Hewlett Packard
Enterprise

Intelligent Provisioning 3.6 User Guide for HPE ProLiantGen10, ProLiant Gen10 Plus Servers, and HPE Synergy

Part Number: 30-68E7D0AB-036
Published: April 2021
Edition: 1

Intelligent Provisioning User Guide for HPE ProLiant Gen10, ProLiant Gen10 Plus 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 Plus servers and HPE Synergy compute modules.

Part Number: 30-68E7D0AB-036
Published: April 2021
Edition: 1

Notices

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.

Table of contents

Introduction

TIP:

The information in this guide is for using Intelligent Provisioning with ProLiant Gen10 Plus 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 (**https://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 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 Lifecycle Management. Lifecycle Management allows you to access Intelligent Provisioning without rebooting your server.

F10/Remote console features

F10/Remote console allows you to:

- Access 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.
- Perform firmware updates from the HPE repository.

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

NOTE:
Intelligent Provisioning 3.40 and later requires iLO firmware version 2.10 or later.

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 (**https://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
Language 	Enables you to select the language to use.
Home 	Returns to the Intelligent Provisioning home page, with the Rapid Setup and Perform Maintenance menus. This icon is available only after completing the initial configuration and registration tasks.
Job Cart 	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.
Help 	Opens the online help to the section about the current screen.
System Information 	Displays system information, including the Intelligent Provisioning version.
Power 	Power down or reboot the server.
Log Out 	Logs the current user out of Intelligent Provisioning. **NOTE:** This icon is only displayed in Always On mode.
Previous 	Returns you to the previous screen after validating and saving your choices.
Continue 	Takes you forward to the next screen after validating and saving your choices.

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
- Smart Storage Administrator (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. From the navigation tree, click **Lifecycle Management**.
4. Navigate to the **Intelligent Provisioning** tab and then click **Always On** button.

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.
   - `.Net Console`
   - `HTML5 Console`
   - `Java IRC Web Start`

   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 .

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 able to use Intelligent Provisioning.

Intelligent Provisioning offer tools to provision and maintain servers.

Intelligent Provisioning
Provisioning multiple servers.
Configuring multiple RAID arrays.
Users who have servers provisioned and deployed.

Selecting F10 mode to use

Procedure

1. Boot the server.
2. On the POST screen, press `F10`.
3. Enter Intelligent Provisioning, if Host Authentication is disabled in iLO. If Host Authentication is enabled, pass the credentials to use Intelligent Provisioning.

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 do not 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 Software Update
   - System Time
   - Choose network interface for updates and installs
   - 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
   - Use Proxy
   - DHCP Auto-configuration: Deselect this option to manually enter DHCP settings, including using IPv6 protocol.
8. To save the changes, click Next, iLO network setting is available to change.
9. 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.
4. Click Save & Exit, and then reboot the server.

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 (**https://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.
   - Gen10 Plus supports Intelligent Provisioning from 3.40.

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.
   - Copy the recovery media to a USB key.
4. To power up the server Press ON.
5. To display the boot menu, press F11 during server POST.
6. Select CD/DVD to boot from the mounted ISO.
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)

Prerequisites

- For SLES 15.x series, before the installation the user might needs to install `gptfdisk`, `sdparm`, and `mdadm`.
- For RHEL 8.x series, before the installation the user might needs to install `sdparm`.

> **NOTE:**
>
> Not supported on RHEL 8.0.

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/repo/ip/).
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:

   ```
   #./hpsetup
   ```

5. Execute the command:

   ```
   #reboot
   ```

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 **Rapid Setup** menu to complete the following tasks:

Procedure

1. Select Install Source
2. Configure Installation Settings
3. Reviewing your settings

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, 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 Rapid Setup 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.

Select Install Source

Prerequisites

- Make sure that the source files are accessible by the system.

Procedure

1. Select Rapid Setup on the Intelligent Provisioning home screen.
2. A Proxy Setting Window prompts. Configure the Proxy Setting if you need it else skip it.
3. Select an Install Source from the icons. The options and the required information and action for each are described in the following table.

Media type	Required information/action
File on a USB drive	Allows you to install an OS from a USB drive. **NOTE:** • This source is not supported in Always On Intelligent Provisioning mode. • You need to extract the ISO and put in the USB before the installation for RHEL 7.x, 8.x and SLES.
DVD-ROM Media	Allows you to install an OS from a DVD-ROM.
SMB/CIFS (Windows Share)	Allows you to install an OS from a Windows Share directory. You need the following network connection information, including: • Server Name or IP Address —Server name or IP address of the server that hosts the OS contents. If a server name is specified, a DNS entry is also required. • Share Name—The name of the network share using Server Message Block (SMB) protocol that hosts the OS contents. • 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	Allows you to install an OS through an FTP source. You need the following network connection information, including: • Server Name or IP Address —FTP server name or IP address of the server that hosts the OS contents. FTP support requires anonymous access to the FTP server and does not support connecting to an FTP server through a proxy. **IMPORTANT:** When entering an FTP path, remove spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).
Install from Internet	Allows you to download source files from an Internet URL.
Virtual media	Allows you to install the OS from a virtual media source. Only supported in Always On Intelligent Provisioning mode.

4. Go to the Install Summary page if the media is supported automatically.

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.

Configure Installation Settings

Prerequisites

To install an OS from an FTP server, extract the installation ISO.

Configure OS Setting

Procedure

1. Enter the required information for the location of the OS files.

   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 **https://www.hpe.com/info/esxidownload**.

