



Hewlett Packard
Enterprise

Intelligent Provisioning 4.34 User Guide for HPE ProLiant and Synergy Gen11 Servers

Part Number: 30-A50246BA-005a
Published: February 2025
Edition: 2

Intelligent Provisioning 4.34 User Guide for HPE ProLiant and Synergy Gen11 Servers

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 Gen11 servers and HPE Synergy compute modules.

Part Number: 30-A50246BA-005a

Published: February 2025

Edition: 2

© Copyright 2017–2024 Hewlett Packard Enterprise Development LP

Notices

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

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

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

Acknowledgments

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

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
 - Intelligent Provisioning
 - F10/Remote console features
 - Always On Intelligent Provisioning (AoIP)
 - Intelligent Provisioning operation
 - Navigating Intelligent Provisioning
- Accessing Intelligent Provisioning
 - Accessing Intelligent Provisioning from the iLO web interface
 - Accessing Intelligent Provisioning using an iLO remote console session
- F10 mode options
 - Selecting an F10 mode
 - Initial configuration in Intelligent Provisioning
 - Using the First Time Setup wizard
 - Entering First Time Wizard settings
 - Re-enabling Intelligent Provisioning
 - Reinstalling Intelligent Provisioning
 - Reinstalling using an ISO image
 - Reinstalling using an RPM package (Linux)
- Configuring the hardware and installing an operating system
 - Configuring the hardware and installing an OS with Intelligent Provisioning
 - Server support and special characters
 - Source media types and installation methods supported for each OS
 - Select install source
 - Configure Installation Settings
 - Configure OS setting
 - Converting the MR controller drives to the Unconfigured Good state
 - Configuring the controller
 - Select an OS drive and set partitions
 - Configure Firmware Update
 - Reviewing your settings
 - Checking installation parameters
 - Creating RAID Volume on VROC (Virtual Raid on CPU)
 - Enabling the VROC
 - Creating the VROC RAID volume
 - About RAID arrays
 - RAID 0
 - RAID 1 and RAID 1+0 (RAID 10)
 - RAID 5
 - RAID 50

- RAID 6
- RAID 60
- Dedicated spare
- Failure spare activation
- Performing maintenance
 - Updating firmware
 - Determining the installed Intelligent Provisioning version
 - Setting Intelligent Provisioning preferences
 - Downloading Active Health System data
 - Downloading an Active Health System log
 - Uploading an AHS log to AHSV
 - Using deployment settings
 - Creating a deployment using Intelligent Provisioning
 - Using a deployment to configure a single server
 - Using the BIOS Configuration (RBSU) utility
 - About iLO Configuration
 - Administering
 - Resetting the options
 - Configuring intelligent storage
 - Creating a new array or logical drive using advanced mode
 - Configuring an array or logical drive
 - About Hardware Validation Tool
 - Using the hardware validation tool
 - About erasing data in Intelligent Provisioning
 - One-button secure erase
 - One-button secure erase access methods
 - Prerequisites for initiating the One-button secure erase process
 - Initiating the One-button secure erase process
 - Returning a system to operational state after One-button secure erase
 - Viewing the One-button secure erase report
 - One-button secure erase report details
 - Saving the One-button secure erase report to a CSV file
 - Deleting the One-button secure erase report
 - Impacts to the system after One-button secure erase completes
 - Hardware components that are reverted to the factory state
 - Hardware components that are not reverted to the factory state
 - One-button secure erase FAQ
 - Using System Erase and Reset
 - System Erase and Reset options
 - Creating a RAID configuration with SR Storage Administrator (SSA)
 - Using SSA

- SSA features
- Accessing SSA
- Configuration
- Diagnose
- Creating a RAID configuration with MR Storage Administrator (MRSA)
 - Using MRSA
 - MRSA features
 - Accessing MRSA
 - Controller dashboard
 - Controller configurations
- Using the USB Key Utility
- Troubleshooting
 - Troubleshooting general issues
 - iLO log on required during Intelligent Provisioning F10 boot
 - Intelligent Provisioning does not launch when F10 is pressed
 - Intelligent Provisioning does not reimage AOIP
 - Accessing version information in deployment settings
 - A browser does not import a deployment profile correctly
 - Cannot create a custom partition size
 - Intelligent Provisioning cannot launch One-Button secure erase
 - One-Button secure erase is unsuccessful or reports errors
 - One-Button secure erase succeeds but some drives are not erased
 - One-Button secure erase reports errors, but no specific details.
 - Troubleshooting Linux-specific issues
 - Assisted installation of Red Hat OS stops responding
 - Showing "Unable to install without the usb_storage driver loaded, Aborting",when upgrade or install with rpm
 - Unable to install Red Hat Enterprise Linux with secure boot enabled
 - Troubleshooting VMware-specific issues
 - Server reboots during VMware Assisted installation
- Websites
- Support and other resources
 - Accessing Hewlett Packard Enterprise Support
 - Accessing updates
 - Remote support
 - Warranty information
 - Regulatory information
 - Documentation feedback

Introduction



TIP

The information in this guide is for using Intelligent Provisioning with ProLiant Gen11 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>).

Subtopics

Intelligent Provisioning

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, and their enclosures. The same solution for HPE Synergy compute modules is now called Synergy Service Pack (SSP). These components are preloaded with a basic set of firmware and OS components that are installed along with Intelligent Provisioning.



IMPORTANT

HPE Synergy servers do not support OS 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 Intelligent Provisioning.
- From the iLO web interface, using Lifecycle Management. Lifecycle Management allows you to access Intelligent Provisioning without rebooting your server.



NOTE

1. HPE ProLiant RL3xx Gen 11 platforms do not support Intelligent Provisioning through both F10 and Lifecycle Management.
2. HPE Gen11 platforms running OpenBMC do not support Intelligent Provisioning.

Subtopics

F10/Remote console features

Always On Intelligent Provisioning (AoIP)

Intelligent Provisioning operation

Navigating Intelligent Provisioning

F10/Remote console features

F10/Remote console allows you to:

- Access SR Storage Administrator (SSA) for disk configuration.
- Access MR Storage Administrator (MRSA) for disk configuration from Intelligent Provisioning V4.30
- 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 (AoIP)

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 posted at <https://www.hpe.com/support/ilo-docs>.



NOTE

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

Intelligent Provisioning operation



NOTE

Intelligent Provisioning 4.00 and later requires iLO 6 firmware version 1.00 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 that the latest supported features are available.
- For ProLiant servers, firmware is updated using the Intelligent Provisioning Firmware Update utility.
- For HPE Synergy compute modules, firmware is updated using HPE OneView.
- 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

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

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

Icon	Function
	Enables you to select the language to use.
	Returns to the Intelligent Provisioning home page, with the Rapid Setup and Perform Maintenance menus. This icon is available only after completing the initial configuration and registration tasks.
	Displays the job configuration viewer screen, which displays the status of jobs in the queue. You can use this screen to monitor configuration tasks and jobs as they are processed.
	Opens the online help to the section about the current screen.
	Displays system information, including the Intelligent Provisioning version.
	Power down or reboot the server.
	Logs the current user out of Intelligent Provisioning. <div data-bbox="300 877 1481 1003">  NOTE This icon is only displayed in Always On mode. </div>
	Returns you to the previous screen after validating and saving your choices.
	Takes you forward to the next screen after validating and saving your choices.

Accessing Intelligent Provisioning

Different ways of accessing Intelligent Provisioning Home page:

Subtopics

[Accessing Intelligent Provisioning from the iLO web interface](#)

[Accessing Intelligent Provisioning using an iLO remote console session](#)

Accessing Intelligent Provisioning from the iLO web interface

Procedure

1. Open a browser.

2. Enter `https://<iLO host name or IP address>` to log on to the iLO web interface.
3. Enter a user account name and password, and click Log In.
4. From the navigation tree, click **Lifecycle Management**.
5. Navigate to the **Intelligent Provisioning** tab.
6. Click the **Always On** button.

