Hewlett Packard Enterprise

Technical white paper

Smart Update Technology

An end-to-end update solution for HPE ProLiant servers and HPE BladeSystem and HPE Synergy infrastructure

Contents

Executive summary

HPE's Smart Update Technology is an innovative server and infrastructure maintenance solution that simplifies the time-consuming, expensive, and error-prone task of keeping servers and data center infrastructure up-to-date and secure. Smart Update provides an end-to-end update solution for HPE ProLiant servers, and HPE BladeSystem and HPE Synergy infrastructure, including:

- Reducing the time and cost of server and infrastructure maintenance
- Maintaining consistent firmware and driver versions across servers and infrastructure
- Providing scalability through integration with HPE OneView, iLO Amplifier Pack, and other system management software

Smart Update addresses the challenges of server and infrastructure maintenance, not as is a single monolithic application, but as a system of interlocking pieces that work together to address the issues of the update challenge, including:

- Consistent, integrated, and fully-supported update sets (service packs) for firmware, drivers, and system software
- Simple and powerful server and infrastructure update technology that updates systems while they are online
- Scalability to thousands of servers through integrations with HPE OneView and iLO Amplifier Pack

This white paper provides an overview of HPE's Smart Update technology for technical professionals interested in understanding the Smart Update architecture and components as well as how Smart Update integrates with other HPE system maintenance tools and management software.

General knowledge of HPE ProLiant servers, HPE BladeSystem and HPE Synergy infrastructure, HPE OneView, and HPE iLO is helpful in understanding the Smart Update technology, but not required.

Introduction to Smart Update

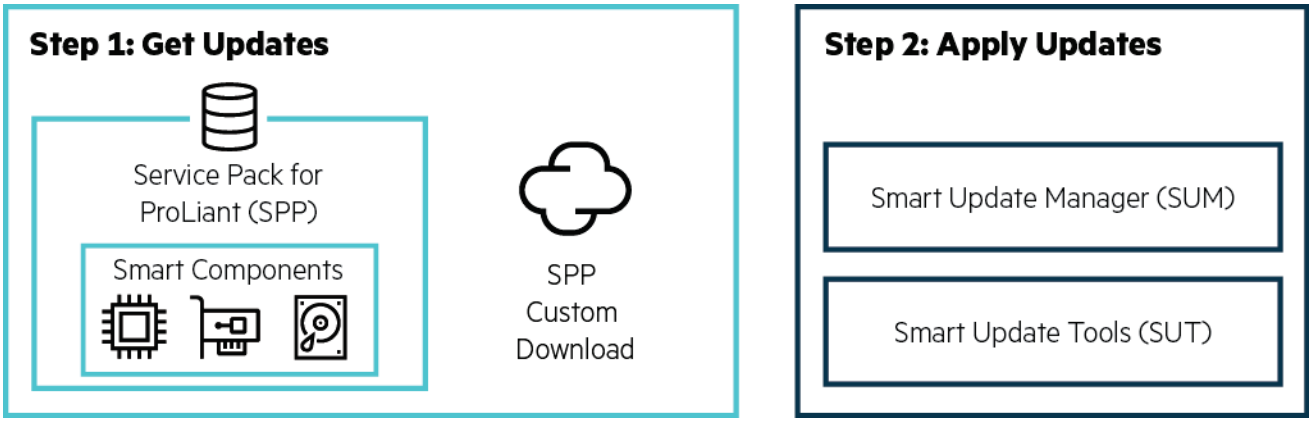
There are three release triggers for updating server and infrastructure firmware, drivers, and system software:

- **Hot fix**—The release of an update that may require immediate attention. Hot fixes are typically security, data destructive, data loss, or performance loss related updates.
- **Support call fix**—Refers to when a customer-initiated support request results in an update to resolve a specific issue.
- **Routine maintenance**—Part of a regular server maintenance schedule; this varies by customer, but is typically every 12 to 18 months.

The numbers of servers and infrastructure components that need to be updated differs for each of the three triggers, but the same basic update workflow is used for each.

For example, the preparation, testing, and update effort required to update every server in the data center as part of the yearly maintenance update is much larger than the effort to update one device on a single server model to resolve a vendor issue. The yearly server maintenance update is typically planned and executed over several months and consumes considerable IT resources, whereas the update to address a vendor issue could require just a couple of hours and would consume much fewer IT resources.

HPE's Smart Update technology is a collection of building blocks, based on the Service Pack for ProLiant (SPP) and Smart Update Manager (SUM) that combine to solve the problem of time-consuming, expensive, and error-prone updates using a two-step process.



Step 1: Get Updates

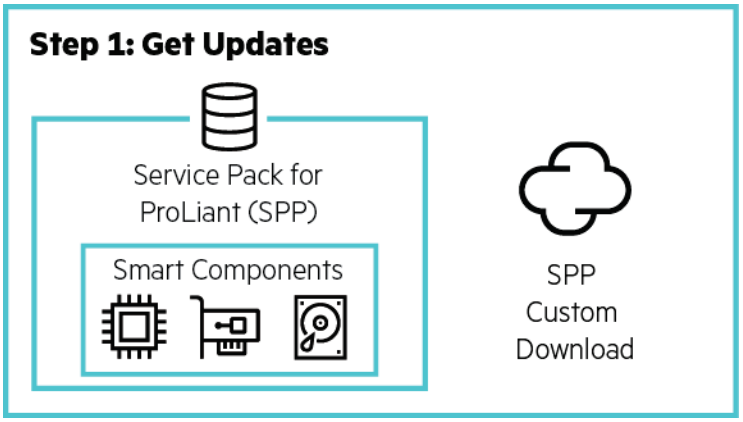
- Service Pack for ProLiant (SPP)—A comprehensive collection of smart components (firmware, drivers, and system software) tested together as a single solution stack and used for updating HPE ProLiant servers and HPE Synergy and HPE BladeSystem infrastructure.
- Smart Components—Self-contained executables modules delivered on the SPP that contain the firmware, drivers, and system software updates as well as the code to install the updates.
- SPP Custom Download—A web service that allows you to reduce the size of the SPP by excluding smart components for operating systems and server models that you don't needed.

