

NOTE: You can also use the iLO RESTful tool to launch the One-button secure erase feature.

System Erase and Reset

The System Erase and Reset function overwrites data on drives by using the guidelines from DoD 5220.22-M. This feature is analogous to the NIST SP 800-88 Minimum Sanitization Recommendations Revision 1 description of **clearing** data. In this method, software overwrites all block devices attached to the system by applying random patterns. This method can be used to overwrite devices that do not support One-button secure erase. For example, use this option for drives that do not support a native sanitize method.

-
- ⚠ CAUTION:** One-button secure erase and System Erase and Reset should be used with extreme caution, and only when a system is being decommissioned or used for a different purpose. The system and iLO may reboot multiple times until the process completes. The erase features:
- Wipe data from drives and any non-volatile/persistent storage.
 - Reset iLO and delete all licenses stored there.
 - Reset BIOS settings.
 - Delete AHS and warranty data stored in the system.
 - The processes also delete any deployment settings profiles.
-

Using One-button secure erase

Prerequisites

- An active iLO Advanced license is installed.
- You have an iLO user account with all iLO 5 privileges, including **Recovery Set**.
- Disable the following:
 - Server Configuration Lock
For instructions, see the *UEFI System Utilities User Guide for HPE ProLiant Gen10 Servers and HPE Synergy*.
 - Smart Array Encryption
For instructions, see the "Clearing the encryption configuration" section in the *HPE Smart Array SR Secure Encryption Installation and User Guide*.
- If iLO is configured to use the High Security, FIPS, or CNSA security state, change the security state to Production.
For instructions, see the *HPE iLO 5 User Guide*.

NOTE: Intelligent Provisioning does not support the High Security, FIPS, or CNSA security states. On servers that use these security states, you can use REST tools to initiate the One-button secure erase process. For more information, see the REST documentation.

- c-Class and HPE Synergy users:
 - Remove HPE OneView or Virtual Connect profiles assigned to the system.
- The iLO security setting on the system maintenance switch must be in the OFF position.
- Hewlett Packard Enterprise recommends configuring SNMP, AlertMail, or iLO RESTful API alerts before initiating the One-button secure erase process. If errors occur when individual components are erased, an Integrated Management Log (IML) entry is logged for each error. The IML is erased later during the One-button secure erase process. After the log is erased, the individual component errors will be unavailable. Using SNMP, AlertMail, or iLO RESTful API alerts allow you to review the IML log.

Procedure

1. Disconnect or detach any storage devices that you do not want to be erased using this procedure. This includes any removable drives, external storage, and shared storage.

NOTE:

- Hewlett Packard Enterprise recommends disconnecting or detaching drives that are not being erased to reduce the chances of data loss.
- An Integrated Management Log (IML) reports an erase failure for each drive not supporting native sanitize methods. Other errors might also occur when erasing the drives and are reported in the IML. Consult the IML and Troubleshooting guide for details. The overall status of user data erase, that includes erase of drives, is reported as "Completed with errors" in these cases.

-
2. From the main Intelligent Provisioning screen, click **Perform Maintenance**, and then follow the onscreen prompts to begin erasing the system.
 3. Click One-button secure erase.

! **IMPORTANT:** Securely erasing the system might take up to a day or more to complete, depending on the storage size. Avoid interactions with iLO or the system that involves configuration changes and powering the system off, until the procedure is complete.

The server reboots and the BIOS deletes the data that it controls. After the BIOS finishes this process, the system powers off. iLO then deletes the remaining items.

If errors occur when individual components are erased, an Integrated Management Log (IML) entry is logged for each error and you receive a notification if you configured SNMP, AlertMail, or Redfish alerts. The IML is erased later during the One-button secure erase process. After the log is erased, the individual component errors will be unavailable. When the One-button secure erase process is complete, a final IML entry is logged. This entry provides summary information and does not include failure information for specific components.

The overall progress of the operation can be viewed from the **Always On Intelligent Provisioning** page, which is accessible from the iLO web interface. This page is not accessible during an iLO reset.

On c-Class and HPE Synergy servers, the iLO network settings might be reassigned after the process is complete, and the system might power on.