2. To proceed, do the following:

   - For Windows Server/Hyper-V Server Installation, it provides the following settings:
     - Operating System: User can select different edition of Windows server for installation.
     - Computer Name
     - Organization Name
     - Owner Name
     - Password
     - Confirm Password
     - OS Language
     - OS Keyboard
     - Time Zone
     - Selection to install Hyper-V role on this system

       NOTE:
       This function will not show up while installing Hyper-V Server.

     - Selection to Enable Windows Firewall
   - For other Linux systems, it only provides the following settings:
     - Operating System
     - OS Hostname
     - Password
     - Confirm Password

     NOTE:
     The default password for EXSi 6.x and 7.x is _Passw0rd_.

Configure Controller

In this page, the user can configure and allocate the disk space. On the OS installation summary page, IP checks the RAID and drive status and performs the following:

- If there is an existing logical drive on the hardware/software raid, then IP just displays the information.
- If there is no existing logical drive, then IP automatically creates an OS drive and Data drive based on the number of drives available.
- You can modify the following logical drives:
  1. Recommended raid configuration that IP automatically created.
  2. Array / Logical drive user created from the RSS.
- You cannot modify any existing array / logical drive on the server.

Procedure

1. Click the Pencil icon on the top-right corner of this page.
2. Click Create Array.
3. Check in the Model number and how you want to use it as an Array or Spare.
4. Click Next.
5. Select the Raid Mode, Raid Size (GB), Accelerator, Legacy Boot priority and Strip size (KB) .
6. Click Next to review your settings.
7. You can either click Back and change the setting or click Done to confirm it.
8. Under, Create Logical Drive you can view the drive information.
9. If you want to delete the current allocation, click Clear all array.

Select OS drive and set partition

In this page, the user can choose to perform manual partition, or let the operating system perform the automatic partition during installation.

For automatic partition:

1. Leave the Use Recommended Partition check box checked.
2. Open Select one following drive to configure as OS drive drop-down menu, select the hard drive on which you wish you install the OS.

For manual partition:

1. Uncheck Use Recommended Partition check box; then the below section displays the chart for the default partition. The chart varies based on the Operating system.

   - For Windows/Hyper-V:

Mount Point	Size (MB)	File System Type	Partition Label
Recovery	500	NTFS	
EFI system partition	100	FAT32	
Microsoft reserved partition	16	NTFS	
Basic data partition	Rest of HDD	NTFS	

   While users can only make change on the Basic data partition, the rest of the partitions are also crucial for maintenance, and should not be changed.

   - For SUSE system:

Mount Point	Size (MiB)	File System Type	Partition Label
`Swap`	2000	`swap`	
`/boot/efi`	150	`vfat`	
`/`	40000	`btrfs`	
`/home`	Rest of HDD	`Xfs`	

   For SUSE system, `/boot/efi` partition does not occur when the boot mode is in legacy mode. While the user can only make change on `/home` partition, the rest of the partitions are crucial for maintenance and should not be changed.

   - For Red Hat Enterprise Linux /ClearOS system:

Mount Point	Size (MiB)	File System Type	Partition Label
`/boot`	1000	`Xfs`	
`/boot/efi`	200	`efi`	
`swap`	1000	`swap`	
`/`	10000	`xfs`	
`/home`	Rest of HDD	`xfs`	

Boot partition should be `biosboot` when the boot mode is in legacy mode. While the user can only make change on `/home partition`, the rest partitions are crucial for maintenance and should not be changed.

NOTE:

a. VMware and RHEL 6.x does not allow manual partition.

b. When boot mode is switched to Legacy mode, manual partition is disabled for Windows/Hyper-V server.

2. To change the partition scheme, for Windows/Hyper-V system:

a. Click the cell you want to change.

b. Adjust the Percentage or Size for this partition, input the Partition Label if necessary, then click the Check icon.

An editable row appears at the top of the table.

c. Enter the data in the following columns:

- Mount Point
- Size
- Percentage
- File System Type

  NOTE: For Windows/Hyper-V , the user can only use **NTFS**.

- Partition Label

Then, click the Check icon to complete.

d. Repeat steps c and d to create more partitions.

To change the partition scheme for SUSE/Red Hat/ClearOS system:

a. Click the /home, and click the cell you want to edit.

b. Adjust the Percentage or Size for this partition, enter Partition Label if necessary, then click the Save Changes button.

c. Should see an editable row at the top of the table.

d. Enter the data in the following fields:

- Mount Point
- Size
- File System Type: for SUSE/Red Hat/ClearOS, user can have the following choices:
  - `btrfs`
  - `ext2`
  - `ext3`
  - `ext4`
  - `vfat`
  - `xfs`
  - `swap`
- Partition Label

  Then click the Create button to complete.

e. Repeat step c and d to create more partitions.

Configure Firmware Update

In this page, the user can choose to Attempt Firmware Update.

Procedure

1. Use the slider available on the screen to update the Firmware.
    - Under the Name tab you will see a list of Firmware Updates available.
    - Under the Available and Current tab you can compare the version number.
2. Click the check box in front of the Firmware name to choose the firmware you want to update.

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 action does not affect the first-time setup, because there is no data present on the server.

Procedure

1. Review and confirm your deployment settings.
2. Click Back to navigate to the Summary and Install button on the top-right corner.
3. Review the setting from the Summary and Install menu.
4. Click the Accept Configure button on the top-right corner to process the OS 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 configured properly. 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.