Results

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.
2. Enter `https://<iLO host name or IP address>` to log on to the iLO web interface.
3. From the iLO web interface, navigate to the **Remote Console & Media** page.
4. Verify that your system meets the requirements for using the remote console application you want to use.
5. Click the launch button for your selected application.
 - `.Net Console`
 - `HTML5 Console`

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

6. Restart or power on the server.

The server restarts and the POST screen appears.
7. Press F10 when prompted during the server POST.
8. Select Intelligent Provisioning.

Results

If you are using Intelligent Provisioning for the first time, the **First Time Setup** wizard guides you through the 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.

Subtopics

[Selecting an F10 mode](#)

[Initial configuration in Intelligent Provisioning](#)

Selecting an F10 mode

About this task

Procedure

1. Boot the server.
2. On the POST screen, press
F10.
3. Perform one of the following steps based on the conditions:
 - Access Intelligent Provisioning directly, if Host Authentication is disabled in iLO.
 - Enter the credentials to access Intelligent Provisioning, if Host Authentication is enabled.

Initial configuration in Intelligent Provisioning

Basic configuration tasks for Intelligent Provisioning.

Subtopics

[Using the First Time Setup wizard](#)

[Re-enabling Intelligent Provisioning](#)

[Reinstalling Intelligent Provisioning](#)

Using the First Time Setup wizard

About this task

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.

Subtopics

[Entering First Time Wizard settings](#)

Entering First Time Wizard settings

About this task

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
 - 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

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.

Subtopics

[Reinstalling using an ISO image](#)

[Reinstalling using an RPM package \(Linux\)](#)

Reinstalling using an ISO image

About this task

Procedure

1. Download the ISO image file for the latest Intelligent Provisioning recovery media by clicking **Download** from the Intelligent Provisioning website (https://support.hpe.com/connect/s/softwaredetails?language=en_US&softwareId=MTX_0e528dc701d14e04864ba71f27).



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.
- Gen11 supports Intelligent Provisioning from 4.x

2. To download the ISO image file, complete the onscreen instructions.
3. Mount the ISO file in one of the following ways:

- Using iLO virtual media.



NOTE

When using iLO virtual media, the installation time depends on the network condition.

- 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 (See section [Using the USB Key Utility](#) for more information).
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/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. After the installation completes, reboot the server by pressing F10.

Reinstalling using an RPM package (Linux)

Prerequisites

- You have `gptfdisk`, `sdparm`, and `mdadm` for SLES 15.x.
- You have `sdparm` for RHEL 8.x.

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 hardware and installing an operating system

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

- [Selecting hardware settings](#)
- [Selecting the OS](#)
- [Reviewing your settings](#)

Subtopics

[Configuring the hardware and installing an OS with Intelligent Provisioning](#)

[Creating RAID Volume on VROC \(Virtual Raid on CPU\)](#)

[About RAID arrays](#)

Configuring the hardware and installing an OS with Intelligent Provisioning

About this task



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](#)

Subtopics

[Server support and special characters](#)

[Source media types and installation methods supported for each OS](#)

[Select install source](#)

[Configure Installation Settings](#)

[Reviewing your settings](#)

[Checking installation parameters](#)

Server support and special characters

- HPE Synergy Servers do not support OS installations with Intelligent Provisioning. These servers do support the maintenance features described in [Performing maintenance](#), except deploying the OS 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 path-name.

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. The installation process may fail to correctly identify such versions of the OS.
- Manual install is not supported in Intelligent Provisioning.

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 or action
File on a USB drive	Allows you to install an OS from a USB drive. <div>  NOTE <ul style="list-style-type: none"> This source is not supported in Always On Intelligent Provisioning mode. You must extract the ISO and put in the USB before the installation for RHEL and SLES. </div>
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: <ul style="list-style-type: none"> Server Name or IP Address —Server name or IP address of the server that hosts the OS contents. If a server name is specified, a DNS entry is also required. Share Name—The name of the network share using Server Message Block (SMB) protocol that hosts the OS contents. Domain Name(optional)- The path to directory or file. 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. Confirm Password (not encrypted)- Re-enter the password to avoid errors.
An anonymous FTP server	Allows you to install an OS through an FTP source. You need the following network connection information, including: <ul style="list-style-type: none"> 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. <div>  IMPORTANT <p>When entering an FTP path, remove spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).</p> </div>
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.

Subtopics

[Configure OS setting](#)

[Converting the MR controller drives to the Unconfigured Good state](#)

[Configuring the controller](#)

[Select an OS drive and set partitions](#)

[Configure Firmware Update](#)

Configure OS setting

Procedure

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

Supported OS families include:

- Microsoft Windows
- VMware vSphere Custom Image
- SUSE Linux Enterprise Server
- Red Hat Enterprise Linux



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 or Hyper-V Server Installation, it provides the following settings:
 - Operating System



TIP

Users can select different editions 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 Red Hat Enterprise Linux is not set up.

The default password for SUSE Linux Enterprise Server is `password`.

The default password for ESXi 7.x and 8.x is `_Passw0rd_`.

Converting the MR controller drives to the Unconfigured Good state

About this task

If the drives connected to the MR controller are in JBOD state, they cannot be used for RAID/array configuration. To create a RAID volume on any of the drives, convert them to the Unconfigured Good state. Converting the drives to the Unconfigured Good state is only required in MR controllers.

Procedure

1. Restart or power on the server.
2. Press F9 on the server POST screen.
The System Utilities screen appears.
3. On the System Utilities screen, select System Configuration.
4. To view the state of the drives attached to the MR controller, select MR Controller >Main Menu >Drive Management .
The list of all the drives with their respective states appears.
5. Select Main Menu >Configuration Management >Make Unconfigured Good.
6. Select the drives to be converted, and click OK.

7. Select Confirm and Yes to confirm the selection.

A success message appears.

8. Select OK.

Results

To ensure that the drive state has been changed to the `Unconfigured Good` state, perform step 4.
To return to the Intelligent Provisioning screen, select `> Embedded Applications > Intelligent Provisioning`.

Configuring the controller

About this task

In this page, the user can configure and allocate the disk space.

For configuring the drives in the MR controller, see [Converting the MR controller drives to the Unconfigured Good state](#).

On the OS installation summary page, Intelligent Provisioning checks the RAID and drive status and performs the following:

- If there is an existing logical drive on the hardware/software raid, then Intelligent Provisioning just displays the information.
- If there is no existing logical drive, then Intelligent Provisioning 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 Intelligent Provisioning automatically created.
 2. Array / Logical drive user created from the RSS.
- You cannot modify any existing array / logical drive on the server.



NOTE

If there is more than one RAID controller installed on the server, Intelligent Provisioning will automatically select the best RAID controller for configuration.

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 an OS drive and set partitions



About this task

In this page, the user can choose to perform manual partition, or let the OS 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 want you install the OS.

For manual partition:

- 1. Deselect the Use Recommended Partition check-box.

The following section displays the chart for the default partition. (The chart varies based on the OS and version.)

- 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 modify the Basic data partition, the rest of the partitions are also crucial for maintenance, and must 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	

While the user can only modify the /home partition, the rest of the partitions are crucial for maintenance and must not be changed.

- For Red Hat Enterprise Linux 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	



While the user can only modify the `/home` partition, the rest partitions are crucial for maintenance and must not be changed.