Step 2: Apply Updates

- Smart Update Manager (SUM)—The core engine for sequencing and deploying firmware, driver, and system software updates using the smart components.
- Smart Update Tools (SUT)—A SUM extension that enables HPE OneView and iLO Amplifier Pack to stage, schedule, and apply updates automatically to reduce IT operations.

Together the SPP, smart components, SPP Custom Download, SUM, and SUT provide better operating stability and help protect uptime for HPE infrastructure.

Step 1: Get Updates



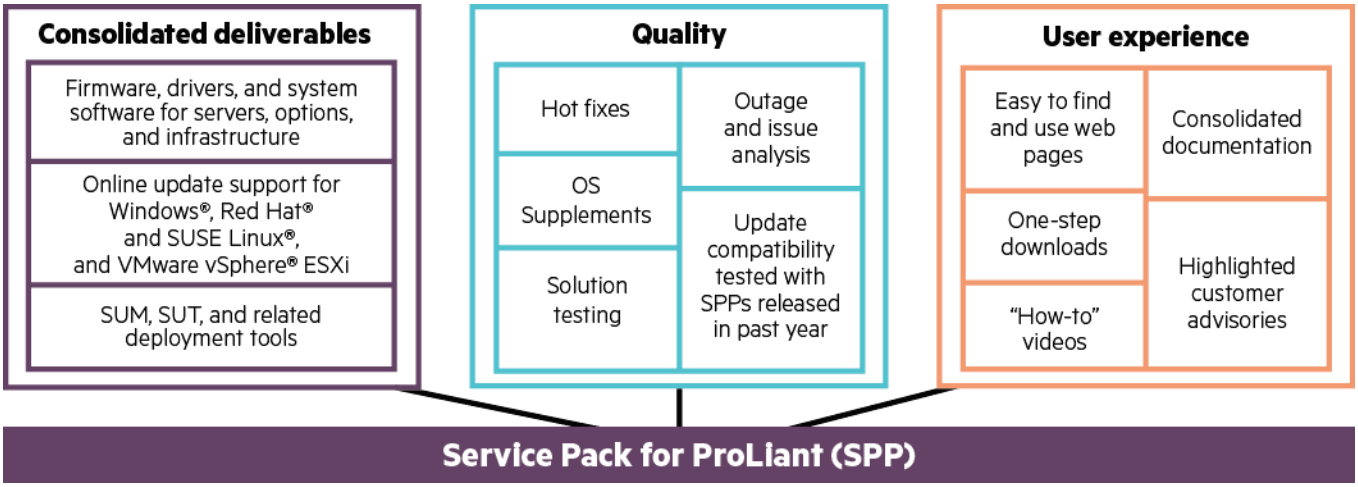
The first step in the update process is triggered by one of the three release triggers (hot fix, support call fix, or routine maintenance). This section covers the:

- Smart Update building blocks
- Information you need to know about the updates, such as:
  - What's changed?
  - Do the updates apply to my servers and infrastructure?
  - Is the update critical, recommended, or optional?
- How to download the updates

Smart components

Smart components are self-contained executables modules delivered on the SPP that contain the firmware, drivers, and system software updates, as well as the code to install the updates. Smart components are released as part of an SPP and released as individual components to HPE Support Center.

Service Pack for ProLiant (SPP)



The SPP is a comprehensive collection of smart components (firmware, drivers, and system software) tested together as a single-solution stack and used for updating HPE ProLiant servers and HPE Synergy and HPE BladeSystem infrastructure. The SPP provides two distinct advantages that enhance and simplify the update experience:

- Because the SPP packages all of the smart components as a single deliverable and download, you no longer need to download and manage individual firmware, driver, and system software updates.
- Because the smart components have been tested together as a single solution stack, you no longer need to perform extensive testing to ensure the firmware, driver, and system software updates will work.

Each SPP is released in one of the following three formats:

- **SPP ISO:** The SPP ISO is a bootable ISO that contains the latest versions of the smart components, SUM, and SUT. You can perform:
  - Offline firmware updates by booting directly to the SPP ISO, or
  - Online firmware, driver, and system software updates using SUM with the SPP ISO as your baseline

- **OS supplement:** An OS supplement is an SPP-tested bundle containing the driver and system software smart component updates needed for a new OS/hypervisor version. OS Supplements are released when the release date of the new OS/hypervisor version doesn't align with the SPP release schedule.
  - You can apply the smart component updates in the OS supplement by merging the OS supplement with the previously released SPP.
  - HPE's goal is to support new OS/hypervisor versions without releasing smart component driver updates and OS Supplements are released only when that's not possible.
- **Maintenance Supplement Bundle (MSB):** MSB releases are rare; an MSB is an SPP-tested bundle of smart component updates released since the last SPP, such as hot fixes, security updates, OS supplements, and new product/device support. You can apply the smart component updates included in the MSB by merging the MSB with the previously released SPP.

Hot fixes

Smart component updates that are released outside of an SPP ISO, OS supplement, or MSB to resolve an issue are known as hot fixes. Hot fixes are important smart component updates to resolve critical issues that have been approved as out of cycle releases to get them to customers faster. Hot fixes are tested individually against the SPPs released in the last year. For each hot fix, HPE publishes a customer advisory (CA) to help customers understand the problem addressed. Note that:

- You do not need to apply every hot fix, and should individually choose hot fixes as a practical way to manage the impact of these updates in the context of your business.
- You can apply a hot fix by merging the hot fix with the SPP it applies to.

