Hewlett Packard Enterprise

SUM Best Practices Planning Guide

Abstract

This document describes the best practices for performing a firmware and software update for your server environment with SUM. This document is intended for individuals who perform updates and understand the configuration and operations of Microsoft Windows, Windows Server, Linux, smart components, and the risk of data loss from performing updates.

Part Number: 658524-007
Published: November, 2016
Edition: 1

Contents

Introduction

Overview

Firmware, software, and drivers for your server environment are crucial for maintaining server systems. HPE has created the update packages to help you maintain your servers as consistently and easily as possible. Planning for your updates helps make the process go smoothly and minimizes downtime.

This document offers best practice and update planning guidelines to help plan firmware, software, and driver updates to your environment.

Explanation of SUM guides

This section describes the two Best Practices guides.

These guides are written to help you create strategies for using SUM with update packages.

- *SUM Best Practices Planning Guide*

  –Provides an outline for creating a firmware update plan to follow before updating your server environment.
- *SUM Best Practices Implementation Guide*

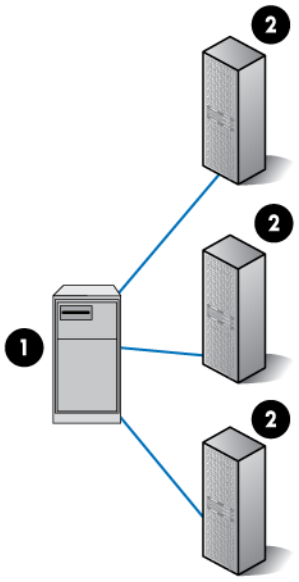
  –Provides examples for implementing an update.

You can find these guides on the SUM Information Library at **http://www.hpe.com/info/sum-docs**.

Planning for server environment scenarios

Updating one or more servers in a single physical location

If you have an environment where all the servers are in one physical location you can use one of the servers to run the server updates. You can also use a non-server workstation to run the server updates, and deploy updates to the other servers. Use the following instructions to gather the information required to create a server update plan.



Item	Description
1	Workstation
2	Server

Procedure

1. Download the update package you want to use, for example, SPP or Integrity bundle. For more information on downloading the files, see **Downloading the SPP** on page 20 or **Downloading Integrity bundles** on page 20.

   NOTE:

   The SPP and Integrity bundles include a copy of SUM. You can download the latest version of SUM from the SUM website at **http://www.hpe.com/servers/sum**.

2. Determine if you must create a custom ISO. For more information about creating a custom ISO, see **Creating a custom ISO or baseline overview** on page 21.
3. Determine which updates you need to apply. Use SUM to do the following:
   - Create a baseline.
   - Add the nodes you want to update.

- Inventory the nodes.
- Generate the **Deploy preview** report.
- Review the updates for your server.

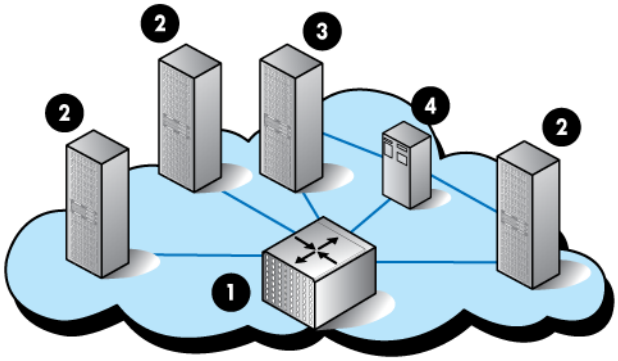
4. Determine if the software updates or new features are items you need immediately, or if you can wait for a regularly scheduled maintenance window to apply them.
5. Configure the firewall to allow remote support for SUM. You might need to enable traffic that the remote server initiates. For more information, see the *Smart Update Manager User Guide*.
6. For Windows servers, be sure that you enable file and print services. For Linux and HP-UX servers, be sure you turn on the SSH service.

NOTE:

In some cases, updating the iLO firmware separately helps decrease update duration.

Updating a single BladeSystem enclosure

This section covers the process to update a single c-Class enclosure with servers and associated interconnect modules.