NOTE

- a. VMware does not allow manual partition
- b. When boot mode is switched to Legacy mode, manual partition is disabled for Windows or Hyper-V Server

2. To change the partition scheme, for Windows or Hyper-V systems:

- a. Click the cell that 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 or 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 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. You would 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, user can have the following choices:
 - `btrfs`
 - `ext2`
 - `ext3`
 - `ext4`
 - `vfat`
 - `xf`s
 - `swap`
- Partition Label

Then click the Create button to complete.

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

Configure Firmware Update

About this task

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

About this task



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.



NOTE

If firmware update is enabled, a popup for token authorization will be shown. Please follow the steps in [Firmware Update](#) section for detail.

Checking installation parameters

During the installation and configuration process, consider the following:

- A EULA might be displayed.
- If you attempt to deploy an OS on a server with no installed drives, it will show up an error message stating `Rapid Setup did not find any supported disk installed on this system`, 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.

Creating RAID Volume on VROC (Virtual Raid on CPU)

Steps for creating a RAID volume on VROC:

1. Enabling the VROC
- 2.. Creating the VROC RAID volume

Subtopics

[Enabling the VROC](#)

[Creating the VROC RAID volume](#)

Enabling the VROC

Procedure

1. Restart or Power on the server.
2. Press F9 on the server POST screen.

The System Utilities screen appears.
3. On the System Utilities screen, select System Configuration.
4. Select BIOS/Platform Configuration (RBSU).
5. Select Storage Options and click SATA Controller Options.
6. In Embedded SATA Configuration select the Intel VROC SATA Support.
7. Reboot the server.

Creating the VROC RAID volume

Procedure

1. Press F9 on the server POST screen.

The System Utilities screen appears.
2. On the System Utilities screen, select System Configuration.
3. Select the Intel VROC SATA controller.

The controller where you want to create the RAID.
4. Select Create RAID Volume.
5. Select the RAID level, disk and click Create Volume.

The RAID Volume is created.



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.

Subtopics

[RAID 0](#)

[RAID 1 and RAID 1+0 \(RAID 10\)](#)

[RAID 5](#)

[RAID 50](#)

[RAID 6](#)

[RAID 60](#)

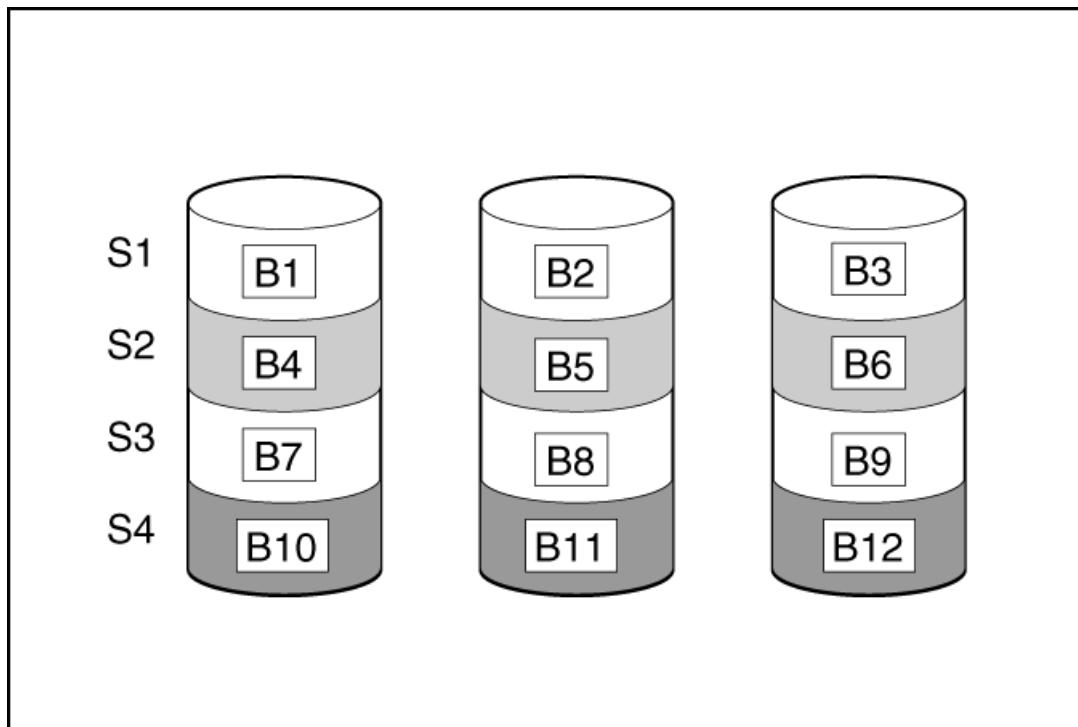
[Dedicated spare](#)

[Failure spare activation](#)

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.

The maximum number of drives supported for RAID 0 is 32.



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.

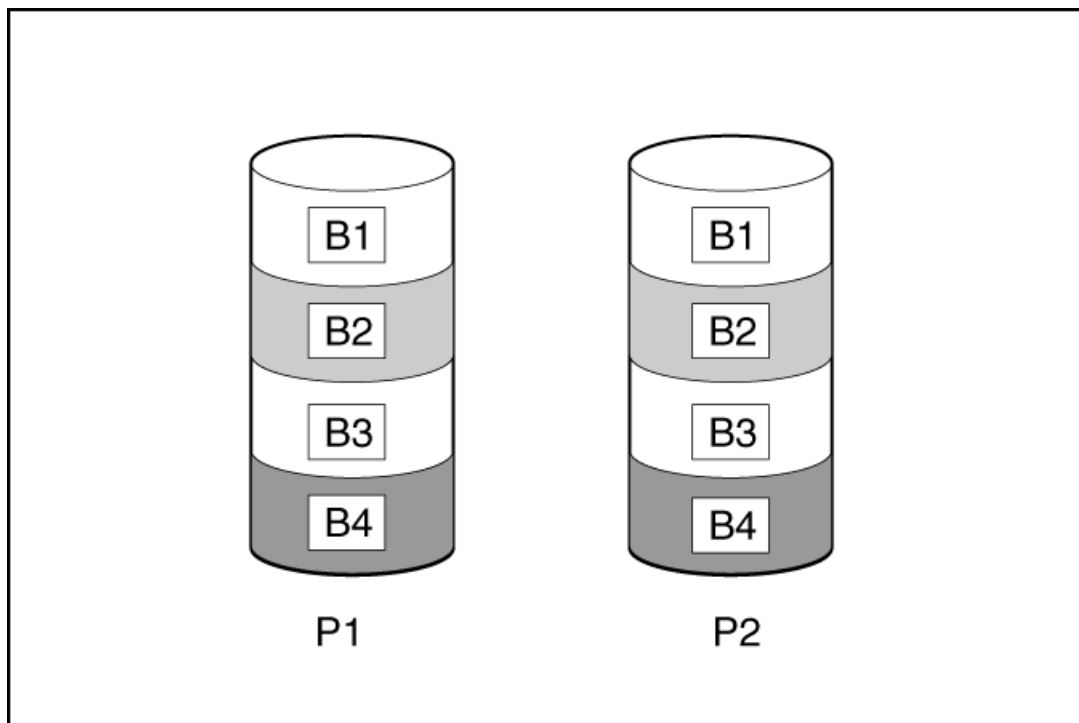
- It uses the entire drive capacity to store data (none allocated for fault tolerance).

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 $C \times (n / 2)$ where C is the drive capacity with n drives in the array. A minimum of two drives is required.