Impacts to the system after One-button secure erase completes

The One-button secure erase feature reverts the system and supported components to the factory state. To use the system, reprovision the server.

- All data on impacted storage drives and persistent memory is erased and is not recoverable. All RAID settings, disk partitions, and OS installations are removed.
- BIOS and iLO 5 settings are reset to the factory default settings.
 - iLO 5 network and other settings are erased and will need to be reconfigured.
 - iLO 5 Language Packs are removed and iLO 5 will display text in English only.
 - Installed iLO 5 licenses are removed and the license status reverts to iLO Standard.
 - The System Recovery Set is removed and will need to be recreated.
 - iLO 5 user accounts are removed. After the process is complete, log in with the default factory Administrator account and password.
 - The Active Health System, Integrated Management Log, and iLO Event Log are cleared.
 - BIOS and SmartStorage Redfish API data is removed and then recreated on the next boot.

- Secure Boot is disabled and enrolled certificates are removed (other than the factory installed certificates).
- Boot options and BIOS user-defined defaults are removed.
- Passwords, pass-phrases, and encryption keys stored in the TPM or BIOS are removed.
- The date, time, DST, and time zone are reset.
- The system will boot with the most recent BIOS revision flashed.

- Intelligent Provisioning will not boot and will need to be reinstalled.

Returning the system to an operational state requires the following:

- Configure the iLO 5 network settings. For more information, see the *iLO 5 User Guide*.
- Install Intelligent Provisioning using an Intelligent Provisioning recovery image.
- Install an operating system.
- Install iLO licenses.
- Configure BIOS settings.

NOTE: Requirements differ based on the system contents and system use.

Hardware components that are reverted to the factory state:

Gen10 hardware impacted	Hardware not impacted
UEFI Configuration store	USB drives
RTC (System Date and Time)	SD cards
Trusted Platform Module	iLO Virtual Media
NVRAM	Configuration on PCI controllers
<ul style="list-style-type: none"> • BIOS Settings • iLO Settings • Integrated Management Log • iLO Event Log 	
<ul style="list-style-type: none"> • HPE Smart Array SR controllers and drives connected on the internal ports. For example, 3I:1:1 • HPE Smart Array S100i Software RAID 	<ul style="list-style-type: none"> • HPE Smart Array MR controllers and connected storage • Drives connected to external ports on HPE Smart Array SR controllers, for example, 1E:1:1. • SAS HBAs and connected drives

Table Continued

Gen10 hardware impacted	Hardware not impacted
Drive data (for drives that support native sanitize methods). <ul style="list-style-type: none"> • SATA, SAS drives (SSD and HDD) • NVM Express 	SATA, SAS, and NVM Express drives that do not support native sanitize methods. For example, most drives used with Gen9 and earlier servers.
Persistent memory <ul style="list-style-type: none"> • NVDIMM-N • Intel Optane DC Persistent Memory 	FCoE, iSCSI storage
Embedded Flash <ul style="list-style-type: none"> • RESTful API data • AHS • Firmware repository 	GPGPUs Other FPGAs, accelerators, offload engines that have keys or storage

One-button secure erase FAQ

Does One-button secure erase purge USB devices and internal SD cards?

No. One-button secure erase does not erase USB devices and internal SD cards.

If an HDD does not support the Purge function, does One-button secure erase attempt to purge it?

No. One-button secure erase skips a drive that does not support the purge function.

Does One-button secure erase support Smart Array controllers?

Only HPE Smart Array "SR" controllers are supported for One-button secure erase.

Does Smart Array erase drives that do not support Purge?

Smart Array can wipe drives (overwrite with a pattern) that do not support the purge operation. One-button secure erase does not request the Smart Array to perform this nonsecure wipe. Use the Intelligent Provisioning "System Erase and Reset" feature to wipe data on such drives.

Does One-button secure erase erase battery backed cache?

See the table following for more information.

How does One-button secure erase process the erase commands?

See the following table for information on how One-button secure erase purges or overwrites data.

What requirements do users need to launch One-button secure erase?

Users need all iLO privileges to launch One-button secure erase.

Does One-button secure erase remove the serial number and product ID?

No, these items are not erased by One-button secure erase.

How long does the process take?