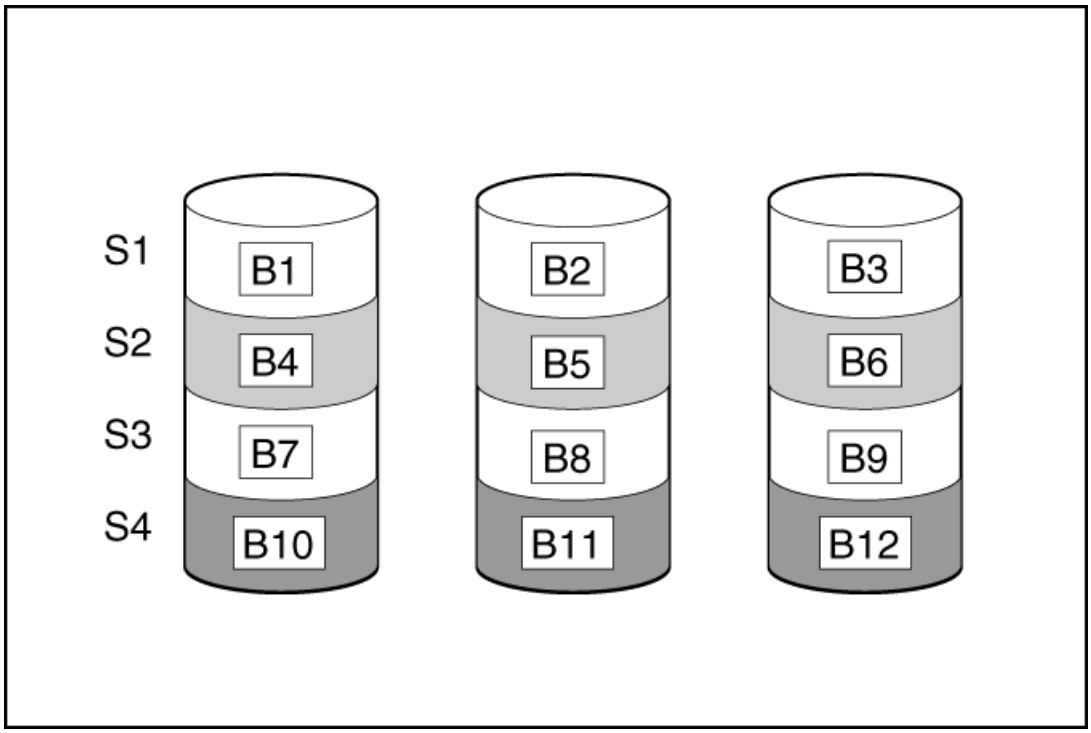
  If the Firmware Update screen is displayed, follow the onscreen prompts to obtain and install the latest firmware on server components. When the updates are complete, the Installing OS page is displayed, ready to begin the OS installation.
- If you attempt to deploy an OS on a server with no installed drives, first the controller selection will not show up, and when the user proceeds to "select OS drive and set partition" page, it will show up an error message stating "No available disk for installation", and the user will not be able to proceed.
- 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.

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.



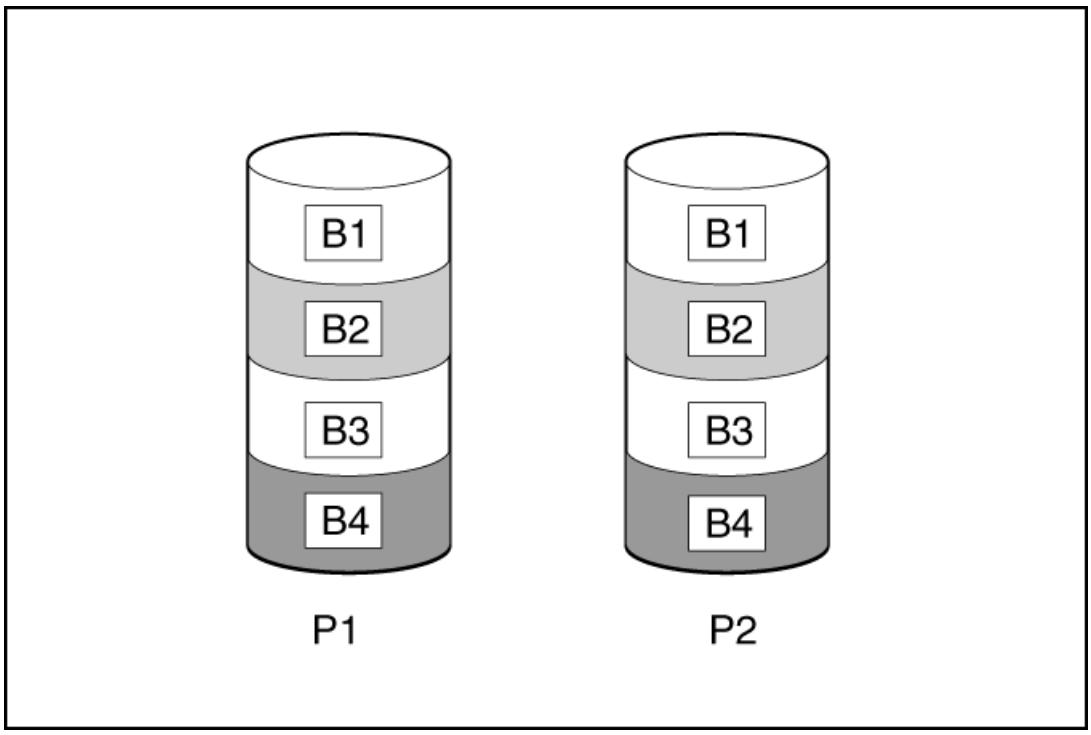
This method has the following benefits:

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

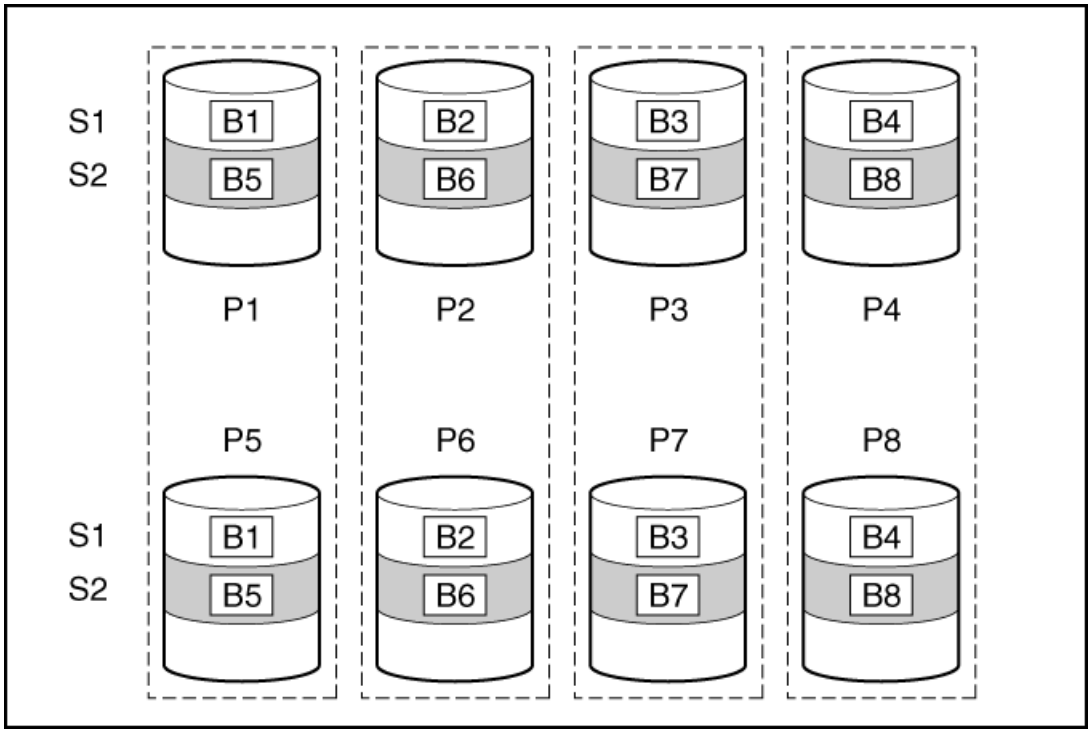
RAID 1 and RAID 1+0 (RAID 10)

In RAID 1 and RAID 1+0 (RAID 10) configurations, data is duplicated to a second drive. The usable capacity is C x (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.

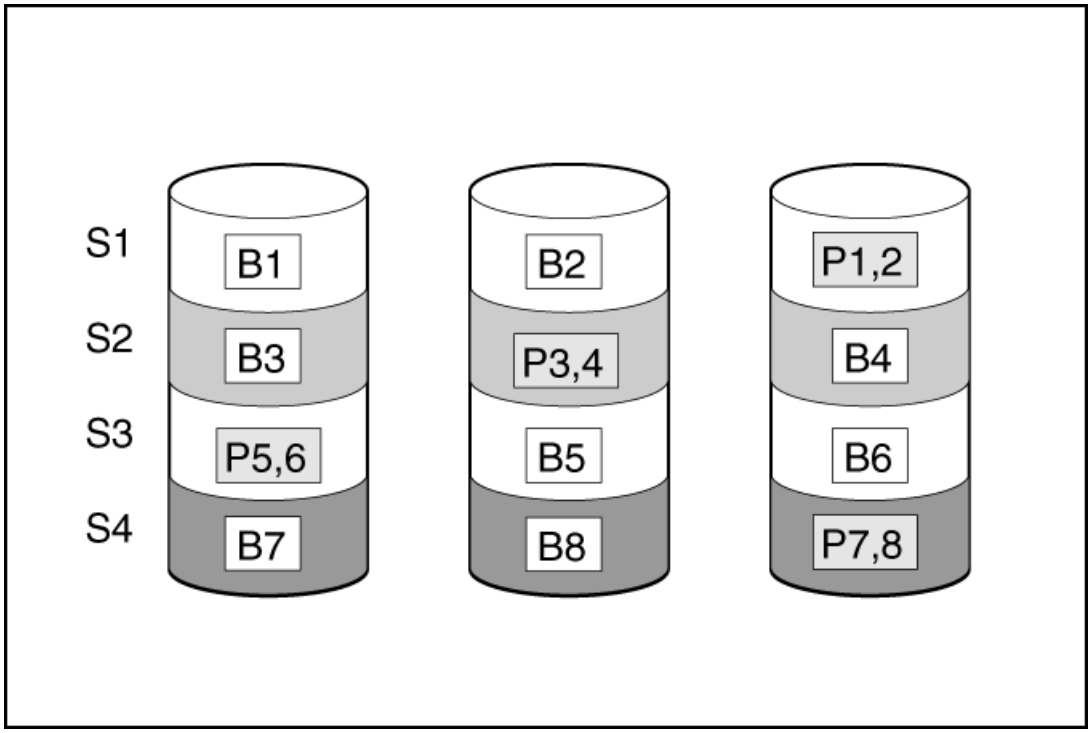


This method has the following benefits:

- 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 Px,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 x (n - 1) where C is the drive capacity with n drives in the array. A minimum of three drives is required.