For the list of hot fixes by SPP release, see the "Hot Fixes & Advisories" tab of the SPP download page.

Production and Post-Production SPPs

To reduce the frequency of server updates, especially for older server generations, HPE releases two types of SPPs:

- A single "Production SPP" with support for the production server generations.
- Multiple generation specific "Post-Production SPPs" with support for one specific post-production server generation.

Production SPP

The production server generations, which include the latest generation and one generation back, are the server generations where HPE is adding support for new technology, features, options, and new major OS/hypervisor versions. All of these involve adding new functionality to or modifying existing functionality in the firmware, drivers, and system software, and releasing updated versions.

Firmware, drivers, and system software updates for the production server generations may include bug fixes, security updates, plus new features, functionality, and OS/hypervisor version support and require more frequent updates and testing.

For the production server generations, HPE releases a single "Production SPP" approximately two to four times per year.

Because the updates contain new functionality, bug fixes, and security updates, HPE recommends updating production server generations on a yearly cadence.

Post-Production SPP

The post-production server generations (two or more generations back) are the server generations where HPE is no longer adding support for new technology, features, options, or major OS/hypervisor versions. When a server generation is in post-production, modifications to the firmware, drivers, and system software for that server generation is limited to bug fixes and security updates.

For the post-production server generations, HPE freezes the smart component versions and releases a Post-Production SPP for that server generation. Once in post-production, updates are only released to resolve a specific issue and are released as hot fixes against the Post-Production SPP.

Because updates are only released to resolve specific issue, HPE recommends updating to Post-Production SPP and then applying only the hot fixes that apply to your server models, OS/hypervisor versions, and environment.

Post-Production SPPs are supported for the support life of that server generation and you do not need to perform yearly updates on post-production server generations.

Which SPP should I use?

Server generation	Classification	SPP to use
Gen10 and Gen9	Production	Latest Production SPP version
Gen8	Post-Production	Gen8 Post-Production
G7	Post-Production	G7 Post-Production
G6 and older	Post-Production	Use the last Production SPP version that contained the smart components for your server model(s)

SPP release documentation

With each SPP release, HPE provides the following release documentation:

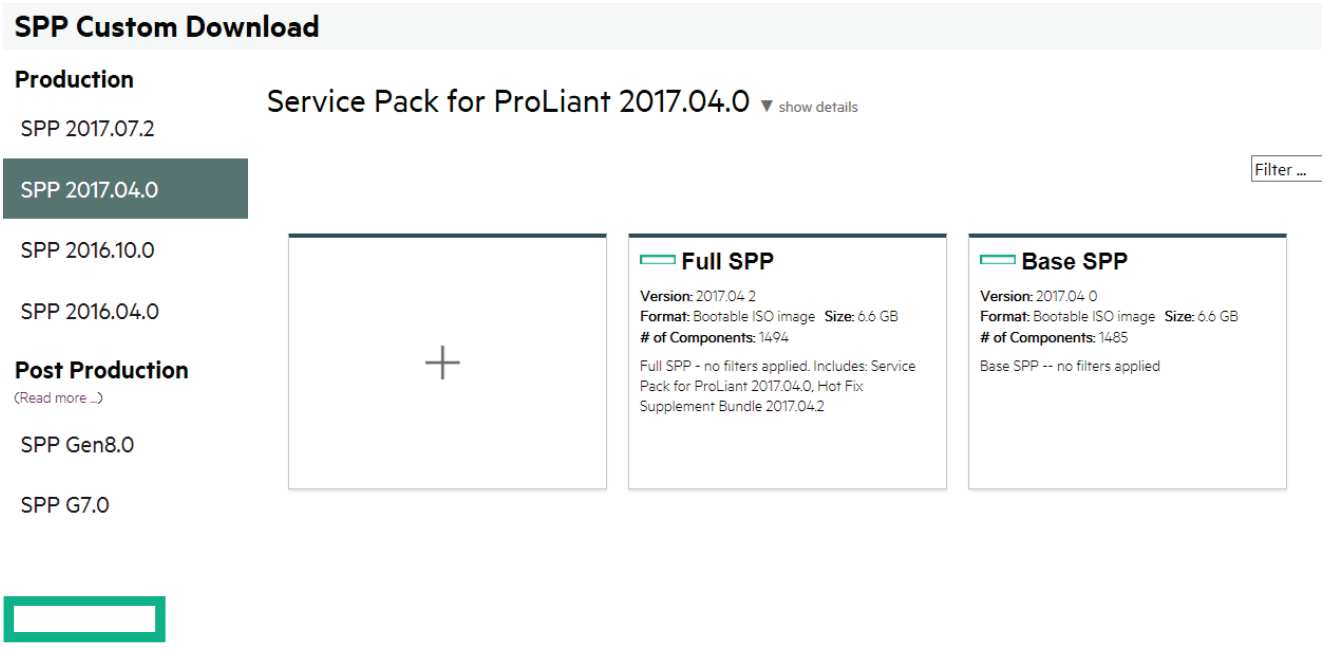
- **SPP release notes**—Release notes for the SPP release including the important notes, enhancements, supported online update OS/hypervisor versions, prerequisites, and deployment instructions.
- **Server support guide**—List of servers supported in the SPP release and the server support list for each smart component included on the SPP.
- **Contents report**—Report of the smart components included in the SPP release including the product category (e.g., BIOS system ROM), description, version, upgrade requirement, and filename for each smart component.
- **Component release notes**—Individual release notes for each smart component including the upgrade requirement (critical, recommended, and optional), file name, important notes, version, dependencies, enhancements/new features, problems fixed, and prerequisites.

