



Intelligent Provisioning 3.89 User Guide for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy

Part Number: 30-68E7D0AB-002c
Published: July 2026
Edition: 5

Intelligent Provisioning 3.89 User Guide for HPE ProLiant Gen10, ProLiant Gen10 Plus Servers, and HPE Synergy

Abstract

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

Part Number: 30-68E7D0AB-002c

Published: July 2026

Edition: 5

© Copyright 2017–2026 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.....	6
Intelligent Provisioning.....	6
F10/Remote console features.....	7
Always On Intelligent Provisioning (AoIP).....	7
Intelligent Provisioning operation.....	8
Navigating Intelligent Provisioning	9
Accessing Intelligent Provisioning	10
Accessing Intelligent Provisioning from the iLO web interface	10
Accessing Intelligent Provisioning using an iLO remote console session.....	11
F10 mode options.....	11
Selecting an F10 mode.....	12
Initial configuration in Intelligent Provisioning.....	12
Using the first time setup wizard.....	13
Entering First Time Wizard settings.....	13
Re-enabling Intelligent Provisioning.....	14
Reinstalling Intelligent Provisioning	15
Reinstalling using an ISO image.....	15
Reinstalling using an RPM package (Linux).....	16
Configuring the hardware and installing an operating system	17
Configuring the hardware and installing an OS with Intelligent Provisioning.....	17
Server support and special characters.....	18
Source media types and installation methods supported for each OS.....	18
Select install source.....	18
Configure Installation Settings.....	20
Configure OS setting.....	21
Converting the MR controller drives to the Unconfigured Good state.....	22
Configuring the controller	23
Select an OS drive and set partitions.....	24
Configure Firmware Update.....	27
Reviewing your settings.....	28
Checking installation parameters.....	28
Dedicated spare.....	29
Failure spare activation.....	29
Performing maintenance.....	29

Updating firmware	30
Determining the installed Intelligent Provisioning version.....	32
Setting Intelligent Provisioning Preferences	32
Downloading Active Health System data	33
Downloading an Active Health System log.....	34
Uploading an AHS log to AHSV.....	35
Using deployment settings	36
Creating a Deployment Settings package.....	36
Using Deployment Settings package to configure a single server.....	37
Deployment Settings actions.....	38
Using the BIOS Configuration (RBSU) utility.....	39
About iLO Configuration.....	40
Administering.....	41
Resetting the options.....	43
Configuring intelligent storage.....	44
Creating a new array or logical drive using advanced mode.....	44
Configuring an array or logical drive.....	45
About Hardware Validation Tool.....	46
Using the hardware validation tool.....	46
About erasing data in Intelligent Provisioning.....	48
One-button secure erase.....	49
One-button secure erase access methods.....	50
Prerequisites for initiating the One-button secure erase process.....	50
Initiating the One-button secure erase process.....	52
Returning a system to operational state after One-button secure erase.....	53
Viewing the One-button secure erase report.....	54
One-button secure erase report details.....	55
Saving the One-button secure erase report to a CSV file.....	55
Deleting the One-button secure erase report.....	56
Impacts to the system after One-button secure erase completes.....	57
Hardware components that are reverted to the factory state.....	58
Hardware components that are not reverted to the factory state.....	59
One-button secure erase FAQ.....	59
Using System Erase and Reset.....	63
System Erase and Reset options.....	65
Creating a RAID configuration with SR Storage Administrator (SSA).....	66
Accessing SSA.....	66
Creating a RAID configuration with MR Storage Administrator (MRSA)	67