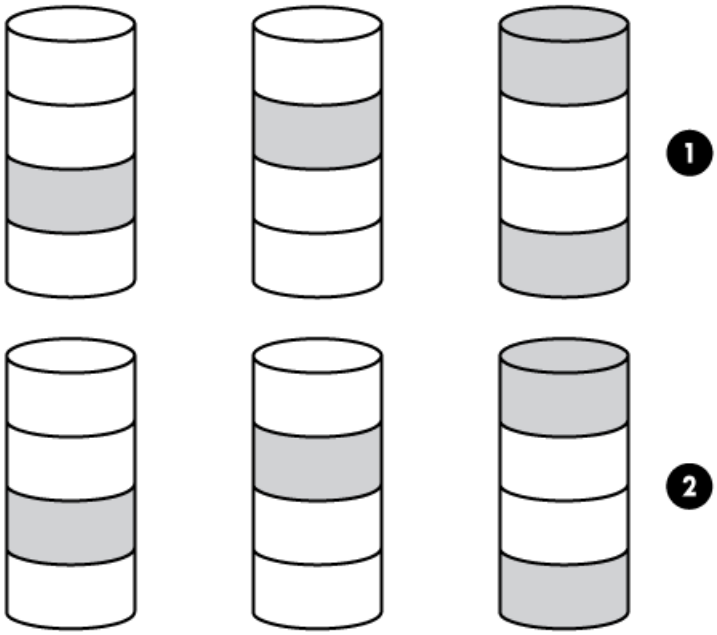


This method has the following benefits:

- 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.

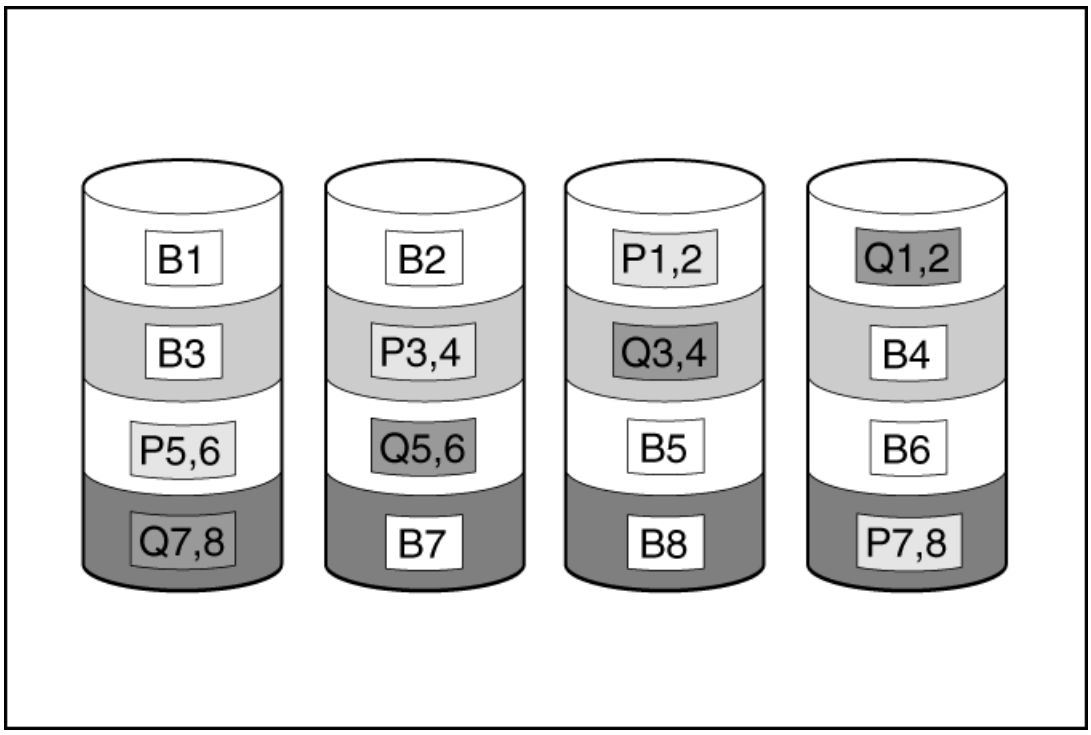
This method has the following benefits:

- 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 Px,y and Qx,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 x (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.

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 and necessary. You can use Intelligent Provisioning to find and deploy available updates.

NOTE:
You can update the Firmware without registering on HPE.

- 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 at **https://www.hpe.com/servers/spp/download**. For instructions on using the ISO, see the Service Pack for ProLiant Quick Start Guide at **https://www.hpe.com/support/SPP_UG_en**.

4. Select one of the following:

   - Newest firmware available

     It displays a list of available firmware update items for this machine.

   - Rollback to previous

     It displays a list available firmware rollback items for this machine. The user must upload the `*.rpm` file to the iLO repository. The IP can only rollback firmware file with file extension `rpm`.

     NOTE:
     The user might need to upload signature file along with `.rpm`.

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

5. Select the items to update, and then click Submit or Rollback.
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**  then check the Intelligent Provisioning version.

Setting Intelligent Provisioning Preferences

Use Intelligent Provisioning Preferences to change the basic preferences, including the interface, 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. In the Basic Setting tab, select settings for the following options:
   - Interface Language
   - Keyboard Language
   - Boot BIOS Mode
     - Legacy Boot Mode
     - UEFI Optimized Boot Disable
     - UEFI Optimized
   - System Software Update—Select a source for firmware update.
     - Update from HPE Website
     - Update from Custom URL
   - Time Zone
   - System Date
   - System Time
   - Enable Feedback
   - Accept EULA, or click Read EULA

   In the Network Settings tab, enter the following details:

   - Choose network interface for updates and installs
   - Use Proxy, and provide proxy details.
   - DHCP Auto-Configuration, `IPv4/IPv6` switch and provide the configuration details.
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 and network sharing 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 **https://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 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. 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 https://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 **https://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
Creating a Deployment Settings package

Creating a Deployment Settings package

Procedure

1. On the Deployment Settings screen, do one of the following:
   a. To create a profile based on an existing one, the user will need to import the profile first and use one of the following options:
      - From Network Share enter:
        - Server Name/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 and Confirm Password —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 Next.
        iii. The newly import deployment named with prefix New Imported.
   b. To create a new customized 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 or special characters.
3. Enter the Version Information—Enter User Notes and Captured From details, and click Done.
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.
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.
6. Enter the Array Configuration—Review or select new settings.
7. Enter Intelligent Provisioning Preferences—See Setting Intelligent Provisioning Preferences .
8. Enter Hardware Validation Tool— Select Hardware Validation Tool options for each deployment.
9. Click Next link on bottom right of the page to save the profile.