The duration depends on the hardware. Sanitization of HDDs takes longer than SSDs.

Table 1: How One-button secure erase affects supported drives

Device	Operation requested	Result
NVRAM	3-pass write: 0x5a, 0xa5, 0xff	All battery backed iLO SRAM memory is overwritten.
Embedded Flash (NAND)	eMMC 5.1 (JEDEC 84-B51) 'Secure Erase' command, with SECURE_REMOVAL_TYPE in Extended CSD = 0	All physical memory blocks are erased.
Intel Optane DC PMM	Secure Erase + Overwrite DIMM	Cryptographic keys are removed and data in all physical memory blocks (both user accessible and in spare blocks) is overwritten with zeros. PCD regions containing all configuration and metadata is also overwritten.
NVDIMM-N	JEDEC JESD245B "Factory Default"	Data in all physical memory blocks is erased except warranty information. All readable registers reset to defaults.
UEFI configuration store	3-pass: Chip erase (0xff), 0x00, Chip erase (0xff)	All physical sectors are overwritten.
RTC	Reset time to 01-01-2001 00:00:00	Date, Time, Time zone, and DST are reset to defaults.
TPM	TPM Clear + Clear NV indices + Delete Platform Symmetric key + Change PPS + Change EPS	All data in TPM is cleared including any nonvolatile information.

Table Continued

Device	Operation requested	Result
HPE Smart Array SR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize <hr/> NOTE: Before initiating the One-button secure erase, the "Security reset function" must be performed manually through the HPE Smart Storage Administrator, if Smart Array Secure Encryption was enabled.	<ul style="list-style-type: none"> The security reset function removes the drive keys that are stored on the ESKM for remote key management. All secrets, keys, and passwords from the controller and drives are cleared. This operation does not remove the controller key on the ESKM. All array configurations, logical drives and metadata are deleted. All controller settings are reset to their factory defaults. Flash backup is cleared and data in the DRAM write back cache is lost when the power is removed. <p>All attached drives are requested to be sanitized. See below for operations requested on the drives.</p>
HPE Smart Array S100i Software RAID	Reset to SATA AHCI mode + Physical drive sanitize	The controller is reset to the default SATA AHCI mode. All array configurations, logical drives, and metadata are deleted. All attached SATA drives are requested to be sanitized as below.
SATA HDD ¹	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten with zeros, including those that are not user accessible. Any previous data in caches are also made inaccessible.
SATA SSD ¹	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.

Table Continued

Device	Operation requested	Result
	A single pass of ATA SANITIZE with BLOCK ERASE option	Previous data in all physical memory blocks, including those that are not user accessible, becomes irretrievable. Any previous data in caches are also made inaccessible.
SAS HDD ²	A single pass of SCSI SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten, including those that are not user accessible. Any data in caches are also sanitized.
SAS SSD ²	A single pass of SCSI SANITIZE with BLOCK ERASE option	All physical memory blocks, including those that are not user accessible, are set to a vendor-specific value. Any data in caches are also sanitized.
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2 if supported	This is a cryptographic erase accomplished by deleting the encryption key.
	A single pass of NVM Express FORMAT with SES = 1	All data and metadata associated with all namespaces is destroyed. All user content present in the NVM subsystem is erased.

1. These drives might be connected to the HPE Smart Array “SR” controllers or the Chipset SATA controller.
2. SAS drives connected only to the HPE Smart Array “SR” controllers are supported.

Supported device(s) that fail the erase, and devices that are not supported, are not erased securely. These drives might contain sensitive data. Isolate drives that are not erased and use other methods to delete the data, or securely dispose of the device according to your organization's security policies.

Using System Erase and Reset

Use System Erase and Reset to clear hard drives and Intelligent Provisioning Preferences.

In this mode, Intelligent Provisioning software overwrites data on the drives using the guidelines from DoD 5220.22-M, which is similar to the NIST description of clearing data. All block devices attached to the system are overwritten by applying random patterns in a three-pass process. These block devices include drives attached to the server. Depending on the amount of storage installed on a system, the overwrite process can take many hours or even days to complete. Use this method to select and erase drives on the system that didn't support the native sanitize methods used by One-button secure erase.