Accessing MRSA.....	67
Using the USB Key Utility.....	67
Troubleshooting.....	68
Basic troubleshooting techniques.....	68
Troubleshooting general issues	68
iLO log on required during Intelligent Provisioning F10 boot.....	69
Intelligent Provisioning does not launch when F10 is pressed.....	69
Intelligent Provisioning does not reimaging AOIP.....	70
A browser does not import a deployment profile correctly.....	71
Some Legacy BIOS Mode installs need specific instructions.....	71
Cannot create a custom partition size.....	72
Intelligent Provisioning cannot launch One-Button secure erase.....	72
One-Button secure erase is unsuccessful or reports errors.....	73
One-Button secure erase succeeds but some drives are not erased.....	74
One-Button secure erase reports errors, but no specific details.....	74
Not able to create or delete logical drive using Software Raid Controller.....	75
Troubleshooting Windows-specific issues	75
Windows Essentials does not install from USB source.....	75
Windows does not install on AMD servers.....	76
Troubleshooting Linux-specific issues	76
Unable to proceed with Assisted installation of Red Hat Enterprise Linux 7.....	77
Assisted installation of Red Hat OS hangs.....	77
Showing "Unable to install without the usb_storage driver loaded, Aborting",when upgrade or install with rpm.....	78
Unable to install Red Hat Enterprise Linux with secure boot enabled.....	78
Troubleshooting VMware-specific issues	79
Server reboots during VMware Assisted installation.....	79
HPE Compute Software and Firmware Product Documentation Quick Links.....	79
Intelligent Provisioning Quick Links	81
Websites.....	81
Support and other resources.....	82
Accessing Hewlett Packard Enterprise Support.....	82
Accessing updates.....	83
Remote support.....	84
Warranty information.....	84
Regulatory information.....	84
Documentation feedback.....	85

Introduction



TIP

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

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, their enclosures, and HPE Synergy compute modules. These components are preloaded with a basic set of firmware and OS components that are installed along with Intelligent Provisioning.



IMPORTANT

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

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

To access Intelligent Provisioning:

- Press **F10** from the POST screen and enter Intelligent Provisioning .

- From the iLO web interface using **Lifecycle Management**. **Lifecycle Management** allows you to access Intelligent Provisioning without rebooting your server.

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 V3.85
- 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.



NOTE

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

Intelligent Provisioning operation



NOTE

Intelligent Provisioning 3.40 and later requires iLO5 firmware version 1.10 or later.

Intelligent Provisioning includes the following components:

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



IMPORTANT

- Although your server is preloaded with firmware and drivers, Hewlett Packard Enterprise recommends updating the firmware upon initial setup. Also, downloading and updating the latest version of Intelligent Provisioning ensures the latest supported features are available.
- For ProLiant servers, firmware is updated using the Intelligent Provisioning Firmware Update utility.
- Do not update firmware if the version you are currently running is required for compatibility.



NOTE

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

Intelligent Provisioning provides installation help for the following operating systems:

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

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

Navigating Intelligent Provisioning

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

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

Icon	Function
Language 	Enables you to select the language to use.
Home 	Returns to the Intelligent Provisioning home page, with the Rapid Setup and Perform Maintenance menus. This icon is available only after completing the initial configuration and registration tasks.
Job Cart 	Displays the job configuration viewer screen, which displays the status of jobs in the queue. You can use this screen to monitor configuration tasks and jobs as they are processed.
Help 	Opens the online help to the section about the current screen.
System Information 	Displays system information, including the Intelligent Provisioning version.
Power 	Power down or reboot the server.
Log Out	Logs the current user out of Intelligent Provisioning.



NOTE

Icon	Function
	 This icon is only displayed in Always On mode.
Previous	Returns you to the previous screen after validating and saving your choices.
	
Continue	Takes you forward to the next screen after validating and saving your choices.
	

Accessing Intelligent Provisioning

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

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 the **Rapid Setup** or the **Perform Maintenance** 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.

Subtopics

Configuring the hardware and installing an OS with Intelligent Provisioning

Dedicated spare

Failure spare activation

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

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

Source media types and installation methods supported for each OS

Each **Rapid Setup** screen provides a guided method for configuring the server, installing an OS, and updating the system software.



IMPORTANT

- Intelligent Provisioning only supports original, licensed vendor media or Hewlett Packard Enterprise-branded versions. Demo or developer versions of the OS, or media that has been modified to slipstream custom software or service packs, are not supported and might not be correctly identified by the installation process.
- Manual install is not supported in Intelligent Provisioning 3.60 and later versions.