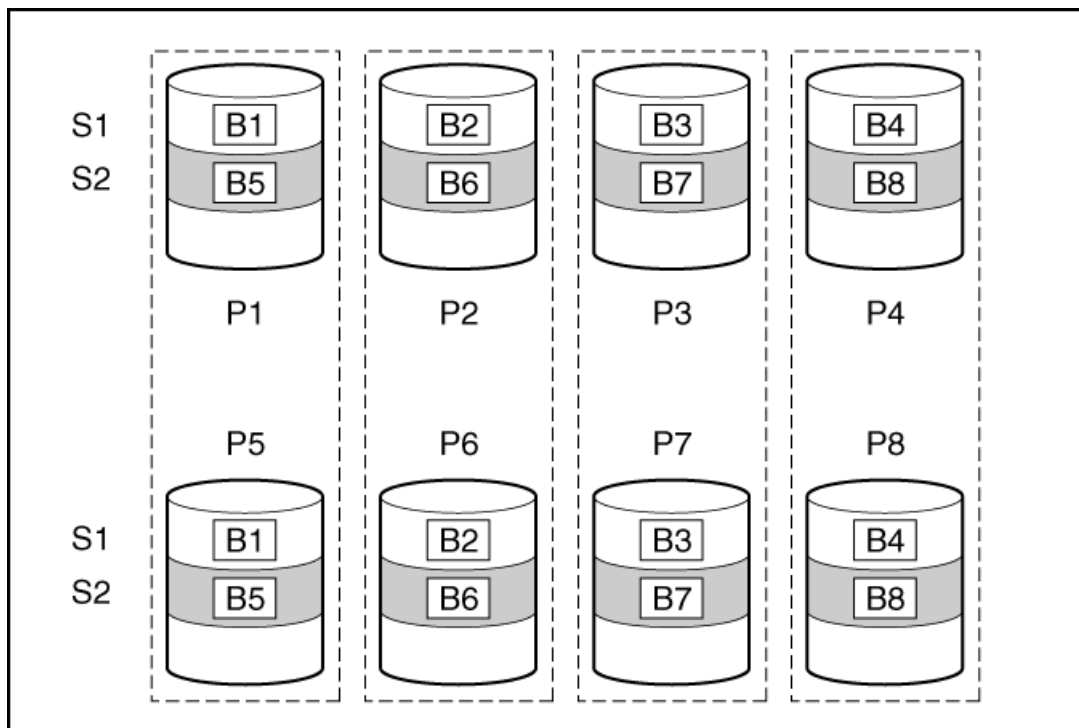
When the array contains only two physical drives, the fault-tolerance method is known as RAID 1.

The maximum number of drives supported for RAID 1 is 32.



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.

The maximum number of drives supported for RAID 10 is 32.



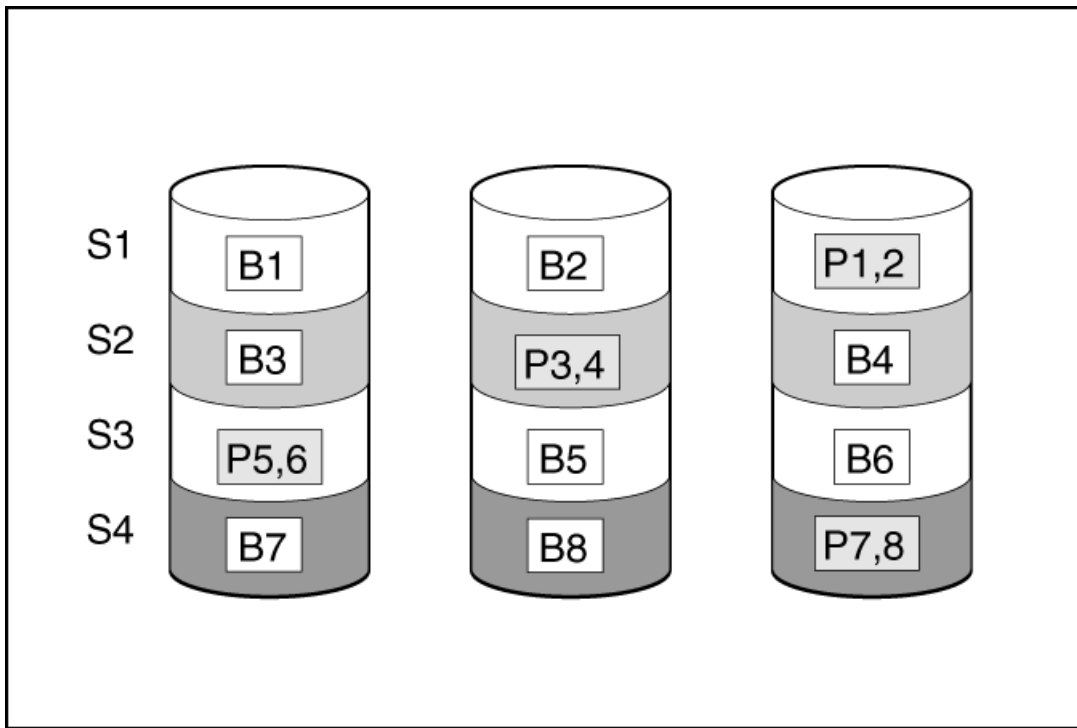
This method has the following benefits:

- It is useful when high performance and data protection are more important than usable capacity.
- This method has the highest write performance of any fault-tolerant configuration.
- No data is lost when a drive fails, as long as no failed drive is mirrored to another failed drive.
- Up to half of the physical drives in the array can fail.

RAID 5

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

The maximum number of drives supported for RAID 5 is 32.

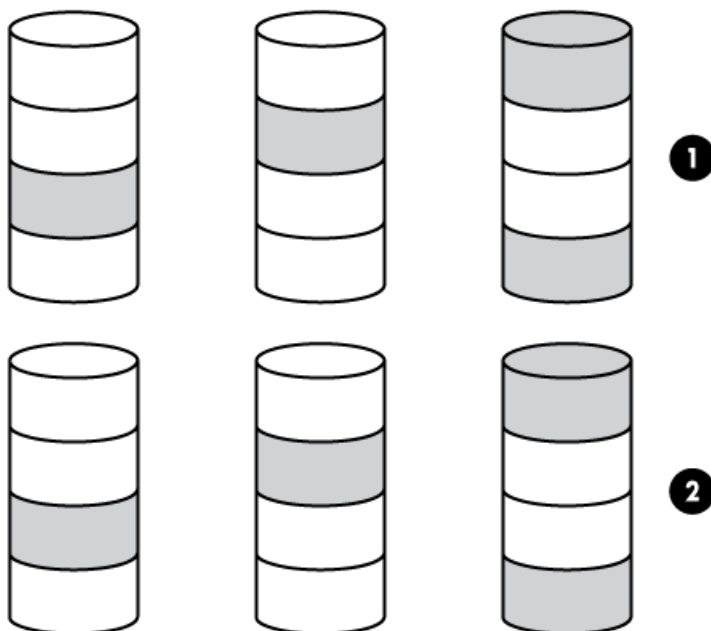


This method has the following benefits:

- 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.

The maximum number of drives supported for RAID 50 is 256.