System Erase and Reset options

The following table includes the options in the System Erase and Reset menu and a description of what selecting each option will do.

Option	Description
All Hard Drives	Erase all hard drives on this server. NOTE: Only supported in F10 mode, not supported in Always On Intelligent Provisioning.
Wipe Hard Drives	Writes a data pattern over all drive sectors. This action might take several hours. NOTE: Only available if you select All Hard Drives .
Intelligent Provisioning Preferences	Clear Intelligent Provisioning preferences.
Active Health System logs	Clears all AHS log files.

Creating a RAID configuration with HPE SSA

Using HPE Smart Storage Administrator (HPE SSA)

HPE SSA provides 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

Procedure

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

The Smart Storage Administrator window is displayed.

Configuration

On the Smart Storage Administrator screen, under **Actions**, click **Configure**. Options include:

- **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

On the Smart Storage Administrator screen, under **Actions**, click **Diagnose**. Options include.

- **Array Diagnostics Report**—Runs reports on selected controllers to display available diagnostic tasks. Reports include SmartSSD Wear Gauge information for supported solid state drives.
 - **View Diagnostic Report**—Generates and displays 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**—Generates 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**—Displays SSD usage and estimated lifetime information.
 - **Save SmartSSD Wear Gauge Report**—Generates a report for export, without presenting a graphical display.

Using the USB Key Utility

The 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.

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.

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

Installing the utility adds a shortcut in USB Key Utility program group in the Programs Start menu folder.

Procedure

1. Double-click the **USB Key Utility** shortcut in the USB Key Utility 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**.

NOTE: Do not select the **Add an additional CD/DVD to a bootable USB key option** with SUM 6.2.0, SPP 2014.02.0, or Intelligent Provisioning 1.60 and later, which no longer support multiple-boot environments on a single device.

- 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: If you do not see your drive key, click **Rescan Target** or 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. To display the `README.TXT` file, click **Finish**.

NOTE: The `README.TXT` file is only displayed if the ISO has one to view.

Adding content to a bootable USB key

The 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: SUM 6.20, SPP 2014.02.0, and Intelligent Provisioning 1.60 and later no longer support multiple-boot environments on a single device. SUM, SPP, and Intelligent Provisioning contain signed parts that work with the UEFI boot loader. This change no longer allows for multi-boot setups on a single device, such as a USB key.

Procedure

1. Follow the instructions for creating a bootable USB key.
2. Double-click the **USB Key Utility** shortcut in the USB Key Utility folder.
3. Complete each step presented by the application:
 - a. Click **Next** at the splash screen.
 - b. Select **Agree**, and then click **Next** after reading the End-User License Agreement.
 - c. Select **Add an additional CD/DVD to a bootable USB key**, and then click **Next**.
 - d. Place the USB flash drive in an available USB port. Insert the media into 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 then click **Next**.
 - f. Click **Next** on the informational screen.

The source contents are copied to the USB flash drive.
 - g. To display the `README.TXT` file, click **Finish**.

NOTE: The `README.TXT` file is only displayed if the ISO has one to view.

4. Repeat steps 2–3 for each source media or image to be transferred to the USB key.

Troubleshooting

Basic troubleshooting techniques

Intelligent Provisioning provides basic troubleshooting tools you can use to resolve issues.

Troubleshooting general issues

iLO log on required during Intelligent Provisioning F10 boot

Symptom

Cannot log on to Intelligent Provisioning without providing iLO user name and password during **F10** boot.

Cause

The RBSU BIOS Admin password has been set.

Action

1. Force a shutdown, and then boot to the RBSU.
2. Delete the Admin password.
3. Click **Save** and exit.
4. Select **System Utilities > Embedded Application > Intelligent Provisioning**.
5. Launch Intelligent Provisioning.

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 Intelligent Provisioning automatically.

Solution 1

Cause

There is an issue with the current Intelligent Provisioning files.

Action

1. Download the Intelligent Provisioning ISO image and the USB Key Utility from hpe.com. See [**Using the USB Key Utility**](#) for more information.
2. Create a bootable USB key, and then copy the ISO image.
3. Insert the USB key, and then power up the unit.
4. To boot from the USB key, press **F11**, and then select **Option 3: One Time Boot to USB Drive Key**.