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.  NOTE • 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.
DVD-ROM Media	Allows you to install an OS from a DVD-ROM.
SMB/CIFS (Windows Share)	Allows you to install an OS from a Windows Share directory. You need the following network connection information, including: • Server Name or IP Address—Server name or IP address of the server that hosts the OS contents. If a server name is specified, a DNS entry is also required. • Share Name—The name of the network share using Server Message Block (SMB) protocol that hosts the OS contents. • 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: • Server Name or IP Address—FTP server name or IP address of the server that hosts the OS contents. FTP support requires anonymous

Media type	Required information or action
	mous access to the FTP server and does not support connecting to an FTP server through a proxy.  IMPORTANT When entering an FTP path, remove spaces and punctuation. The FTP server directory structure cannot contain spaces or special characters (including punctuation).
Install from Internet	Allows you to download source files from an Internet URL.
Virtual media	Allows you to install the OS from a virtual media source. Only supported in Always On Intelligent Provisioning mode.

- 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**.

For more information on RAID and Controllers, see [HPE Storage Controller Documentation Quick Links](#).

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
<code>Swap</code>	2000	<code>swap</code>	
<code>/boot/efi</code>	150	<code>vfat</code>	
<code>/</code>	40000	<code>btrfs</code>	
<code>/home</code>	Rest of HDD	<code>Xfs</code>	

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
<code>/boot</code>	1000	<code>Xfs</code>	
<code>/boot/efi</code>	200	<code>efi</code>	
<code>swap</code>	1000	<code>swap</code>	
<code>/</code>	10000	<code>xfs</code>	

/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

- VMware does not allow manual partition
- 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:

- Click the cell that you want to change.
- 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:

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

Dedicated spare

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

Failure spare activation

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

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

Performing maintenance



NOTE

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

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

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

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

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

To check the Intelligent Provisioning version, click the **System Information**  then check the **Intelligent Provisioning** version.

Setting Intelligent Provisioning Preferences

About this task

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

Procedure

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **Intelligent Provisioning Preferences** from the maintenance options.
3. In the **Basic Setting** tab, select settings for the following options:
 - **Interface Language**
 - **Keyboard Language**
 - **Boot BIOS Mode**
 - **Legacy Boot Mode**
 - **UEFI Optimized Boot Disable**
 - **UEFI Optimized**
 - **System Software Update**—Select a source for firmware update.
 - **Update from HPE Website**
 - **Update from Custom URL**
 - **Time Zone**
 - **System Date**

- **System Time**
- **Enable Feedback**
- Accept **EULA**, or click **Read EULA**

In the **Network Settings** tab, enter the following details:

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

4. Click **Submit**.

Results

When Intelligent Provisioning is run for the first time on a server, this is the first screen that is displayed within Intelligent Provisioning. For more information about the fields on this screen, see [Using the First Time Setup wizard](#).

Downloading Active Health System data

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

About this task

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

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



NOTE

Some browsers do not import deployment profiles correctly. Use the extension `.txt` to ensure browser compatibility.

Procedure

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

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

Subtopics

[Creating a Deployment Settings package](#)

[Using Deployment Settings package to configure a single server](#)

[Deployment Settings actions](#)

More information

[About Hardware Validation Tool](#)

[Creating a Deployment Settings package](#)

Creating a Deployment Settings package

Procedure

1. On the Deployment Settings screen, do one of the following:
 - a. To create a 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 the **Pencil** icon in the end of each row.
2. Enter a **Deployment Name**—Enter a name for this deployment package. Do not include spaces or special characters.
3. Enter **User Notes** and **Captured From** details.
4. Enter **Firmware Update** - Select the option type you want to update.
5. 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.
 - e. Select **Use Automation Controller Setting** or not.
 - f. Configure partition table.
 - g. Click **Save** button if everything is correct.
6. Enter the **ROM Settings**— See [Using the BIOS Configuration \(RBSU\) utility](#).
7. Enter the **Array Configuration**—See [Configuring Intelligent Storage](#).
8. Enter **Intelligent Provisioning Preferences**—See [Setting Intelligent Provisioning Preferences](#).
9. Enter **Hardware Validation Tool**— Select **Hardware Validation Tool** options for each deployment.
10. Click **Save** button to save the profile.

Using Deployment Settings package to configure a single server

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 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".