This method has the following benefits:

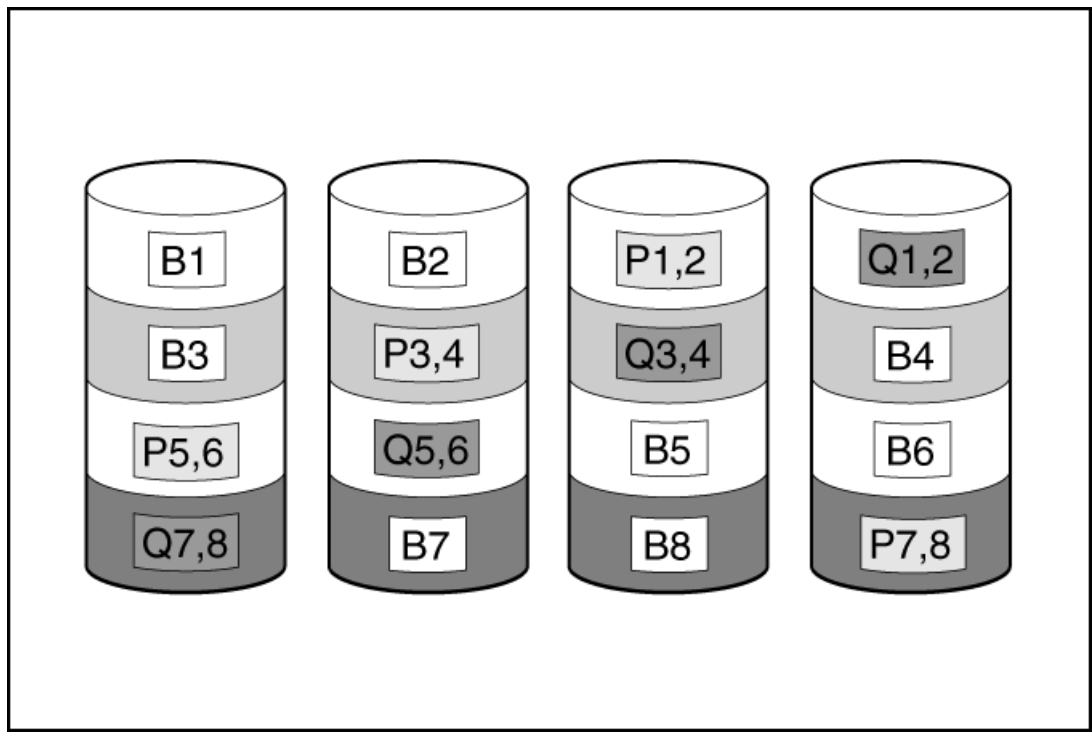
- Higher performance than for RAID 5, especially during writes.
- Better fault tolerance than either RAID 0 or RAID 5.
- Up to n physical drives can fail (where n is the number of parity groups) without loss of data, as long as the failed drives are in different parity groups.

RAID 6

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

A minimum of 4 drives is required.

The maximum number of drives supported for RAID 6 is 32.



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.

The maximum number of drives supported for RAID 60 is 256.

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

A dedicated spare is a spare drive that is dedicated to one array.

A dedicated spare is a spare drive that is shared across multiple arrays within a single RAID controller.

It supports any fault tolerant logical drive such as RAID 1, 10, 5, 6, 50, 60, and CacheCade SSD volumes.

It supports any fault tolerant logical drive such as RAID 1, 10, 5, 6, 50, and 60.

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.

Subtopics

[Updating firmware](#)

[Setting Intelligent Provisioning preferences](#)

[Downloading Active Health System data](#)

[Using deployment settings](#)

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

[About iLO Configuration](#)

[Configuring intelligent storage](#)

[About Hardware Validation Tool](#)

[About erasing data in Intelligent Provisioning](#)

[One-button secure erase](#)

[Using System Erase and Reset](#)

[Creating a RAID configuration with SR Storage Administrator \(SSA\)](#)

[Creating a RAID configuration with MR Storage Administrator \(MRSA\)](#)

Updating firmware

Prerequisites

1. To update firmware, make sure that port 443 is open for SSL communication.
2. Generate token by the following steps:
 - a. Go to the following website, log in and generate token: <https://support.hpe.com/hpsc/swd/entitlement-token-service/generate>
 - b. If you are using embedded IP, then create a text file named `user_token.txt`. Store only the user token string into the text file (without inserting a new line), then put the text file into the USB and plug-in to the server.

About this task

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.

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 results to appear. 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>.

4. Select one of the following:

- Newest firmware available

Displays a list of available firmware update items for this machine. appears.

- Rollback to previous

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



NOTE

The user must upload the 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. Select the USB that contains user token file or copy-paste to the input area.
7. The selected items appear on the Job Configuration Viewer screen.
8. Do one of the following:
 - Launch Now
 - Add another job
9. Click **Reboot** at the completion of the firmware update process.

Subtopics

Determining the installed Intelligent Provisioning version

Determining the installed Intelligent Provisioning version

To select the Intelligent Provisioning version, click the **System Information**  and select the required Intelligent Provisioning version.

Setting Intelligent Provisioning preferences

About this task

Use Intelligent Provisioning Preferences to modify 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 - This is always 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:

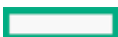
- Choose network interface for updates and installs
- Use Proxy, and provide proxy details.
- DHCP Auto-Configuration, `IPv4/IPv6` switch and provide the configuration details.

4. Click Submit.

Results

When Intelligent Provisioning is run for the first time on a server, it 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



About this task

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.

Subtopics

[Downloading an Active Health System log](#)

[Uploading an AHS log to AHSV](#)

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 10–15 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.

After the data has been downloaded, upload it to the Active Health System Viewer.

Uploading an AHS log to 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.

About this task

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.

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

Information on how to:

- Create a deployment profile/package
- Configure a server using an existing deployment profile

Subtopics

[Creating a deployment using Intelligent Provisioning](#)

[Using a deployment to configure a single server](#)


Creating a deployment using Intelligent Provisioning

About this task

The Intelligent Provisioning Deployment Settings page enables you to create deployments or 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.

Procedure



1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Deployment Settings** from the maintenance options.
3. On the **Deployment Settings** screen, do one of the following:
 - a. To create a new customized profile, click **Create New Deployment**, and navigate the deployment settings screens to complete the settings in the following steps.
 - b. To edit an existing customized profile, click  (**Edit**).
4. Enter a **Deployment Name**—Enter a name for this deployment package. Do not include spaces or special characters.

**NOTE**

Steps 5–10 below, although optional make your deployment profile more precise, resulting in a sound server configuration.

5. (Optional) Enter **User Notes and Captured From** details.
6. (Optional) Enter an **Operating System**:
 - a. Click **Create** button.
 - b. Select the **Install source**.
 - c. Select the **Install media or OS type**.
 - d. Configure **OS settings**.

For example, in a VMware OS and a virtual media source, you could enter a URL of the format: http://x.x.y.z/Repo/OS_Images/VMware-ESXi-7.0.3-19035710-HPE-703.0.0.10.8.1.1-Dec2022.iso
 - e. Select **Use Automation Controller Setting** or not.
 - f. Configure the **partition table**.
 - g. Click **Save** button if everything is correct.
7. (Optional) Enter the **ROM Settings**
8. (Optional) Enter the **Storage Controller Settings**
9. (Optional) Enter **Intelligent Provisioning Preferences**
10. (Optional) Enter **Hardware Validation Tool**— Select **Hardware Validation Tool** options for each deployment.
11. Click **Save** to save the profile.

For more information on how to access intelligent provisioning, see [Accessing Intelligent Provisioning](#)

Using a deployment to configure a single server

Prerequisites

You have a deployment (settings profile or package) available with you on your current server or on a server over the network, or on a USB drive.


About this task

**IMPORTANT**

Do not interrupt the configuration process.

Procedure

Do one of the following:

1. To use the deployment you created on the same server, click  (Deploy).
2. To use a previously created deployment that does not exist on this server:

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
 - a. Insert the USB key containing the deployment.
 - b. Select the deployment from USB and click Next.
 - c. Click Deploy.



NOTE

The newly imported deployment is added with the prefix "New Import".

Using the BIOS Configuration (RBSU) utility

About this task

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 for HPE ProLiant Gen11 Servers and HPE Synergy posted at <https://www.hpe.com/support/UEFIGen11-UG-en>.

For example, you can update:

- 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.