The system boots from the USB key and installs IP Recovery. When the installation is complete, the utility prompts you to remove the USB key.

5. Remove the USB key.
6. Reboot the system and press **F10** (IP Recovery) to verify IP Recovery launches properly.

Solution 2

Cause

The iLO is running in FIPS mode.

Action

1. Enter the iLO configuration screen and turn off FIPS mode.
2. Boot the server into F10 mode.
3. After making all changes, enable FIPS mode.

Intelligent Provisioning PXE flashing doesn't re-image Always On Intelligent Provisioning

Symptom

Intelligent Provisioning PXE flashing doesn't re-image Always On Intelligent Provisioning

Note: User should follow the above said command lines only for the reference and are not recommended to copy the same

Action

Update the Kernel command line with the word "Install". For example:

```
linuxefi /IP3.30/vmlinuz media=net splash quiet isol=http://  
192.168.100.101/iso/IP330.2019_0103.230.iso isolmnt=/mnt/bootdevice  
nicmac=5c:b9:01:c5:43:d0 install  
echo 'Loading initial Ramdisk...'  
initrdefi /IP3.30/initrd.img
```

NOTE: Modify the example to fit your system's details.

OS Host name field missing

Symptom

The OS Host name field on the **Intelligent Provisioning Assisted Install > OS selection** page is missing.

Action

OS Host name has been replaced with the Computer name which performs the same function.

Accessing version information in deployment settings

Symptom

Version information for the Deployment settings utility is blank.

Cause

Version information is no longer located in the Deployment settings utility.

Action

Click the **System Information** icon at the top of the screen for version information.

A browser does not import a deployment profile correctly

Symptom

Intelligent Provisioning does not import a deployment profile correctly.

Action

Verify that the profile is saved as a `.txt` file format.

Some Legacy BIOS Mode installs need specific instructions

If the server boot mode is set to Legacy BIOS Mode, some operating systems need specific installations.

NOTE: Legacy BIOS Mode behavior cannot be modified by pressing **F10**. If you are doing a manual installation in Legacy BIOS Mode, ensure that:

- On Windows systems, the system boots to the DVD.
- On Linux and VMware systems, the system boots to the hard drive.

NOTE: Change the boot order, or press **F11** during the boot process.

Always On Intelligent Provisioning does not display status of NICs

Symptom

When viewing NICs in Always On Intelligent Provisioning, the NIC does not display the status.

Action

1. Check the status of the NIC options in the iLO page or RBSU.
2. Select the port in AOIP, and then continue with the installation.

Cannot create a custom partition size

Symptom

When installing an OS, you cannot create a custom partition size.

Action

No action. Intelligent Provisioning does not support creating a custom partition size when installing the operating system.

Intelligent Provisioning cannot launch One-Button secure erase

Symptom

You are unable to launch One-button secure erase from Intelligent Provisioning.

Solution 1

Cause

You do not have the correct license.

Action

Install an iLO Advanced license to use One-button secure erase.

Solution 2

Cause

The user credentials provided doesn't have sufficient privileges to start the erase.

Action

Log in with a user account that provides all privileges, or change the user privileges.

Solution 3

Cause

Server Configuration Lock is enabled.

Action

Disable Server Configuration Lock.

More information

[Using One-button secure erase on page 51](#)

One-Button secure erase is unsuccessful or reports errors

Symptom

One-button secure erase reports errors for one or more components in the system, and does not successfully erase the system.

Solution 1

Cause

The drive doesn't support the secure erase method, or the drive failed to complete the erase.

Action

1. Do one of the following:

- For drives supported by One-button secure erase: Launch One-button secure erase again.
- For drives that are not supported by One-button secure erase: Use the System Erase and Reset function.

Solution 2

Cause

Drives connected to the external ports of a supported Smart Array controller, the drives are not erased.

Action

Use the System Erase and Reset function to erase external drives.

Make sure that external drives are not connected to other systems before erasing external drives.

Solution 3

Cause

The system failed to complete the One-button secure erase operation on some devices after two attempts.

Action

Use the System Erase and Reset feature in Intelligent Provisioning to overwrite data on these drives.