Item	Description
1	Management server
2	Server
3	Enclosure
4	Storage

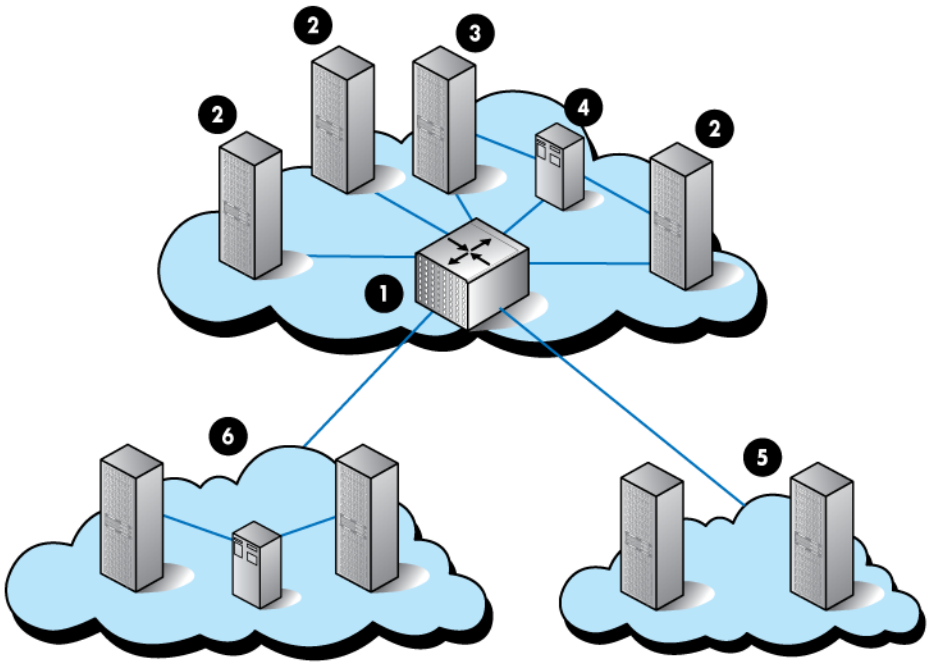
Items to consider when creating an update strategy:

- Determine the baseline to use for deployment.
- Determine if you must create a custom ISO. If so, see **Creating a custom ISO or baseline overview** on page 21 for more information.
- Determine updates to apply and use SUM to do the following:
  - Create a baseline.
  - Add the nodes you want to update.
  - Inventory the nodes.
  - Generate the **Deploy preview** report.
  - Review the updates and hot fixes.

- Determine if the software updates or new features are items you need immediately, or if you can wait for a regularly scheduled maintenance window to apply them.
- Consider methods to minimize business impact from updates. If an enclosure houses multiple departments, look for ways to coordinate updates between different business units.
- Run a health check to be sure your OA and VC firmware are ready for updates.

Updating servers for a distributed corporate customer

The distributed corporate customer has a central data center with servers at multiple remote locations.



Item	Description
1	Management server
2	Server
3	Enclosure
4	Storage
5	Remote servers
6	Two remote servers, one remote storage

Items to consider when creating your update strategy:

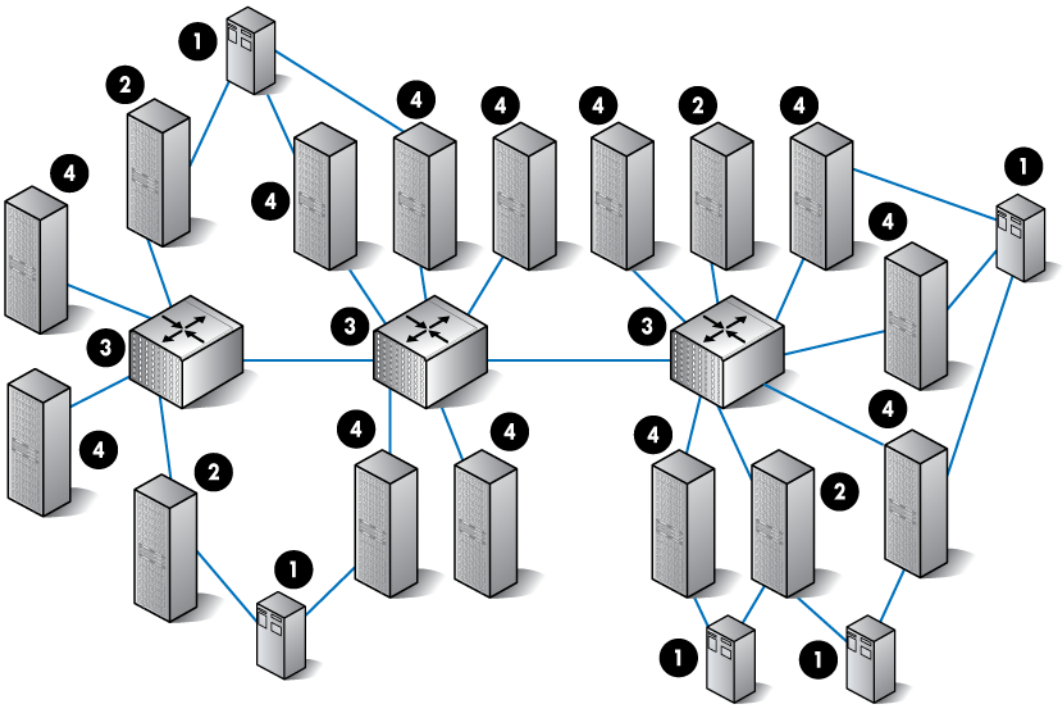
- Determine if you are creating a custom ISO. If so, see **Creating a custom ISO or baseline overview** on page 21 for more information.
- Determine updates to deploy. Use SUM to do the following:
  - Create a baseline.
  - Add the nodes you want to update.
  - Inventory the nodes.