Procedure

1. On the Intelligent Provisioning Home screen, click **Perform Maintenance**.
2. 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
3. To reset the BIOS for this server, click **Reset BIOS** drop-down menu.
4. To update the workload profile, click to open **Workload Profile** drop-down menu.
5. To change RBSU configurations, select from the menu on the left, and then select the section that contains the configuration you want to change.
6. To save changes, click **Update**.
7. 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 Settings button to update.

For Administrator and Rest, see the following sections.

Subtopics

[Administering](#)

[Resetting the options](#)

Administering

Procedure

1. From the Intelligent Provisioning home page, click Perform Maintenance > iLO Configuration > Administration.
2. Configure the following settings:

- View user permissions
- Create account
- Edit account
- Delete account
- Available permissions are listed as follows:
 - Login: Enables 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 Generate NMI to System button.
 - Host BIOS: Enables a user to configure the host BIOS settings by using the UEFI System Utilities. This privilege is required for replacing the active system ROM with the redundant system ROM.

This privilege does not affect configuration through host-based utilities.

- Administer User Accounts: Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you are not assigned this privilege, you can view your own settings and change your own password. For more information, see HPE iLO 6 User Guide posted at <https://www.hpe.com/support/ilo-docs>.
 - Host Storage: Enables a user to configure to host storage settings.
- This privilege does not affect configuration through host-based utilities.
- Remote Console: Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
 - Virtual Media: Enables a user to use the Virtual Media feature 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.

After iLO is configured, revoking this privilege from all users prevents reconfiguration from the following interfaces:

- iLO web interface
- iLO RESTful API
- CLI
- HPQLOCFG

Users who have access to the following interfaces can still reconfigure iLO:

- UEFI System Utilities
- HPONCFG

Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- o Host NIC: Enables a user to configure the host NIC settings.

This privilege does not affect configuration through host-based utilities.

- o Recovery Set: Enables a user to manage the System Recovery Set.

By default, the Recovery Set privilege is assigned to the default Administrator account. This privilege can be added to a user account only by creating or editing the account with an account that already has this privilege.

If there is no user account with the Recovery Set privilege, and an account with this privilege is required, reset the management processor to the factory default settings. The factory default reset creates a default Administrator account with the Recovery Set privilege.

This privilege is not available when iLO security is disabled with the system maintenance switch.

The following privileges are not available through the CLI or RIBCL scripts:

- Host NIC
- Host Storage
- Recovery Set
- Host BIOS
- Login

The following privileges are not available through the iLO 6 Configuration Utility in the UEFI System Utilities:

- Recovery Set
- Login

3. Click Update User button to save configuration.

Resetting the options

Procedure

1. From the Intelligent Provisioning home 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



NOTE

The configuration tab is not available for MR controllers.

For configuring the drives in the MR controller, see [Converting the MR controller drives to the Unconfigured Good state](#).

Subtopics

[Creating a new array or logical drive using advanced mode](#)
[Configuring an array or logical drive](#)

Creating a new array or logical drive using advanced mode

Procedure

1. Click + Create Array.
2. Check the hard drives in the list, then click **Next** to go to next page.
3. Enter a Logical Drive Name.
4. Select a RAID Mode.
5. Select a Stripe Size (KB).
6. Select RAID Size (GB).
7. Select a Legacy Boot Priority, then click the **Right Arrow** to go to next page.
8. In the Summary page, review the array settings.
9. Click Done. The Storage Configuration main page appears, displaying the following message `The operation will execute on the next reboot`.
10. Reboot the machine and let the operation take effect.

Configuring an array or logical drive

Procedure

1. From the main Intelligent Provisioning window, click **Perform Maintenance > Intelligent Storage Configuration > Configuration**.
Intelligent Provisioning takes you to the General configuration page.
2. 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

Subtopics

[Using the hardware validation tool](#)

Using the hardware validation tool



Procedure

1. From the main menu, click Perform Maintenance.
2. Click Hardware Validation Tool.

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

3. After discovery finishes, the tool displays the test results.
4. 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.
 - Integrated Management Log (IML) - Displays the log list.



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



CAUTION

One-button secure erase and System Erase and Reset should be used with extreme caution, and only when a system is being decommissioned. Both utilities will securely erase all accessible block SAN, local storage disks or volumes including D3940 for Synergy. Then each will reset all internal non-volatile devices such as SAS/SATA/NVMe storage, BIOS, and iLO settings and so on. In the case of One-Button Secure Erase, it will remove the HPE Intelligent Provisioning thus requiring software reinstallation.

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

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 that 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 NVMe 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.

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.

One-button secure erase

If you want to decommission a server or prepare it for a different use, you can use the One-button secure erase feature.

One-button secure erase follows the NIST Special Publication 800-88 Revision 1 in the [Guidelines for Media Sanitization guide](#). The appendix recommends minimum sanitization levels for media. For more information about the specification, see Section 2.5, [Guidelines for Media Sanitization](#).

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 that you follow in the Statement of Volatility document for a server.

Subtopics

[One-button secure erase access methods](#)

[Prerequisites for initiating the One-button secure erase process](#)

[Initiating the One-button secure erase process](#)

[Returning a system to operational state after One-button secure erase](#)

[Viewing the One-button secure erase report](#)

[Saving the One-button secure erase report to a CSV file](#)

[Deleting the One-button secure erase report](#)

[Impacts to the system after One-button secure erase completes](#)

[One-button secure erase FAQ](#)

One-button secure erase access methods

You can initiate the One-button secure erase process from the following products:

- iLO

- Intelligent Provisioning
- The iLO RESTful API and iLOREST

This topic describes the One-button secure erase access methods using Intelligent Provisioning.

Prerequisites for initiating the One-button secure erase process

Prerequisites

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 6 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.

- Verify that your iLO user account is assigned all the iLO user account privileges including recovery set.
- Install an iLO license that supports this feature.

For information about the available license types and the features they support, see the licensing documentation at the following website: <https://www.hpe.com/support/ilo-docs>.

- If the following features are enabled, disable them:

- Server Configuration Lock

For instructions, see the [UEFI System Utilities user guide and HPE Synergy](#).

For instructions, see the [UEFI System Utilities user guide](#).

- Smart Array Encryption

For instructions, see the "Clearing the encryption configuration" section in the [HPE Smart Array SR Secure Encryption Installation and User Guide](#).

For instructions, see the instructions for clearing the encryption configuration in the Secure Encryption installation and user guide.

- Intel VROC Encryption

For instructions, see the [Cleaning the security and encryption configurations](#) section in the [Intel Virtual RAID on CPU for HPE Gen 10 Plus User Guide](#)

- For instructions, see the [Cleaning the security and encryption configurations](#) section in the [Intel Virtual RAID on CPU User Guide](#).

- On HPE Synergy systems, remove HPE OneView or Virtual Connect profiles assigned to the system.
- Verify that the iLO security setting on the system maintenance switch is in the OFF position.
- The storage drives that you want to erase 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.

If an attached storage device does not support native sanitize methods, it will not be erased during the One-button secure erase process. An Integrated Management Log (IML) entry will report an erase failure for the device.

- Hewlett Packard Enterprise recommends disconnecting or detaching the removable drives, external storage, or shared storage that you do not want to erase.

- Hewlett Packard Enterprise recommends configuring SNMP alerts, Mail Settings, or iLO RESTful API alerts before initiating the One-button secure erase process.

If errors occur when individual components are erased, an IML entry is logged for each error. You can review the IML log using SNMP alerts, Mail Settings, or iLO RESTful API alerts. The IML is erased later during the One-button secure erase process. After the IML is erased, high-level status information is provided in the secure erase report.

- If you use LDAP Directory Authentication with the HPE Extended Schema, you have another method for logging in to iLO to initiate the One-button secure erase process.

Supported methods include local accounts, Kerberos authentication, CAC Smartcard, and schema-free directory accounts.