Downloading the SPP

The SPP is available as a free download for use on products, which are under an active warranty or an HPE Support Agreement. See HPE ProLiant Servers Firmware Access Update and More Information on Access to HPE Support Materials for more details.

HPE provides several methods to download the SPP:

- SPP Custom Download, at hpe.com/servers/spp/custom, is the preferred method for downloading a Production or Post-Production SPP.
- SPP download page at hpe.com/servers/spp/download, which also provides access to the SPP release documentation, hot fixes and advisories, and FAQs.
- HPE Support Center (hpe.com/support).
- Software Delivery Repository (SDR) at downloads.linux.hpe.com/SDR is a YUM Repository containing the smart components.



Because you don't always need every smart component included on the SPP or because sometimes you need to merge an OS supplement, MSB, or hot fix with the SPP, HPE has created a free web service that allows you to tailor the SPP for your environment. Using the SPP custom download web service you can:

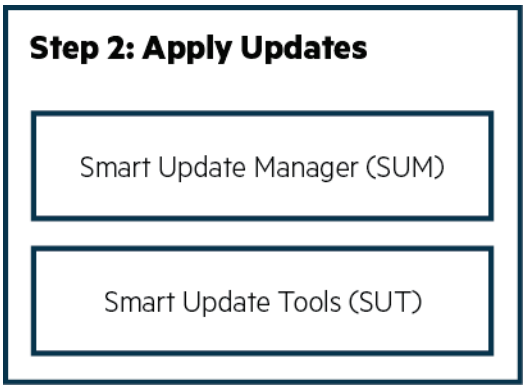
- **Create a custom SPP**—Allows you to reduce the size of the SPP by removing the smart components for the server models you don't have and OS/hypervisor versions you don't use.
- **Download the Base SPP ISO**—HPE-published SPP ISO that is always published and contains the smart components the day the SPP was released.
- **Download the Full SPP ISO**—Published by HPE when one or more hot fixes, OS supplements, or MSBs exist and contains the smart components from the Base SPP ISO plus all hot fixes, OS supplements, and MSBs. Every time a new hot fix, OS supplement, or MSB is published:
  - The Full SPP ISO is regenerated
  - The revision number is updated
  - A new Full SPP ISO is published

By downloading the Full SPP ISO or cloning and customizing the Full SPP ISO, you can be assured you're getting all of the latest SPP tested updates (OS supplements and hot fixes).

Updating from a previous SPP

As part of the comprehensive testing HPE does for each new SPP release, HPE tests the update compatibility of the smart components against the last years' worth of SPP releases. This comprehensive testing allows HPE to provide a one-year update compatibility for each new SPP release, and allows customers running an SPP released in the past year to update directly to the most recent SPP. HPE recommends customers outside of the one-year compatibility window perform intermediate updates—conforming to the one-year compatibility of the SPP they're currently using—to update to the most recent SPP. For example, if you're currently using the 2015.10.0 SPP and want to update to the 2017.10.0 SPP, you'll need to perform two updates: one update from 2015.10.0 to 2016.10.0 and then a second update from 2016.10.0 to 2017.10.0. HPE publishes an SPP compatibility table on the documentation tab of the SPP download page.

Step 2: Apply Updates



SUM

SUM sits at the heart of the Smart Update technology and is the preferred engine for deployment of the smart component updates. At its core, SUM is the update engine that delivers the appropriate smart component updates to target servers and infrastructure and manages the execution of those updates. SUM:

- Includes an integrated discovery engine that finds installed versions of hardware, firmware, drivers, and system software on target servers and infrastructure
- Deploys updates in the correct order to apply the updates correctly and most efficiently as to reduce the impact on operations
- Ensures all dependencies and interdependencies are met before deploying an update
- Provides both a scripted and step-by-step guided update process
- Applies updates to both local and remote servers
- Provides both an online and offline update method
- Provides tamper-proof updates that are digitally validated with iLO 5 (on HPE Gen10 servers)
- Integrates with HPE OneView and iLO Amplifier Pack to provide a convenient update process at scale
- Includes a built-in rollback to revert to the last known good (bookmarked) update (with iLO 5 on HPE Gen10 servers)

SUT

SUT is a SUM extension that enables HPE OneView and iLO Amplifier Pack to stage, schedule, and apply updates automatically and at scale to reduce IT operations. SUT is an OS utility that provides the ability to perform online firmware, driver, and system software updates via the iLO management network without the need for OS credentials.

Agentless updates with dependency checking

Unlike other update engines, SUM is able to perform agentless server and infrastructure updates. This means SUM performs firmware, driver, and system software updates to the devices of target servers and infrastructure without requiring the devices to have permanently installed system management agents running on them. SUM accomplishes this task by downloading and executing a process using the SUM update engine on each target device being updated. This process receives the appropriate smart components that SUM delivers to the server, unpacks the smart components, and allows the smart components to perform the update of their particular system component or device. After the SUM engine has completed the full set of updates, it terminates this process and removes itself from the target server.

SUM's built-in dependency checking allows SUM to update the various system components and devices in the proper order to ensure proper system operation following the updates. Dependency checking is particularly important when SUM is updating interrelated devices such as an HPE ProLiant BladeSystem environment. When updating an HPE BladeSystem environment, the BladeSystem enclosure may require firmware updates to each of the following:

- Individual ProLiant BladeSystem servers and their network adapters
- Virtual Connect modules
- The Onboard Administrator for the BladeSystem enclosure

When updating an HPE BladeSystem environment, the sequencing of the updates is extremely important and SUM's dependency checking ensures the updates are performed in the correct order.