    - Generate the **Deploy preview** report.
    - Review the updates and hot fixes for your environment.
- Determine if the software updates or new features are items you need immediately, or if you can wait for a regularly scheduled maintenance window to apply them.
- Determine how you will distributing the updates.
    - Burn DVDs or create USB keys, and then send the physical media to each remote server.
    - Copy the files to remote servers.
    - Put the ISO contents on a central server and connect to it through network connections (network share in Windows or NFS mount in Linux).
- Determine how you will perform the updates.
    - Install on each target individually.
    - Use PXE boot or iLO Virtual Media to install the SPP or Integrity bundle on servers over the network.
    - Copy the SPP or Integrity bundle to one computer, and then write a script to install it on the other local servers using SUM or iLO Virtual Media.
- Consider methods to minimize business impact from updates. It might be necessary to perform partial updates to enclosures if all servers cannot be taken out of service at once. Even when partial updates are required, follow the recommended installation order. For more information, see **Best practices to minimize server downtime** on page 17.
- Determine if you will update an existing server automatically.
- Determine if you have a lab environment set up. If you are creating your own ISO, be sure that you validate the solution before applying it to targets.
- Determine if you have a backup of the server and the configuration of other targets.
- Determine if you have the ports open to allow remote support for SUM.
- In some instances, it might help decrease the time for the updates to complete if the iLO firmware is updated independently of the other updates.

Updating servers for a large data center

This section discusses updating a large data center that includes multiple enclosures, servers, and other components located in several locations.

Large data center illustration



Item	Description
1	Storage
2	Enclosure
3	Management server
4	Server

The following list contains items to consider when creating your update strategy:

- Determine what firmware, software, and driver versions are you using on your servers. Run SUM to create a report.
  - Create a baseline.
  - Add the nodes you want to update.
  - Inventory the nodes.
  - Generate the **Firmware details** report.
  - Generate the **Deploy preview** report to view available updates for the nodes.
- Determine if you are creating a custom ISO. If so, see **Creating a custom ISO or baseline overview** on page 21 for more information.
- Determine how you group models in your data center. Group the same server models and technologies together in update groups. For example, group all ProLiant G5 servers together, and all ProLiant G1 servers together.
- If you have multiple generations of servers in an enclosure, try not to mix servers that are more than two generations apart in the same enclosure. For example, enclosures that include ProLiant Gen8 and Gen9 server blades should not include ProLiant G6 server blades in them. The three main reasons for this are:

- New generations of blades usually have more updates than older blade generations so updating the enclosures where these older blade generations coexist can lead to extra downtime for these older server blades when the infrastructure is updated.
- As servers age and the number of updates released are reduced, it is best to create a baseline for the servers at a given level of firmware and software and not update them unless there is a need to re-provision them. This reduces the number of servers that need to be updated when a new baseline is introduced to the environment.
- It helps minimize dependencies between different generations of servers that might affect the success of the firmware update process.