The HPE Extended Schema does not support the user privileges required to initiate the One-button secure erase process.

- Disable Microsoft® Secured-core Support.

Initiating the One-button secure erase process

Prerequisites

Your environment meets the [Prerequisites for initiating the One-button secure erase process](#).



CAUTION

Use this feature only when you want to decommission a system or use it for a different purpose. This process resets the server and supported components to the factory state. Depending on the storage capacity, securely erasing the server and components might take up to a day or more to finish. After you initiate this process, it cannot be undone. Until the process is complete, avoid interactions with iLO or the system that involves configuration changes and powering off the system.

Procedure

1. From the Intelligent Provisioning screen, click Perform Maintenance > One button secure erase and then follow the onscreen prompts to begin erasing the system.

The One-button secure erase process begins after the server is restarted. During booting, BIOS deletes the data that it controls. After BIOS completes the process, the server is powered 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. You receive a notification if you configured SNMP, AlertMail, or Redfish alerts. The IML is erased later during the One button secure erase process.

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. To view the detailed erase report, see [Viewing the One-button secure erase report](#)

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

2. (Optional) [Returning a system to operational state after One-button secure erase](#).

3. (Optional) View, save, or delete the One-button secure erase report.

Hewlett Packard Enterprise recommends completing this step.

4. (Optional) If a device failed the erase process, or the device does not support a native sanitize method, do one of the following:

- Isolate these devices and use other methods to delete the data.
- Securely dispose of the devices according to your organization security policies.

Hewlett Packard Enterprise recommends completing this step.

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

About this task

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 6 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 6 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 6 User Guide](#).

Viewing the One-button secure erase report

Prerequisites



NOTE

The One-button secure erase report can only be accessed from iLO.

- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.

If the One-button secure erase process completed on the server, the View Last Erase Report button is available.

2. Click View Last Erase Report.

The Secure Erase Report is displayed.

3. (Optional) To sort by a table column, click the column heading.

To change the sort order to ascending or descending, click the column heading again or click the arrow icon next to the column heading.

4. (Optional) [Saving the One-button secure erase report to a CSV file](#).

Hewlett Packard Enterprise recommends saving a copy of the erase report for future reference.

5. (Optional) [Deleting the One-button secure erase report](#).

Hewlett Packard Enterprise recommends deleting the erase report before decommissioning a server or using it for a different purpose.

One-button secure erase report details

- **Server Serial Number**—The server serial number.
- **Initiated By**—The user who initiated the One-button secure erase process.

The following information is listed for each device type:

- **Device Type**—The device type that was erased.
For information about the affected device types, see [Impacts to the system after One-button secure erase completes](#).
- **Location**—The location of the device in the server.
- **Serial Number**—The device serial number.
- **Status**—The One-button secure erase status for the device.
- **Erase Type**—The type of erase operation. For more information about the operations that were performed, see [One-button secure erase FAQ](#).
- **Start Time**—The One-button secure erase start time for the specific device.
- **End Time**—The One-button secure erase end time for the specific device.

Saving the One-button secure erase report to a CSV file

Prerequisites



NOTE


The One-button secure erase report can only be accessed from iLO.

- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.

About this task

When you use the One-button secure erase feature, Hewlett Packard Enterprise recommends saving a copy of the erase report for future reference.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.
2. Click .
- The CSV Output window is displayed.
3. Click Save, and then follow the browser prompts to save or open the file.

Deleting the One-button secure erase report

Prerequisites



NOTE

The One-button secure erase report can only be accessed from iLO.

- Configure iLO Settings privilege
- The One-button secure erase process completed on the server.
- After the One-button secure erase process completed, iLO was configured with an IP address.
- If you want a copy of the One-button secure erase report for future reference, you saved the report.

About this task

When you decommission or repurpose a server, you might not want the One-button secure erase report to remain available in the iLO web interface.

Hewlett Packard Enterprise recommends deleting the erase report before decommissioning a server or using it for a different purpose.

Procedure

1. Click Lifecycle Management in the navigation tree, and then click the Decommission tab.

If the One-button secure erase process completed on the server, the View Last Erase Report button is available.

2. Click View Last Erase Report.

The Secure Erase Report is displayed.

3. Click .

iLO securely erases the report file, and then resets immediately.

The event log, IML, security log, and configuration settings made up to this point are reset to the factory default settings. iLO might attempt an auto-restore operation when it starts.

Impacts to the system after One-button secure erase completes

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

- All data on the impacted storage drives and Persistent Memory are erased and not recoverable. All RAID settings, disk partitions, and OS installations are removed.

The following BIOS and iLO 6 settings are erased or reset to the factory default settings.

- Factory provisioned server identity (iLO IDevID), User defined server identity (iLO LDevID), and Factory provisioned TCG compliant system identity (System IDevID) are erased.
- Platform certificate, System IAK certificate, and all other enrolled certificates (other than factory preinstalled UEFI Secure boot certificates are erased.
- iLO network and other settings are erased and must be reconfigured.
- Installed iLO licenses are removed and the license status reverts to iLO Standard.

If the iLO Advanced license is preinstalled at the factory with the #0D1 option, the license is reinstated when the One-button secure erase process is finished. For more information about this license option, see the HPE iLO Licensing Guide.

- 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, Security 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.

Subtopics

Hardware components that are reverted to the factory state

Hardware components that are not reverted to the factory state

Hardware components that are reverted to the factory state

The following components are reverted to the factory state during the One-button secure erase process.

- UEFI Configuration store
- RTC (System Date and Time)
- Trusted Platform Module
- NVRAM
 - BIOS Settings
 - iLO configuration settings
 - iLO Event Log
 - Integrated Management Log
 - Security Log
- HPE SR controllers, MR controllers, NS controllers and connected storage drives.

For more information about controllers, see, "Supported storage products" section in the iLO six User Guide.

- Intel VROC
- Drive data (for drives that support native sanitize methods).
 - SATA, SAS drives (SSD and HDD)
 - NVMe Express
- Embedded Flash
 - iLO RESTful API datums
 - Active Health System
 - Firmware repository

Hardware components that are not reverted to the factory state

One-button secure erase process does not affect the following components:

- USB drives
- SD cards
- iLO virtual media
- Configuration on PCI controllers
- SAS HBAs and connected drives
- SATA, SAS, and NVMe Express drives that do not support native sanitize methods.
- FCoE, iSCSI storage
- 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?

HPE SR, MR, and NS controllers are supported for One-button secure erase.

Does Smart Array erase drives that do not support Purge?

RAID controllers can wipe drives (overwrite with a pattern) that do not support the purge operation. One-button secure erase does not request the controller to perform this nonsecure wipe. To wipe data on such drives, use the Intelligent Provisioning “System Erase and Reset” feature.

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 must 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, One-button secure erase does not delete these items.

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.



Device	Operation requested	Result
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.
UEFI configuration store	3-pass: Chips 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.
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.	<ul style="list-style-type: none"> 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 following for operations requested on the drives.
HPE Smart Array MR controllers	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	<ul style="list-style-type: none"> All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. Encryption keys are cleared. 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 following for operations requested on the drives.

Device	Operation requested	Result
HPE NS Boot Controller	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	<ul style="list-style-type: none"> All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. <p>All attached drives are requested to be sanitized. See following for operations requested on the drives.</p>
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 One-button secure erase FAQ 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	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	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.
	NVM Express SANITIZE if supported (for drives supporting NVM Express version 1.3 or later).	All data and metadata associated with all namespaces is destroyed. All user content present in the NVM subsystem is erased.
	A single pass of NVM Express FORMAT with SES = 1	This option is used if the drive does not support SANITIZE.

¹ These drives might be connected to the HPE “SR and MR” controllers or the Chipset SATA controller.

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.