Server and Infrastructure update methods with SUM

SUM provides:

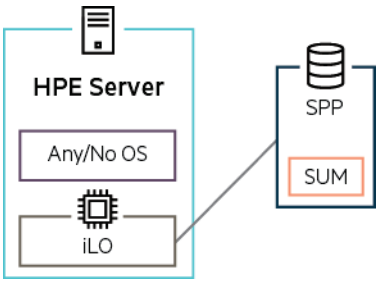
- Web-based user interface (UI) to guide you through the discovery and updates
- Command line interface (CLI) so that you can script the discovery and updates

In order to provide firmware, driver, and system software updates across a wide range of OS/hypervisors vendors and customer requirements, SUM provides a number of different update methods.

Update method	Smart components updated	Common scenarios
Offline	Firmware only	Need to update the firmware of a server with no OS/hypervisor installed or running an OS/hypervisor version not supported by the SPP.
Online update of a local server running Windows or Linux	Firmware, drivers, and system software	Need to update the firmware, drivers, and system software of a single server running a Windows or Linux version supported by the SPP.
Online update of a remote server running Windows or Linux	Firmware, drivers, and system software	Need to update the firmware, drivers, and system software of a single server running a Windows or Linux version supported by the SPP.
Online update of remote server running VMware vSphere ESXi	Firmware, drivers, and system software	Need to update the firmware, drivers, and system software of a single server running a VMware vSphere ESXi version supported by the SPP.
Online update of multiple remote servers from a Windows or Linux node	Firmware, drivers, and system software	Need to update the firmware, drivers, and system software of multiple servers, all of which are running a Windows, Linux, or VMware vSphere ESXi version supported by the SPP.
Update of BladeSystem or Synergy infrastructure	Firmware only	Need to update the firmware of the BladeSystem or Synergy infrastructure.

Note
The online OS/hypervisor version support varies from SPP to SPP; see the SPP OS Guide or the SPP release notes for the online OS/hypervisor version support for a specific SPP.

Offline Update of a Server



The offline update method is most commonly used to update:

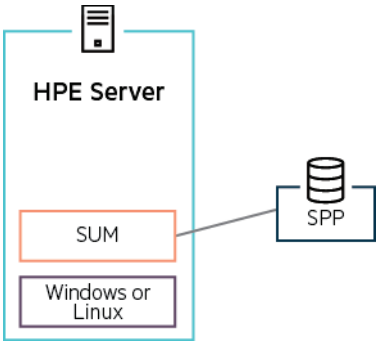
- A server's firmware prior to the OS installation
- Servers running an OS/hypervisor version that the SPP doesn't support
- Servers using the in-box drivers from an OS/hypervisor vendor

To perform the offline update method:

- The administrator takes the server offline and boots the server to the SPP ISO, typically using iLO's virtual media feature
- The server boots to the SPP boot environment and invokes the SUM instance on the SPP ISO
- SUM discovers and updates the firmware using the Linux version of the smart components

Once the update is complete, the SPP ISO is disconnected, the server reboots, and is placed back online.

Online update of a local server running Windows or Linux

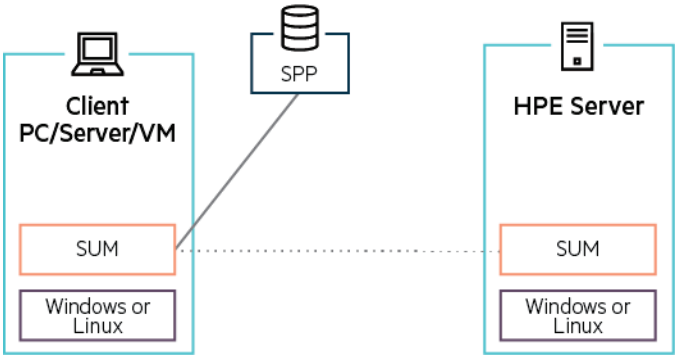


The online update of a local server running Windows or Linux involves:

- Installing and running SUM on the target server
- Using SUM to discover and update the firmware, drivers, and/or system software

Once the update is complete, the local server is rebooted, only if required by the updates.

Online update of a remote server running Windows or Linux

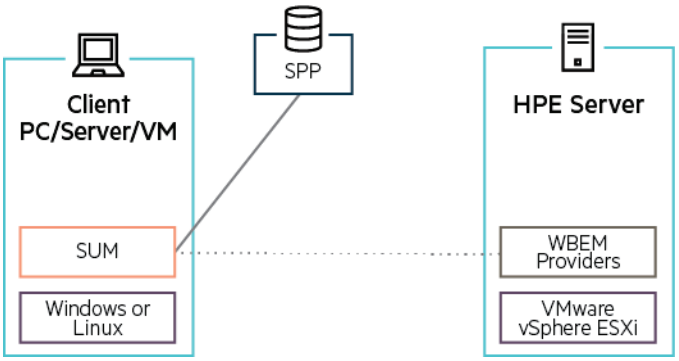


The online update of a remote server running Windows or Linux involves:

- Installing and running SUM on a client—PC, server, or VM—running Windows or Linux
- Using SUM on the client to discover the remote Windows/Linux server
- SUM on the client then downloads the SUM update engine to the remote Windows/Linux server
- The SUM update engine running on the remote server then discovers and updates the firmware, drivers, and/or system software and reports the results back to SUM on the client

Once the update is complete, the SUM engine is deleted from the remote server and the remote server is rebooted, only if required by the updates.