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) and Confirm Password —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 Next.
        iii. Click Deploy.
2. As the deployment runs, a validation screen applies settings for the following elements:
   - ROM Settings
   - Array Configuration
   - Version Information
   - Operating System
   - Intelligent Provisioning Preferences
   - Hardware Validation Tool

Deployment Settings actions

Icon	Description
	Click the Deploy icon to launch the automatic configuration utility.
	Click the Edit icon to change the following options: • Version Information • Operating System parameters • Intelligent Provisioning Preferences • Array Configuration information • ROM Settings • Hardware Validation Tool
	Click the Delete icon to delete the selected deployment.
	Click Download to download the performance package to a network share or a USB drive.

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
- System Options
- Memory Options
- Server Security

NOTE:
If a lock icon is shown next to a BIOS option, it means 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. After installing the server with the latest ROM, that is, iLO and IP 3.50RR Build 78, the tinker storage controller fails to detect in the RAID configuration utility. However, the tinker storage controller detects in the F9 page and in the iLO webpage under the Firmware section.

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 drop-down menu.
3. To update the workload profile, click to open Workload Profile drop-down menu.
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 page allows you to change some iLO configurations from the Intelligent Provisioning. For a description on iLO configuration, see **https://www.hpe.com/info/ilo/docs**. Intelligent Provisioning provides the following options to configure the iLO:

- Display iLO Self-Test
- iLO Federation
- Remote Console & Media
- iLO Dedicated Network Port
- iLO Shared Network Port
- Administration
- Security
- Management
- Reset Options

Procedure

1. From the main Intelligent Provisioning page, click Perform Maintenance -> iLO configuration.
2. To navigate to different pages, click the menu.
3. Change the columns.
4. Click Save button to update.

For Administrator and Rest, see the following sections.

Administration

Procedure

1. From the main Intelligent Provisioning page, click Perform Maintenance > iLO Configuration > Administration.
2. Configure the following settings:
   - View user's permission
   - Create account
   - Edit account
   - Delete account
   - Available permissions are listed below:
     - Login: Enable a user to log in to iLO.
     - Virtual Power and Reset: Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the button.
     - Host BIOS: Enable a user to configure the host BIOS settings by using the UEFI System Utilities.
     - Administrator User Accounts: For more information, see HPE iLO 5 User Guide.
     - Host Storage: Enable a user to configure to host storage settings.
     - Remote Console: Enable a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
     - Virtual Media: Enable a user to use the Virtual Media feature in the host system.
     - Configure iLO Settings: Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration.
     - Host NIC: Enable a user to configure the host storage settings.
     - Recovery Set: For more information, see HPE iLO 5 User Guide.

Reset Options

Procedure

1. From the main Intelligent Provisioning page, click Perform Maintenance > iLO Configuration > Management Settings > Reset Options.
2. Reset option performs the following functions:
   - 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.
- Change configuration settings
- View system messages

NOTE:
If the system contains more than one drive, and you configure only one drive as a RAID, the remaining drives are listed as Unconfigured drives.

Creating a new array or logical drive using simple mode

Procedure

1. Click + Create Array.
2. To create a simple array, select Simple Configuration Mode.
3. Select a Logical Drive Type.
4. Select the Number of Drives.
5. Enter a Logical Spare Drive, then click Next to go to next page.
6. Enter a Logical Drive Name.
7. Select a RAID Mode.
8. Select a Minimum Array Size.
9. Select Accelerator and Legacy Boot Priority, and then click Next to go to next page
10. Review the array settings in the Summary page.
11. Click Submit. The Storage Configuration main page appears, displaying the following message "The operation will execute on the next button".
12. Reboot the machine and let the operation take effect.

Creating a new array or logical drive using advanced mode

Procedure

1. Click + Create Array.
2. Switch from Simple Configuration Mode to Advanced Mode.

   It will display a list of installed hard drive, and the physical location chart of the hard drives. The hard drives are marked according to the following conditions:

   - Selected: This field describes the hard drives selected in the list below.
   - Unconfigured: This field describes the hard drives, which are not configured as arrays or logical drives.
   - Configured: This field describes the hard drives, which are configured as arrays or logical drives.
   - Empty: This field describes the slots that does not installed hard drive.
3. Check the hard drives in the list that are marked as Unconfigured in the physical location chart, then click Next to go to next page.
4. Enter a Logical Drive Name.
5. Select a RAID Mode.
6. Select a Stripe Size (KB).
7. Select an Accelerator.
8. Select RAID Size (GB).
9. Select a Legacy Boot Priority, then click **Next** to go to next page.
10. In the Summary page, review the array settings.
11. Click Submit. The Storage Configuration main page appears, displaying the following message "The operation will execute on the next button".
12. Reboot the machine and let the operation take effect.

Configuring an array or logical drive

Procedure

Make changes to the following options:

> **NOTE:**
> Changes take place during the next reboot.