Deployment Settings actions

Icon	Description
	Click the Deploy icon to launch the automatic configuration utility.
	Click the Edit icon to change the following options: • Version Information • Operating System parameters • Intelligent Provisioning Preferences

Icon	Description
	• Array Configuration information • ROM Settings • Hardware Validation Tool
	Click the Delete icon to delete the selected deployment.
	Click Download to download the performance package to a network share or a USB drive.

Using the BIOS Configuration (RBSU) utility

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 5 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.

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

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

- **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 5 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 an **Accelerator**.
7. Select **RAID Size (GB)**.
8. Select a **Legacy Boot Priority**, then click the **Right Arrow** to go to next page.
9. In the **Summary** page, review the array settings.

- .0. Click **Done**. The Storage Configuration main page appears, displaying the following message `The operation will execute on the next reboot`.
- .1. 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.

Subtopics

One-button secure erase

Using System Erase and Reset

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

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



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.

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

- 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 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 the System Erase and Reset feature with extreme caution as such use will result in all internal and external storage drives and volumes accessible to the system being erased.

If you use the System Erase and Reset feature through Intelligent Provisioning v3.89 or earlier (Gen10, Gen10 Plus) or v4.32 or earlier (Gen11), there is no pop-up or any other type of warning displayed in the application.

Prior to implementing the **System Erase and Reset**, it is critical to **preserve data in drives or storage volumes that you do not want to erase**. Failure to do so will result in all accessible storage-attached devices exposed to the server being erased. HPE will not be responsible for any loss arising from storage-attached devices being erased by using the System Erase and Reset feature.

System Erase and Reset will securely erase any accessible storage disk or volume, including without limitation, FCOE, iSCSI, SAN, NVMe, SAN-attached, and direct-attached storage.

Examples of such accessible storage volumes are the ones presented from a SAN storage frame. Other examples include a D3940 on an HPE Synergy Frame.

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, the BIOS deletes the data that it controls. After the 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 have 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) View, save, or delete the One-button-Secure-Erase report.

Hewlett Packard Enterprise recommends completing this step.

3. (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 5 User Guide.

2. Install Intelligent Provisioning using an Intelligent Provisioning recovery image.
3. Install an operating system.
4. Optional: Install an iLO license.

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

5. Configure the BIOS settings and the iLO settings that apply to your environment.

6. (Optional) Create a System Recovery Set.

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

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.

Subtopics

[One-button secure erase report details](#)

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 5 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 #OD1 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.
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	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

Device	Operation requested	Result
	Administrator, if Smart Array Secure Encryption was enabled.	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	• 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.
HPE NS Boot Controller	Delete Logical drives + Clear Configuration Metadata + Factory Reset + Physical drive sanitize	• All array configurations, logical drives, and metadata are deleted. All controller settings are reset to their factory defaults. All attached drives are requested to be sanitized. See following for operations requested on the drives.
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.

Device	Operation requested	Result
		ata, 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

Prerequisites

Ensure that you preserve the data on drives or storage volumes that you do not want to erase.

- For rack systems that support Intelligent Provisioning with external storage, remove the physical cables, remove the server from the SAN zoning, or remove the server from the storage presentation prior to such use.
- For HPE Synergy or HPE BladeSystem c7000 blades with non-Virtual Connect SAN-managed connections, either remove the server from the SAN zoning or remove the server from the storage presentation prior to such use.
- In all cases, for HPE Synergy or HPE BladeSystem c7000, remove the server profile because this action ensures the removal of any Virtual Connect SAN-configured connections to any external storage. On a Synergy blade, this action removes any connection to D3940 storage.

About this task

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.



CAUTION

Use the System Erase and Reset feature with extreme caution as such use will result in all internal and external storage drives and volumes accessible to the system being erased.

If you use the System Erase and Reset feature through Intelligent Provisioning v3.89 or earlier (Gen10, Gen10 Plus) or v4.32 or earlier (Gen11), there is no pop-up or any other type of warning displayed in the application.

Prior to implementing the System Erase and Reset, it is critical to preserve the data in drives or storage volumes that you do not want to erase (mentioned in prerequisites above). Failure to follow these instructions will result in all accessible storage-attached devices exposed to the server being erased. HPE will not be responsible for any loss arising from storage-attached devices being erased by using the System Erase and Reset feature.