Online update of a remote server running VMware vSphere ESXi

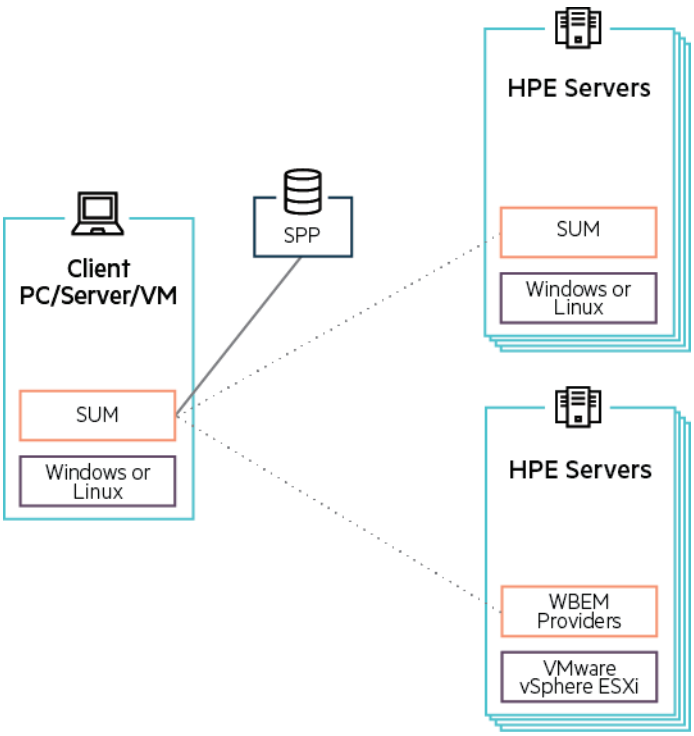


The online update of a remote server running VMware vSphere ESXi involves:

- Installing the HPE WBEM providers on the remote VMware vSphere ESXi server
- Installing and running SUM on a client—PC, server, or VM—running Windows or Linux
- Using SUM to discover the remote VMware vSphere ESXi server
- SUM communicating with the WBEM providers to discover and update the firmware, drivers, and/or system software

Once the update is complete, the remote server is rebooted, only if required by the updates.

Online update of multiple remote servers running Windows, Linux, or VMware vSphere ESXi

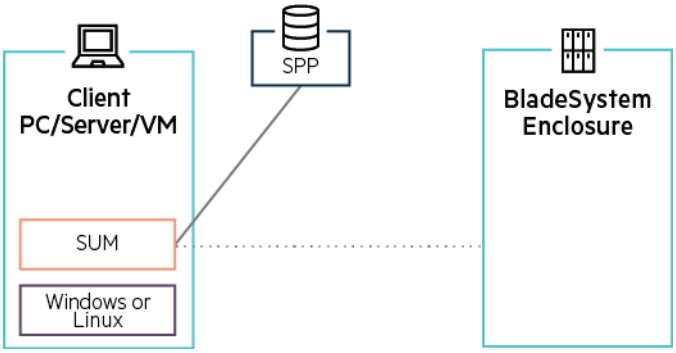


Online update of remote servers is limited to servers running Windows, Linux, or VMware vSphere ESXi.

The process for updating each individual server matches the process described in the "Online update of a remote server running Windows or Linux" and the "Online update of a remote server running VMware vSphere ESXi" sections discussed previously.

The only difference is you're performing the updates simultaneously using a single instance of SUM. See the SUM user documentation for the simultaneous update maximums for Windows, Linux, and VMware vSphere ESXi.

Update of an HPE BladeSystem or HPE Synergy Infrastructure



You can use SUM or HPE OneView to update the firmware of your HPE BladeSystem infrastructure.

You must use HPE OneView to update the firmware of your HPE Synergy infrastructure.

When using HPE OneView to perform the update, HPE OneView communicates with SUM and SUM performs the update. The update method description here provides a high-level overview of the HPE OneView and HPE Synergy infrastructure update. For a more detailed description, see the HPE OneView user documentation.

The update of BladeSystem or Synergy infrastructure involves:

- Installing and running SUM on a client—PC, server, or VM—running Windows or Linux or running HPE OneView
- Using SUM or HPE OneView to discover and update the firmware of the HPE BladeSystem or HPE Synergy infrastructure

Server Update Methods using HPE OneView and iLO Amplifier Pack

To perform updates at scale, Smart Update integrates with two other HPE products: HPE OneView and iLO Amplifier Pack. The high-level update methodology and integration with Smart Update is the same for both products. Therefore, this paper describes the update method for both products together.

For more details on HPE OneView, see hpe.com/oneview.

For more details on iLO Amplifier Pack, see hpe.com/servers/iloamplifierpack.

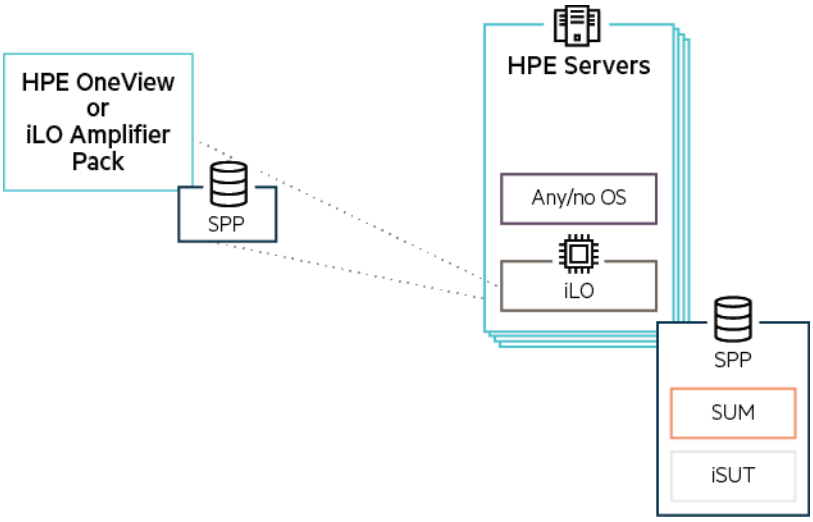
At the core of the integration with HPE OneView and iLO Amplifier Pack is SUT. SUT is an extension of SUM that enables HPE OneView and iLO Amplifier Pack to stage, schedule, and apply updates automatically and at scale. SUT is an OS/hypervisor utility that provides the ability to perform online firmware, driver, and system software updates via the iLO management network without the need for OS credentials.