- Determine how you deploy updates.
  - Verify that updates apply to your servers and targets.
  - The number of updates that support a server decreases over time. Check the update information to be sure the firmware and software updates apply to your server generations. Most updates affect the latest generation.
- Determine if you have third-party vendor equipment in your environment. If so, be sure that updates you apply are supported by HPE and your third-party vendor.
- Consider methods to minimize business impact from updates. Schedule any outages. It might be necessary to perform partial updates to enclosures if you cannot update all at once. Even when partial updates are required, follow the installation order. For more information, see **Best practices to minimize server downtime** on page 17

  .

CloudSystem and CloudSystem Matrix

Helion CloudSystem overview

Helion CloudSystem operates with supported and current HyperVisors from third-party vendors. Driver deployment, firmware deployment, and implementation best practices are influenced and dictated by the same HyperVisor support processes per supported hardware/server platform.

For more information on Helion CloudSystem, see **http://www.hpe.com/info/cloudsystem**.

CloudSystem Matrix overview

CloudSystem Matrix, built on HPE BladeSystem architecture, is a converged infrastructure platform for shared services. CloudSystem Matrix delivers one virtualized pool of network, storage, and computer resources that enables you to adjust to dynamic business demands by provisioning and modifying a complex infrastructure in minutes rather than days, weeks, or even months.

CloudSystem Matrix combines automated design and provisioning through a self-service portal with capacity planning and disaster recovery into a command center that unites your physical and virtual worlds.

To assist you in setup, HPE Services provides a three-step service to achieve full conversion:

1. Initial assessment.
2. Site-specific preparation.
3. Conversion to CloudSystem Matrix.

For more information, see the CloudSystem Matrix website at **http://www.hpe.com/info/matrixoe**.

HPE Services overview

This section is an overview of the Lifecycle Event Services for the firmware update best practices documents.

HPE Services can help you optimize business results with consulting, outsourcing, and support services. For more information about services available, go to the Services website at **http://www.hpe.com/services**.

Planning maintenance and update best practices

Planning maintenance and update best practices overview

The best practices mentioned here are recommendations that work for most environments. Modify your update plans based on your unique environment. The tips listed below provide a recommended approach and general guidance. You can derive specific steps when you consider both operational maintenance needs and consistent update success.

Use the following sections for specific planning input for single or multi-server and site deployment scenarios.

General server deployment planning

- Review the available documentation about performing updates, including the

  SUM Best Practices Implementation Guide and *Smart Update Manager User Guide* at **http://www.hpe.com/info/sum-docs**.
- Determine the currently installed software and firmware versions:
  - Create a baseline, for example an SPP or Integrity bundle.
  - Add the nodes you want to update.
  - Inventory the nodes.
  - Generate the **Firmware details** report.
  - Generate the **Deploy preview** report to view available updates for the nodes.
- Create a process to manage your updates.
- Define a set of updates to apply across all server and enclosures. You can also create a custom baseline that includes only updates for specific servers.
- Determine how frequently you update the node baseline.
- Determine whether there are any dependencies and interim updates you will need to apply.
- Review the critical updates for your server:
  - For more information about SPP updates, see the SPP website at **http://www.hpe.com/servers/spp**.
  - For more information about Integrity bundles, see *Manage HPE Integrity Servers Firmware Updates* at **http://www.hpe.com/info/smartupdate/integrity**.
- Consider methods to minimize business impact from updates. For example, perform partial updates to enclosures or clustered environments if all servers cannot be taken out of service at once.
- Back up all nodes you are going to update.
- Configure the firewall to allow two-way communication between the host running SUM and the node you are updating. For more information, see the Network ports section of the *Smart Update Manager Release Notes* at **http://www.hpe.com/info/sum-docs**.
- Permit anti-virus applications to allow SUM and other tools to deploy updates.
- For Windows servers, enable file and print services. For Linux and HP-UX servers, enable the SSH service.
- In some instances, it might help decrease the time for the updates to complete if the iLO firmware is updated independently.
- Test your environment in a lab before rolling into the production environment:
  - In CLI mode, use the `/dryrun` attribute to simulate an installation.
  - If you do not have a lab, choose one server to update and run the server for a few days under a normal workload. When the server proves stable, update the remaining servers in your environment.

Server update planning

Before you start updating servers

Procedure

1. Backup the server before starting an update.
2. Use SUM to generate reports of firmware and software currently installed on targets. Use the report to determine recommended updates for each target before deploying updates.