System Erase and Reset will securely erase any accessible storage disk or volume, including without limitation, FCOE, iSCSI, SAN, NVMe, SAN-attached, and direct-attached storage.

Examples of such accessible storage volumes are the ones presented from a SAN storage frame. Other examples include a D3940 on an HPE Synergy Frame.

Procedure

1. On the Intelligent Provisioning home screen, click **Perform Maintenance**.
2. Select **System Erase and Reset** from the maintenance options.

The **Select Devices to erase** page appears giving you multiple options.

3. Depending on your requirements, choose one or more from the following job-actions:
 - a. To clear your Intelligent Provisioning Preferences, enable the **Clear Intelligent Provisioning Preferences** option.
 - b. To clear your AHS logs, enable the **Active Health System log** option.
 - c. To erase file system or partition table signatures, enable the **All HDD and SSD** option.

When you enable **All HDD and SSD**, a code-based warning appears; if you click **Ok** in that warning, it starts displaying an automatically enabled **Secure Erase** option below **All HDD and SSD**.



NOTE

All HDD and SSD option is active for users only when a Hard Disk Drive or Solid State Device is connected to the server.

4. Click **Submit**.

The **Job Configuration Viewer** page appears indicating the number of jobs you have selected as part of the Secure Erase process.

5. Click **Launch Now** to proceed with the system erase and reset process.

The 'System Erase and Reset' job status appears in a progress bar on the **Job Viewer** page until the process is complete.

6. Select **Reboot** to restart the server.

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	Erases all hard drives and solid state drives on this server.  NOTE • Only supported in F10 mode, not supported in AI ways 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.
Secure Erase	Writes a data pattern over all drive sectors. This action might take several hours.  NOTE

Option	Description
	 Only available if you select All Hard Drives .
Intelligent Provisioning Preferences	Clear Intelligent Provisioning preferences.
Active Health System logs	Clears all AHS log files.

Creating a RAID configuration with SR Storage Administrator (SSA)

The following section introduces the concept of SSA. For more information related to SSA, see the [HPE Smart Storage Administrator GUI User Guide](#).

Subtopics

[Accessing SSA](#)

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 the **Intelligent Provisioning** Home page
 - On the **Intelligent Provisioning** Home page, click **Perform Maintenance**.
 - Select **SR Storage Administrator** from the maintenance options.

The **Smart Storage Administrator** window is displayed.

Creating a RAID configuration with MR Storage Administrator (MRSA)

The following section introduces the concept of MRSA. For more information related to MRSA, see the [HPE MR Storage Administrator User Guide](#).

Subtopics

[Accessing MRSA](#)

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.

- **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 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 volume label is used to identify the drive.

4. Select the drive and click **Save**.



NOTE

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

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

Basic troubleshooting techniques

Troubleshooting general issues

Troubleshooting Windows-specific issues

Troubleshooting Linux-specific issues

Troubleshooting VMware-specific issues

Basic troubleshooting techniques

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

Troubleshooting general issues

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
A browser does not import a deployment profile correctly
Some Legacy BIOS Mode installs need specific instructions
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.
Not able to create or delete logical drive using Software Raid Controller

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



NOTE

Modify the command as per the system requirements.

A browser does not import a deployment profile correctly

Symptom

Intelligent Provisioning does not import a deployment profile correctly.

Action

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

Some Legacy BIOS Mode installs need specific instructions

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



NOTE

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

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



NOTE

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

Cannot create a custom partition size

Symptom

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

Action

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

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

Intelligent Provisioning cannot launch One-Button secure erase

Symptom

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

Solution 1

Cause

You do not have the correct license.

Action

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

Solution 2

Cause

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

Action

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

Solution 3

Cause

Server Configuration Lock is enabled.

Action

Disable Server Configuration Lock.

One-Button secure erase is unsuccessful or reports errors

Symptom

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

Solution 1

Cause

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

Action

Do one of the following:

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

Solution 2

Cause

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

Action

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

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

Symptom

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

Cause

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

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



NOTE

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

Action

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



NOTE

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

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

Symptom

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

Cause

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

Action

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

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

Symptom

Cannot create or delete logical drives using **Software Raid Controller**.