The offline and online update methods of HPE OneView and iLO Amplifier Pack are detailed in the sections below.

Online updates using HPE OneView and iLO Amplifier Pack require SUT to be installed in the OS/hypervisor of the remote servers or in a helper OS appliance as follows:

OS/hypervisor of remote server	Server generation	SUT to use	Where is SUT installed and running?
Windows	Gen10, Gen9, and Gen8	Integrated SUT (iSUT) for Windows	In the Windows instance of each remote server
Red Hat or SUSE	Gen10, Gen9, and Gen8	Integrated SUT (iSUT) for Linux	In the Red Hat or SUSE instance of each remote server
VMware vSphere ESXi	Gen10	Not currently supported	Online updates not currently supported, use the offline update method
VMware vSphere ESXi	Gen9 and Gen8	SUT for VMware vSphere ESXi	In a Red Hat instance running on a physical server, or VM

Offline update of a remote server using HPE OneView or iLO Amplifier Pack



The HPE OneView and iLO Amplifier Pack offline update of a remote server method does not require SUT to be installed in the OS/hypervisor of the remote server and is very similar to the "Offline Update" method of single server described previously and is most commonly used to update servers:

- A server's firmware prior to the OS installation
- Servers running an OS/hypervisor version that the SPP doesn't support
- Servers using the in-box drivers from an OS/hypervisor vendor

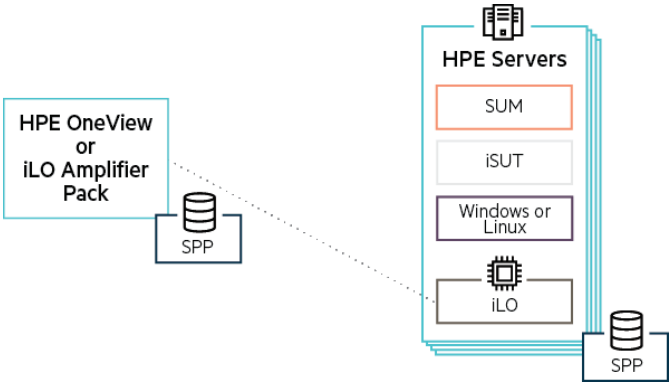
To perform the offline update of a remote server using HPE OneView and iLO Amplifier Pack:

- Use HPE OneView/iLO Amplifier Pack to initiate an offline update of the remote server
- HPE OneView/iLO Amplifier Pack attaches the SPP ISO to the remote server using iLO's virtual media
- The server reboots to the SPP boot environment, invokes the iSUT instance on the SPP ISO
- iSUT invokes the SUM instance on the SPP ISO
- SUM discovers and updates the firmware using the Linux version of the smart components on the SPP ISO

Once the update is complete:

- iSUT reports the results back to HPE OneView/iLO Amplifier Pack
- The SPP ISO is disconnected from the remote server
- The server reboots and is placed back online

Online update of a remote server running Windows or Linux using HPE OneView or iLO Amplifier Pack



The HPE OneView and iLO Amplifier Pack online update of a remote server running Windows or Linux requires iSUT for Windows/Linux to be installed in the OS of the remote server and involves:

- Using HPE OneView/iLO Amplifier Pack to initiate an online update of the remote server
- HPE OneView/iLO Amplifier Pack attaching the SPP ISO to the remote server using iLO's virtual media
- iSUT copying the smart components from the SPP ISO into the OS of the remote server
- iSUT loading and running the SUM instance on the SPP ISO in the OS of the remote server
- SUM discovering and updating the firmware, drivers, and system software, using the previously copied smart components

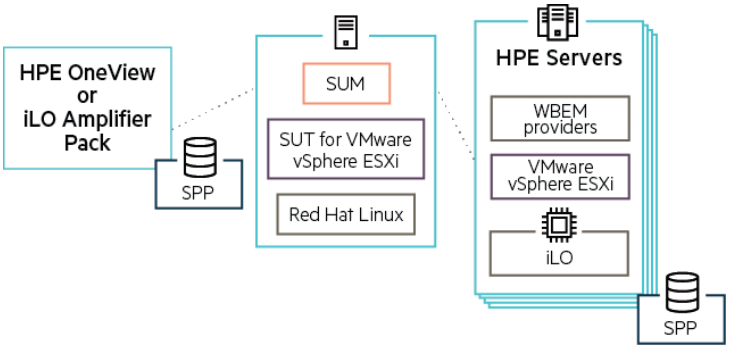
Once the update is complete:

- iSUT reports the results back to HPE OneView or iLO Amplifier Pack
- The SPP ISO is disconnected from the remote server
- SUM is removed from the remote server
- The remote server is rebooted, only if required by the updates

Online update of a remote server running VMware vSphere ESXi using HPE OneView

The SUT architecture for performing online updates of a remote Gen9 or Gen8 server running VMware vSphere ESXi is different from performing an online update of a remote Gen10 server running VMware® ESXi™.