   NOTE:

   Some updates require an offline update. For information on which updates require offline updates, see the *Support Pack for ProLiant Release Notes*.

Updating the servers

Procedure

1. Deploy drivers concurrently with firmware updates to ensure dependencies are fulfilled. If you must deploy firmware or software separately, use the following order:
   - Update drivers first.
   - Update additional software, such as agents and utilities.
   - Update the firmware.

   Do not downgrade or rewrite firmware unless there is a specific need to do so.

   NOTE:

   Downgrading firmware might cause incompatibilities between devices if the downgraded firmware does not work well with other device firmware or drivers.
2. Use a USB or network file share to add or remove software and firmware.
3. For new servers, update the firmware before installing the operating system. You might need to run the updates twice to install the most recent updates.
4. Reboot the server after server-based firmware, software, or driver upgrades. This clears the memory and allows the update component to start fresh.

Testing the updated environment in a lab

Before you put the updated servers into the production, test your environment.

Procedure

1. Use `/dryrun` from the command line in SUM to simulate an installation.
2. If you do not have a lab, choose one server to update and run the server for a few days under a normal workload. When the server proves stable, update the remaining servers in your environment.

BladeSystem enclosure and server planning

- If possible, do not mix servers that include more than two generations difference in the same enclosure. For example, if your enclosure includes ProLiant G6 and G7 servers, do not add ProLiant Gen9 servers.

NOTE:

If you update enclosures that mix multiple generations, plan for more downtime for server blades when you perform updates.

- As servers age, fewer critical updates and hot fixes are released. Create a baseline with the firmware, software, and drivers used for each server.
- Ensure that the NIC firmware included in a release set is supported by the operating system vendor and external network switch vendors before updating it. Review the following known issues:
  - A purple screen (PSOD) occurs on some 10GbE adapters. For more information, see the customer advisory website at **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c02496982**.
  - Updating Broadcom 1GbE drivers for Windows Servers requires first updating to version 4.6.16.0. For more information, see the customer advisory website at **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c01684544**.
  - Emulex be2net Inbox Driver version 4.0.88.0 does not support Flex-10 or Flex Fabric Adapters. For more information, see the customer advisory website at **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c03005737**.

NOTE:

Some Broadcom firmware updates require you to update the driver and reboot the system to activate the driver before you can update the firmware.

- Do not update servers unless you need to re-provision a server. This reduces the number of servers you update when you introduce a new baseline.
- Integrity and ProLiant servers might have different OA and VC firmware version requirements.
- Consider these known issues:
  - ProLiant G2, G5, and G6 server ROMs dates May 2011 and later cannot be downgraded without using special steps. For more information, see the customer advisory website at **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c02838375**.
  - CPLD firmware for ProLiant G7 and earlier servers require you to physically remove the power source for 30 seconds before an update activates.
- Ensure that the FC HBA firmware included in a release set is supported by the external storage vendor before you update the FC HBA. For more information about comparing supported HBA driver versions and storage devices, see the Single Point of Connectivity Knowledge (SPOCK) website at **http://www.hpe.com/storage/spock**.
- Gen8 and Gen9 servers: Review the *SPP Release Notes* and VMware firmware recipe documentation before creating a custom baseline or ISO to deploy updates. For more information see: **http://www.hpe.com/info/spp/documentation** and **http://vibsdepot.hpe.com/hpq/recipes/**.

VC firmware planning

- Check the compatibility matrix before you update an enclosure in mixed environments.
- Run a health check before you update OA or VC firmware.
- Verify that firewall programs are not blocking VC firmware updates.
- Be sure that you update profiles if you move blades around and between enclosures.
- Review the latest VC release notes for any VC firmware release to determine any firmware and driver changes needed for Ethernet, FC HBA, and CNA adapters in the servers. For more information about Virtual Connect release notes, see the Virtual Connect website at **http://www.hpe.com/info/vc/manuals**.
- General guidance does not mandate the use of either SUM over Virtual Connect Software Utility (VCSU). See the following document on the Hewlett Packard Enterprise website for more information whether to use SUM or VCSU: **http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=c02885443**.
- Be sure that the VC modules are set up in a redundant configuration.
- Use VCSU to update modules that are not set up in a redundant configuration.

- Monitor customer advisories for VC firmware update issues.
- Validate the NICs and the FC HBA and CNA firmware and driver compatibility.