One-Button secure erase succeeds but some drives are not erased.

Symptom

One-button secure erase finishes successfully, but some components are not erased.

Cause

Some components are not supported by One-button secure erase. For example:

- HPE Smart Array MR controllers and drives connected to these controllers are not supported.
- SAS HBAs and connected drives are not supported.
- Storage attached to iSCSI, FC/FCoE, USB, iLO Virtual Media, SD cards are not supported.

NOTE: For more information, see the One-button secure erase prerequisites.

Action

Use the System Erase and Reset feature in Intelligent Provisioning to overwrite the data on these devices.

NOTE: Data that is overwritten does not meet the same erase standard as data that is purged by One-button secure erase.

More information

[Using One-button secure erase on page 51](#)

One-Button secure erase reports errors, but no specific details.

Symptom

One-button secure erase reports errors, but provides no details on specific component failures.

Cause

One-button secure erase clears all logs from the system. It erases errors reported during One-button secure erase. Only a final message indicating a summary of the procedure is available after all erase completes.

Action

Configure SNMP, AlertMail, or Redfish alerts in iLO to receive error notifications during One-button secure erase.

Troubleshooting Windows-specific issues

Windows Essentials does not install from USB source

Symptom

Windows Essentials does not install from a USB source.

Cause

USB installations are not supported for Windows Essentials.

Action

Install Windows Essentials from an ISO source.

Windows does not install on AMD servers

Symptom

Intelligent Provisioning does not install Windows on AMD servers as expected.

Cause

The BIOS setting IOMMU is activated.

Action

1. From the Intelligent Provisioning main screen, select **Perform Maintenance > BIOS/Platform Configuration > Virtualization Options > AMD (R) IOMMU**.
2. Select **Disabled**.
3. Save the setting, and then reinstall the operating system.

Troubleshooting Linux-specific issues

Unable to proceed with Assisted installation of Red Hat Enterprise Linux 7

Symptom

When installing Red Hat Enterprise Linux 7, you are unable to proceed with the Assisted installation with valid OS images through FTP source media.

Cause

Required Red Hat OS files are missing or incorrectly placed.

Action

1. Make sure that all the required Red Hat OS files are present in the OS flat file folder.
2. Make sure that two `TRANS.TBL` files are present in the Red Hat OS flat files folder. One file must be present in the main OS file folder, and another must be present inside the Server folder inside the main OS file folder.
3. Retry the installation.

Assisted installation of Red Hat OS hangs

Symptom

When using the Assisted installation method for Red Hat OS installation with FTP source media, one of the following problems occurs:

- 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.
- The installation completes successfully even if there are missing flat files for the OS installation.

Cause

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

Action

1. Obtain the DUD from the HPE Support Center.
2. Install the OS outside of Intelligent Provisioning.

Troubleshooting VMware-specific issues

Server reboots during VMware Assisted installation

Symptom

When performing a VMware Assisted installation with DVD as source media, after Pre-installation is complete, the server reboots and the server begins loading the ESXi installer again rather than opening the OS.

Cause

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

Action

1. Remove the USB device.
2. Continue the installation.

Websites

Hewlett Packard Enterprise Information Library	<u>www.hpe.com/info/EIL</u>
Intelligent Provisioning	<u>http://www.hpe.com/servers/intelligentprovisioning</u>
Intelligent Provisioning Information Library	<u>http://www.hpe.com/info/intelligentprovisioning/docs</u>
Service Pack for ProLiant	<u>www.hpe.com/servers/spp</u>
Service Pack for ProLiant documentation	<u>www.hpe.com/info/spp/documentation</u>
Service Pack for ProLiant downloads	<u>www.hpe.com/servers/spp/download</u>
Service Pack for ProLiant custom downloads	<u>www.hpe.com/servers/spp/custom</u>
HPE SDR site	<u>downloads.linux.hpe.com</u>

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<http://www.hpe.com/info/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<http://www.hpe.com/support/hpesc>

Information to collect

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

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:
Hewlett Packard Enterprise Support Center
www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Center: Software downloads
www.hpe.com/support/downloads
Software Depot
www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:
www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

HPE ProLiant and IA-32 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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