When there are no logical drives, the configuration option is not available.

- 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. Also, identifies the time taken to run the tests by enabling the time, that is elapsed time and sets the test loop.
   - 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.

> **NOTE:**
>
> It is recommended to use Hardware Validation Tool only for limited loop testing. Using it for endless loop testing will fill up the log space. If there are no failures reported at the end of the 2 to 3 testing loops, then the system is working as expected.

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 and later 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 and later 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.
- Server's Initial Device Identity (IDevID)
- Platform Certificate

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 Plus 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 Lifecycle Management 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.

NOTE:
The user needs to login with local user credentials, which has all the privileges.

- 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 network and other settings are erased and must be reconfigured.
  - Installed iLO licenses are removed and the license status reverts to iLO Standard.
  - The System Recovery Set is removed and must be recreated.
  - iLO user accounts are removed. After the process is complete, log in with the default factory Administrator account and password.
  - The Active Health System, Integrated Management Log, and iLO Event Log are cleared.
  - BIOS and SmartStorage Redfish API data is removed and then recreated on the next boot.
  - Secure Boot is disabled and enrolled certificates are removed (other than the factory installed certificates).
  - Boot options and BIOS user-defined defaults are removed.
  - Passwords, pass-phrases, and encryption keys stored in the TPM or BIOS are removed.
  - The date, time, DST, and time zone are reset.
  - The system will boot with the most recent BIOS revision flashed.
- Intelligent Provisioning will not boot and must be reinstalled.

Hardware components that are reverted to the factory state

Hardware impacted	Hardware not impacted
UEFI Configuration store	USB drives
RTC (System Date and Time)	SD cards
Trusted Platform Module	iLO Virtual Media
NVRAM • BIOS Settings • iLO configuration settings • iLO Event Log • Integrated Management Log • Security Log	Configuration on PCI controllers
• HPE Smart Array SR controllers and drives connected on the internal ports. For example, 3I:1:1 • HPE Smart Array S100i Software RAID	• HPE Smart Array MR controllers and connected storage • SAS HBAs and connected drives
Drive data (for drives that support native sanitize methods). • 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.

Hardware impacted	Hardware not impacted
Persistent memory • NVDIMM-N • Intel Optane DC Persistent Memory	FCoE, iSCSI storage
Embedded Flash • 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 privileges do users need to launch One-button secure erase?

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

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

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

How long does the process take?

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

How One-button secure erase affects supported drives

Device	Operation requested	Result
NVRAM	3-pass write: 0x5a, 0xa5, 0xff	All battery backed iLO SRAM memory is overwritten.
Embedded Flash (NAND)	eMMC 5.1 (JEDEC 84-B51) Secure Erase command with SECURE_REMOVAL_TYPE in Extended CSD register set to physical memory erase, if supported by the device.	Data in physical memory is erased.
Intel Optane DC PMM	Secure Erase + Overwrite DIMM	Cryptographic keys are removed and data in all physical memory blocks (both user accessible and in spare blocks) is overwritten with zeros. PCD regions containing all configuration and metadata is also overwritten.
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	All data in TPM is cleared including any nonvolatile information.

Device	Operation requested	Result
HPE Smart Array SR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize **Note:** Before initiating the One-button secure erase, the Security reset function must be performed manually through the Smart Storage Administrator, if Smart Array Secure Encryption was enabled.	• The security reset function removes the drive keys that are stored on the key manager for remote key management. All secrets, keys, and passwords from the controller and drives are cleared. This operation does not remove the controller key on the key manager. • All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. • Flash backup is cleared and data in the DRAM write back cache is lost when the power is removed. All attached drives are requested to be sanitized. See below for operations requested on the drives.
HPE Smart Array S100i Software RAID	Reset to SATA AHCI mode + Physical drive sanitize	The controller is reset to the default SATA AHCI mode. 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 physical sectors that are not user accessible. Any previous data in caches are also made inaccessible.
SATA SSD [1]	ATA SANITIZE with CRYPTO SCRAMBLE EXT if supported.	The CRYPTO SCRAMBLE EXT command changes the internal encryption keys that are used for user data, so the user data is irretrievable.
	A single pass of ATA SANITIZE with BLOCK ERASE option	Previous data in all physical memory blocks, including physical memory blocks that are not user accessible, becomes irretrievable. Any previous data in caches are also made inaccessible.
SAS HDD [2]	A single pass of SCSI SANITIZE with OVERWRITE EXT option	All physical sectors are overwritten, including physical sectors that are not user accessible. Any data in caches are also sanitized.
SAS SSD [2]	A single pass of SCSI SANITIZE with BLOCK ERASE option	All physical memory blocks, including physical memory blocks that are not user accessible, are set to a vendor-specific value. Any data in caches are also sanitized.
NVM Express	NVM Express FORMAT with Secure Erase Setting (SES) = 2, if supported.	This is a cryptographic erase accomplished by deleting the encryption key.
	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 devices that fail the erase process and unsupported devices are not erased securely. These devices might contain sensitive data. Isolate devices that are not erased and use other methods to delete the data, or securely dispose of the devices according to your organization security policies.

Returning a system to operational state after One-button secure erase

After a system is erased with the One-button secure erase process, use the following procedure to return it to an operational state.

Procedure

1. Configure the iLO network settings.

   For more information, see the HPE iLO 5 User Guide.
2. Install Intelligent Provisioning using an Intelligent Provisioning recovery image.
3. Install an operating system.
4. Optional: Install an iLO license.

   For more information, see the HPE iLO 5 User Guide.
5. Configure the BIOS settings and the iLO settings that apply to your environment.
6. (Optional) Create a System Recovery Set.