Online update of a remote Gen9 or Gen8 server running VMware vSphere ESXi using HPE OneView



The HPE OneView online update of a remote server running VMware vSphere ESXi requires SUT for VMware vSphere ESXi to be installed in a Red Hat helper appliance, the HPE WBEM providers be installed on the remote server, and involves:

- Using HPE OneView to initiate an online update of the remote server
- HPE OneView attaching the SPP ISO to the remote server using iLO's virtual media
- SUT in the Red Hat helper appliance loading and running the SUM instance on the SPP ISO in the Red Hat helper appliance
- SUM communicating with the WBEM providers on the remote server to copy the smart components from the SPP ISO onto the VMware vSphere ESXi remote server
- SUM communicating with the WBEM providers to discover and update the firmware, drivers, and system software, using the previously copied smart components

Once the update is complete:

- SUT reports the results back to HPE OneView
- The SPP ISO is disconnected
- The remote server is rebooted, only if required by the updates

Online update of a remote Gen10 server running VMware vSphere ESXi using HPE OneView
The online update of a remote Gen10 server running VMware vSphere ESXi is not currently available. When it is available, online updates will utilize the iLO Repository update methodology described in the "Remote server update changes in Gen10 with iLO 5 and the iLO Repository" section below.

Remote server update changes in Gen10 with iLO 5 and the iLO Repository

With the release of the Gen10 servers, HPE provides two ways to perform online updates: legacy mode update and iLO Repository update.

Legacy mode update
The legacy mode update method is the traditional update method, where the updates are deployed through the OS using SUM over the production network. The legacy mode update methods are the update methods described previously in this document.

For remote Windows and Linux servers—legacy mode updates can be performed on Gen10 and older servers.

For remote VMware vSphere ESXi servers—legacy mode updates can be performed on Gen9 and older servers.

iLO repository update
The iLO repository update method is new with the introduction of the Gen10 servers and iLO 5. With the iLO repository update method the updates are deployed though iLO 5 utilizing the iLO repository and iSUT over the iLO management network. The iLO repository update method uses SUM or iLO to manage, save, deploy, and rollback install sets.

iLO repository updates require iLO 5 and therefore are only available on Gen10 servers.

Install set
An install set is a group of components—firmware, drivers, and system software—that can be applied to a server.

iLO repository
The iLO repository is a secure storage area in the iLO NAND nonvolatile flash memory embedded on the system board and is where the components are stored.

Rollbacks
A rollback is the process whereby SUM or iLO deploys a previously saved install set. The previously saved install set can be:

- An install set specified by the administrator
- A last know good install set
- The system recovery set

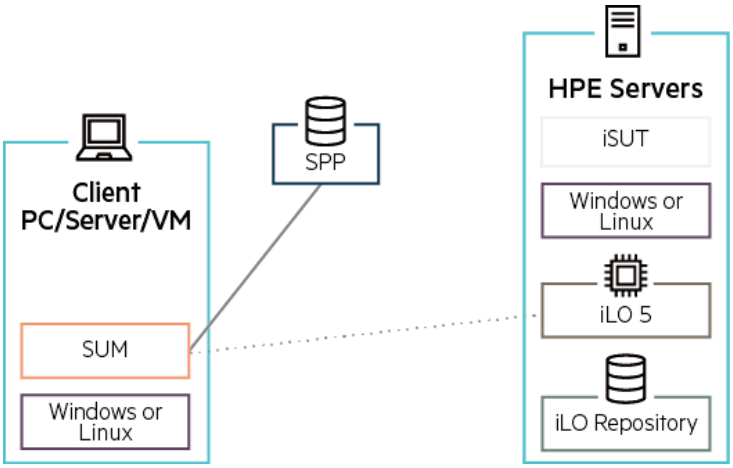
System recovery set
By default, the initial system recovery install set is the version of the components deployed when the server is built. Only iLO user accounts with the recovery set privilege can configure or modify the system recovery set.

The following firmware components are included in the default system recovery set:

- System ROM (BIOS)
- iLO firmware
- Complex Programmable Logic Device (CPLD)
- Innovation Engine (IE)
- Server Platform Services (SPS) firmware

If the default system recovery set is deleted, a user with the recovery set privilege can use SUM to create an install set, and then designate that install set as the system recovery set. Only one system recovery install set can exist at a time.

iLO repository online update of a remote Gen10 server running Windows or Linux



The iLO repository online update of a remote Gen10 server running Windows or Linux requires iSUT for Windows/Linux and the AMS management tools to be installed in the OS of the remote server and involves:

- Installing and running SUM on a client—PC, server, or VM—running Windows or Linux
- Using SUM on the client to discover the iLO of the remote Windows/Linux server
- SUM communicating with iLO 5 over the iLO management network to discover the firmware, drivers, and/or system software
- SUM communicating with iLO 5 to upload the firmware, drivers, and system software updates into the iLO Repository as an install set
- iLO 5 and the UEFI ROM deploying the firmware updates, with the exception of the hard drive and NIC firmware
- iLO 5 communicating with iSUT to deploy the rest of the firmware, driver, and system software updates

Once the update is complete, iLO 5 reports the results back to SUM and the remote server is rebooted, only if required by the updates.

iLO repository online update of a Remote Gen10 server running VMware vSphere ESXi
iLO repository online updates of a Gen10 server running VMware vSphere ESXi are not available at this time.

Resources

Products

Smart Update: hpe.com/info/smartupdate

Service Pack for ProLiant (SPP): hpe.com/servers/spp

Smart Update Manager (SUM): hpe.com/servers/sum

Smart Update Tools (SUT): hpe.com/servers/sut

Downloads

SPP Custom Download: hpe.com/servers/spp/custom

Service Pack for ProLiant (SPP): hpe.com/servers/spp/download

Documentation

Service Pack for ProLiant (SPP): hpe.com/info/spp/documentation

Smart Update Manager (SUM): hpe.com/info/sum-docs

Learn more at

hpe.com/info/smartupdate

Sign up for updates

4AA4-6947ENW, February 2018, Rev. 2