Action

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

Troubleshooting Windows-specific issues

Subtopics

Windows Essentials does not install from USB source

Windows does not install on AMD servers

Windows Essentials does not install from USB source

Symptom

Windows Essentials does not install from a USB source.

Cause

USB installations are not supported for Windows Essentials.

Action

Install Windows Essentials from an ISO source.

Windows does not install on AMD servers

Symptom

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

Cause

The BIOS settings IOMMU and Hyper-V are activated.

Action

1. From the Intelligent Provisioning main screen, select **Perform Maintenance > BIOS/Platform Configuration > Virtualization Options > AMD (R) IOMMU**.
2. Select **Disabled**.
3. Save the setting.
4. Download and install all operating system patches.
5. Reboot the system and then enable IOMMU settings.

Troubleshooting Linux-specific issues

Subtopics

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

Assisted installation of Red Hat OS hangs

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

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

Symptom

When installing Red Hat Enterprise Linux 7, you are unable to proceed with the Assisted installation with valid OS images through FTP source media. The failure was seen with a long file path for CIFS share, however, it succeeds with a short path (less than 32 bytes).

Cause

Required Red Hat OS files are missing or incorrectly placed.

Action

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

Assisted installation of Red Hat OS hangs

Symptom

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

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

Cause

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

Action

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

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

Symptom

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

Cause

The usb_storage module is disabled.

Action

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

Unable to install Red Hat Enterprise Linux with secure boot enabled

Symptom

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

Cause

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

Action

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

Troubleshooting VMware-specific issues

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.

HPE Compute Software and Firmware Product Documentation Quick Links

This infographic provides quick links for documentation for the listed HPE products. It offers easy access to documentation that helps you to understand, implement, and troubleshoot your products.

Each product-specific section lists the current version, the earlier two major versions, and their revisions.



Click each product label to access its documentation

Software & aaS Management platform

Firmware/ System Software

HPE Compute
Ops Management

HPE OneView Plug-ins

HPE iLO

HPE Compute Ops
Management Plug-in for
VMware vCenter

HPE Serviceguard

Intelligent
Provisioning

Integrated
Smart Update Tools

Smart Update Manager

Service Pack for
HPE ProLiant

HPE OneView

HPE VMware ESXi
Server

UEFI
System Utilities

Agentless
Management Service

Navigating the Hewlett Packard Enterprise Support Center

•



Navigation and workspace

•



Search and product knowledge

Subtopics

Intelligent Provisioning Quick Links

This page is a comprehensive list of all the documents for Intelligent Provisioning. It provides quick links to the recent versions of each document.

Intelligent Provisioning Quick Links

This page is a comprehensive list of all the documents for Intelligent Provisioning. It provides quick links to the recent versions of each document.

Documents	Gen12 Servers	Gen11 Servers	Gen10/Gen10 Plus Servers
Intelligent Provisioning Release Notes	<u>5.04</u>	<u>4.37</u>	<u>3.92</u>
	<u>5.03</u>	<u>4.36</u>	<u>3.91</u>
	<u>5.02</u>	<u>4.35</u>	<u>3.90</u>
	<u>5.00</u>	<u>4.32</u>	<u>3.86</u>
Intelligent Provisioning User Guide	<u>5.04</u>	-	-
	<u>5.03</u>	<u>4.34</u>	<u>3.89</u>
	<u>5.02</u>	<u>4.32</u>	<u>3.88</u>
	<u>5.00</u>	<u>4.31</u>	<u>3.86</u>
ProLiant Gen12 Intelligent Provisioning (IP) Debug Document	<u>Gen12</u>		
Alerts-Customer Advisories	<u>All Versions</u>		

Websites

Intelligent Provisioning

<https://www.hpe.com/servers/intelligentprovisioning>

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

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>

My HPE Software Center

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

- To subscribe to eNewsletters and alerts:

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

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

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



IMPORTANT

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

Remote support

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

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

HPE Get Connected

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

HPE Tech Care Service

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

HPE Complete Care

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

Warranty information

To view the warranty information for your product, see the **[warranty check tool](#)**.

Regulatory information

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

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

Additional regulatory information

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

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

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

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

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

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

Documentation feedback

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