   For more information, see the HPE iLO 5 User Guide.

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.

NOTE:
The erase option is not applicable for synergy servers.

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. • When there is no hard drive installed in the system, then this function will become unavailable.
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 SSA

Using Smart Storage Administrator (SSA)

SSA provides high-availability configuration, management, and diagnostic capabilities for all Smart Array products.

SSA features

SSA is a browser-based utility that runs in either offline or online mode. 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 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 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 from left panel of Available Device (s) select a RAID controller item under Smart Array Controllers section, and then, under Actions, click Configure. Options include:

- Modify Controller settings—Configures the supported controller settings. Depending on the controller, the options can include setting the array accelerator cache ratio, transform and rebuild priorities, and surface scan delay.
- Set Sanitize Lock—Changes your Sanitize Lock Settings. This option is only available on controllers that support Freeze or Anti-Freeze.
- Advanced Controller Settings—Configures the supported advanced controller settings. The settings can help improve the controller performance for Video-On-Demand applications. For example, changing the elevator sort parameters.
- Modify spare activation mode —Switches the spare activation mode from the default behavior (activate on failure only) to predictive spare activation and back.
- Clear configuration—Resets the controller configuration to its default state. Existing arrays or logical drives are deleted, and data on the logical drives is lost. Confirm that this option is the preferred action before proceeding.
- Manage Power Settings—Modifies the controller power mode and enables or disables survival mode for supported controllers. A reboot or cold boot may be required after changing power modes to optimize power savings and performance.
- 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.
- Check Online Firmware Activation Readiness—Check the current configuration to determine if an Online Firmware Activation is allowed.
- Manage Device Identification LEDs—Turn the physical drive identification LEDs On or Off.
- 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.
- 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.
- 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 its child devices, when applicable.

Diagnose

On the Smart Storage Administrator screen from left panel of Available Device (s), select Server under Server section, and then, 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:
  - 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.

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 does not reimage AOIP

Symptom

Intelligent Provisioning PXE flashing does not reimage Always On Intelligent Provisioning.

NOTE:
The user can follow the command lines only for the reference.

Action

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

```
linuxefi /IP3.30/vmlinuz media=net splash quiet iso1=http://192.168.100.101/iso/IP330.2019_0103.230.iso iso1mnt=/mnt/bootdevice nicmac=5c:b9:01:c5:43:d0 instal
echo 'Loading initial Ramdisk...'
initrdefi /IP3.30/initrd.img
```

NOTE:
Modify the command as per the system requirements.

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

In 3.50 version, the user is allowed to perform manual partition before the OS installation begins. However, manual partition is not supported for the following cases:

- All the versions of **VMware**, in both **UEFI** and **Legacy** modes.
- All the versions of **Windows/Hyper-V Server** in **Legacy** mode.

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

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

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

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

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.

Not able to create or delete logical drive using Software Raid Controller

Symptom

Cannot create or delete logical drives using Software Raid Controller.

Action

1. Set the UEFI POST Discovery Mode to Force Full Discovery in the BIOS using the following procedure:
   - Boot the BIOS
   - From the System Utility screen, select System Configuration > BIOS/Platform Configuration (RBSU) > System Options > Boot Time Optimizations > UEFI POST Discovery Mode
   - Change to Force Full Discovery
2. Save and reboot.
3. Enter Intelligent Provisioning by pressing F10 during POST.

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 settings IOMMU and Hyper-V are 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.
4. Download and install all operating system patches.
5. Reboot the system and then enable IOMMU settings.

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. The failure was seen with a long file path for CIFS share, however, it succeeds with a short path (less than 32 bytes).

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 DVD from the HPE Support Center.
2. Install the OS outside of Intelligent Provisioning.

Showing "Unable to install without the usb_storage driver loaded, Aborting",when upgrade or install with rpm

Symptom

When executing command `./hpsetup`, an error message "Unable to install without the usb_storage driver loaded, Aborting." prompt in console.

Cause

The usb_storage module is disabled.

Action

Enable usb_storage by executing command `modprobe usb-storage`.

Unable to install Red Hat Enterprise Linux with secure boot enabled

Symptom

When installing Red Hat Enterprise Linux or VMware from the Rapid Setup with install method "Assisted Install" after the file copy process is finished, system directly boot into Image without any configuration instead of start the installation process.

Cause

Red Hat Enterprise Linux and VMware are not supported install with secure boot enabled.

Action

1. Disable secure boot in the BIOS.
2. Install target OS from the Intelligent Provisioning.
3. Enable secure boot in the BIOS.

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.

Troubleshooting ClearOS-specific issues

Unable to install ClearOS with secure boot enabled

Symptom

When installing ClearOS from the Rapid Setup install with install method "Assisted Install", the installation process shows "Verification failed: Security Violation" error message.

Cause

ClearOS does not support secure boot.

Action

1. Disable secure boot in the BIOS.
2. Install target OS from the Intelligent Provisioning.

Websites

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

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

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

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

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

Information to collect

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

Accessing updates

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

  Hewlett Packard Enterprise Support Center

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

  Hewlett Packard Enterprise Support Center: Software downloads

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

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter
- To subscribe to eNewsletters and alerts:

  https://www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

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

IMPORTANT:

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

Remote support

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

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

HPE Get Connected

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

HPE Pointnext Tech Care

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

HPE Datacenter Care

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

Warranty information

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

HPE ProLiant and IA-32 Servers and Options

https://www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise and Cloudline Servers

https://www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

https://www.hpe.com/support/Storage-Warranties

HPE Networking Products

https://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:

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

Additional regulatory information

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

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

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

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

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

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

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, 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.