Using System Erase and Reset

Use System Erase and Reset to clear hard drives and reset the 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 did not support the native sanitize methods used by One-button secure erase.

Subtopics

[System Erase and Reset options](#)

System Erase and Reset options

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

Option	Description
All Hard Drives and Solid State Drives	Erase all hard drives and solid state drives on this server. <div> NOTE<ul style="list-style-type: none">Only supported in F10 mode, not supported in Always On Intelligent Provisioning.When there is no hard drive or solid state drive installed in the system, then this function will become unavailable.A hard drive or solid state drive attached to a software RAID controller cannot be erased.</div>
Secure Erase	Writes a data pattern over all drive sectors. This action might take several hours. <div> NOTE<p>Only available if you select All Hard Drives.</p></div>
Intelligent Provisioning Preferences	Clear Intelligent Provisioning preferences.
Active Health System logs	Clears all AHS log files.

Creating a RAID configuration with SR Storage Administrator (SSA)

The following section introduces the concept of SSA.

Subtopics

- [Using SSA](#)
- [SSA features](#)
- [Accessing SSA](#)
- [Configuration](#)
- [Diagnose](#)



Using 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

About this task

- **SSA can be launched from F10**
Press F10 and Select SR Storage Administrator from the menu.

The Smart Storage Administrator window is displayed.
- **Launching SSA from Intelligent Provisioning Home Screen**
 1. On the Intelligent Provisioning home screen, click Perform Maintenance
 2. Select SR Storage Administrator 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.

Creating a RAID configuration with MR Storage Administrator (MRSA)

The following section introduces the concept of SSA.

Subtopics

[Using MRSA](#)

[MRSA features](#)

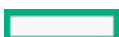
[Accessing MRSA](#)

[Controller dashboard](#)

[Controller configurations](#)

Using MRSA

MRSA provides high-availability configuration, management, and diagnostic capabilities for all MegaRaid products



MRSA features

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

- 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 modes of operation, enabling faster configuration or greater control over the configuration options.
- Displays onscreen tips for individual steps of a configuration procedure.
- Monitors the activities and performance of the server and all the controller cards attached to it.
- Displays information related to drive failures, device failures, and so on
- GUI (Graphical user interface) helps you to view, create, and manage storage configurations.

Accessing MRSA

Launching MRSA:

- **MRSA can be launched from F10**

Press F10 and, select MR Storage Administrator from the menu.

The MR Storage Administrator window appears.

- **Launching MRSA from Intelligent Provisioning Home Screen**

1. On the Intelligent Provisioning home screen, click Perform Maintenance.
2. Select MR Storage Administrator from the maintenance options.

The MR Storage Administrator window appears.

- **Download Support Logs from the MR controllers:**

1. Select Download Support Log inside the MRSA utility.
2. Select Confirm and then click Yes Download.

A Pop up window will open.

3. Select Save file and then click Ok.

You will be directed to the "media" folder where connected USB drives are listed. The drive can be identified by the volume label.

4. Select the drive and click Save.



NOTE

VFAT , EXT4 and HPFS/NTFS/exFAT all work as file systems for the USB key.

Controller dashboard

You can perform controller related actions and view all the information pertaining to a controller from the Controller Dashboard.

The controller Dashboard contains:

1. **Controller Summary:** Displays the name of the MegaRAID controller card, basic controller properties, such as the controller serial

number, vendor ID, SAS address, driver version, device ID, host interface.

2. **Controller Views:** Displays all the configured arrays, logical drives, and drives associated with the selected controller card. It also displays the hardware, such as enclosures and backplanes associated with the controller.
3. **Controller Actions:** Lets you perform the following actions:
 - Create a configuration
 - Clear a configuration
 - Update the controller firmware
 - Import or clear foreign configurations
 - View premium features
 - View the event log

Controller configurations

You can use the MR Storage Administrator application to create and modify storage configurations on systems with Hewlett Packard Enterprise controllers.

Two types of configurations can be created :

- **Simple Configuration:** The simple configuration option is the quickest and easiest way to create a storage configuration. When you select simple configuration mode, the system creates the best configuration possible using the available drives.

To create a simple configuration.

1. Select Configure > Simple Configuration from the Server Dashboard or the Controller Dashboard.

The Simple Configuration page opens.

- **Advanced Configuration:** The advanced configuration option provides an easy way to create a storage configuration. It gives you greater flexibility than simple configuration because you can select the drives and the logical drive parameters when you create a logical drive. In addition, an advanced configuration procedure to create spanned arrays.

To create an advanced configuration.

1. Select Configure > Advanced Configuration from the Server Dashboard or the Controller Dashboard.

The Advanced Configuration page opens.

For more information, see the **HPE MR Storage Administrator User Guide** posted at https://support.hpe.com/hpesc/public/docDisplay?docId=a00048286en_us

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.

Subtopics

[Prerequisites](#)

[Creating a bootable USB key](#)

[Adding content to a bootable USB key](#)

Troubleshooting

Subtopics

[Troubleshooting general issues](#)

[Troubleshooting Linux-specific issues](#)

[Troubleshooting VMware-specific issues](#)

Troubleshooting general issues

Commonly encountered errors and information on how to troubleshoot them.

Subtopics

[iLO log on required during Intelligent Provisioning F10 boot](#)

[Intelligent Provisioning does not launch when F10 is pressed](#)

[Intelligent Provisioning does not reimage AOIP](#)

[Accessing version information in deployment settings](#)

[A browser does not import a deployment profile correctly](#)

[Cannot create a custom partition size](#)

[Intelligent Provisioning cannot launch One-Button secure erase](#)

[One-Button secure erase is unsuccessful or reports errors](#)

[One-Button secure erase succeeds but some drives are not erased](#)

[One-Button secure erase reports errors, but no specific details.](#)

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 from Grub menu.

Action

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

```
linuxefi /IP4.00/vmlinuz media=net splash quiet  
isol=http://192.168.100.101/iso/IP330.2019_0103.230.iso  
isolmnt=/mnt/bootdevice nicmac=5c:b9:01:c5:43:d0 install  
echo 'Loading initial Ramdisk...'  
initrdefi /IP4.00/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.

Cannot create a custom partition size

Symptom

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

Action

The user is allowed to perform manual partition before the OS installation begins. However, manual partition is not supported for all the versions of VMware.

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.

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

One-button secure erase does not support certain components. For example:

- 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 the data that One-button secure erase purges.

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

Symptom

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

Cause

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

Action

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

Troubleshooting Linux-specific issues

Commonly encountered Linux specific errors and information on how to troubleshoot them.

Subtopics

[Assisted installation of Red Hat OS stops responding](#)



Assisted installation of Red Hat OS stops responding

Symptom

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

- The installation stops responding during reboot and a `The Red Hat Enterprise Linux Server CD was not found` error is displayed.
- The installation stops responding 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

Commonly encountered VMware specific errors and information on how to troubleshoot them.

Subtopics

[Server reboots during VMware Assisted installation](#)

Server reboots during VMware Assisted installation

Symptom

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

Cause

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

Action

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

Websites

Intelligent Provisioning	https://www.hpe.com/servers/intelligentprovisioning
HPE Support Center	https://www.hpe.com/support/hpesc
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

Subtopics

[Accessing Hewlett Packard Enterprise Support](#)

[Accessing updates](#)

[Remote support](#)

[Warranty information](#)

[Regulatory information](#)

[Documentation feedback](#)

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 OnePass set up with relevant entitlements.

Remote support

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

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

HPE Get Connected

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

HPE Tech Care Service

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

HPE Complete Care Service

<https://www.hpe.com/services/completecure>

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, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (<https://www.hpe.com/support/hpesc>) to send any errors, suggestions, or comments. This process captures all document information.