ProLiant iLO planning

- iLO 4 firmware, use version 2.03 or later. This resolves issues from previous iLO 4 versions.
- iLO 3 firmware cannot be downgraded from version 1.25 to an earlier version without the downgrade resetting some configuration data to the default value.
- iLO 3 firmware 1.25 can cause a condition where the power is incorrectly reported and might prevent some blades from powering on in a fully populated enclosure. Version 1.26 resolved this issue.
- Event ID 57 errors are corrected for iLO 2 by using firmware version 1.82 or later and ProLiant iLO 2 Management Controller Driver for Windows 1.12.0.0 or later.
- iLO 2 firmware 1.78 or later is required to update Power Management Controller firmware.
- You cannot update iLO 2 firmware 2.00 through the iLO NIC Management interface.
- Use iLO 2 firmware 1.81 or later to update CPLD firmware (ProLiant ML/DL300 series servers).

Best practices to minimize server downtime

The best practices mentioned here are recommendations that work for most environments. Modify your update plans based on your unique environment.

Server downtime causes

The following items frequently cause downtime when you perform updates.

- Driver installation requires a reboot to load the driver.

  NOTE:

  You can deploy some updates online that immediately activate. The activation process might cause a short network connectivity timeout. This might cause some applications that are sensitive to network connections to incur an issue. If you are using applications that are sensitive to network disconnections, only deploy updates during regular maintenance windows.

- Firmware updates require a reboot to activate the new firmware.
- Firmware updates require exclusive access to hardware.
- Dependencies between updates require offline deployment.
- Hot fixes and customer advisories.
- The method of installation.

Node-specific tips to reduce downtime

The following tips help develop a server update plan that minimizes downtime.

OA tips to reduce downtime

- Before performing an OA update, perform a VC health check. If you update the OA when the VC is in an unhealthy state, you risk losing the network connection.
- If using OA version 1.x, you must update to 2.32 before updating to newer versions.

Server tips to reduce downtime

- Use a well-tested baseline, preferably the SPP or Integrity bundle.
- Check for ProLiant hot fixes or Integrity bundles classified as critical or recommended that apply to your systems.
- Perform updates online using SUM or SIM first. This limits, or eliminates, the number of updates required in offline mode.
- Perform infrastructure updates in parallel or prior to performing updates to servers.
- Install the firmware and drivers together. This allows a single reboot to activate the maximum amount of updates.
- If you are using iLO Virtual Media to deploy the updates, update iLO firmware through the iLO web GUI or scripting. For more information, see the *iLO 4 User Guide* or *iLO 4 Scripting and Command Line Guide*, available at **http://www.hpe.com/info/ilo/doc**.
- Update HP-UX and iLO targets on Integrity racks or blade servers. Set SUM to perform reboots to activate the new firmware automatically. SUM will order the updates so only one reboot is required to activate the firmware on both targets.
- Update HP-UX running on nPartitions and partition firmware through the OA in the same SUM session. Set SUM to perform reboots to activate the new firmware automatically. SUM orders the updates and performs one reboot to activate the firmware on both targets.

Enclosure tips to reduce downtime

If you are deploying updates through iLO vMedia in an enclosure, do not update more than 6-8 blades at the same time.

Enclosure Installation tips to reduce downtime

- Online updates enable you to stage multiple updates and reboot once to activate the updates.

  NOTE:

  Some updates require an offline update. For more information, see the *Support Pack for ProLiant Release Notes* at **http://www.hpe.com/info/spp/documentation**.

- Upgrade drivers and firmware at the same time. This minimizes problems that might occur if there are interdependencies between firmware and drivers.
- The number of baselines you use and the number of nodes you update impact the system resources the host system requires. The Input file mode requires fewer resources than GUI mode.
- Use HPE SIM to deploy updates when you are updating more than 50 nodes concurrently.
- New ProLiant hardware deployments require offline updates.

Firmware and software deliverables overview

Release sets overview

Release sets are collections of firmware, software, drivers, and other updates that are released together. SPP, Integrity bundles, and Moonshot Component packs are deliverables that include firmware sets.

Service Pack for ProLiant overview

SPP is a comprehensive systems software (drivers and firmware) solution delivered as a single package with major server releases. This solution uses SUM as the deployment tool and is tested on all supported ProLiant servers including ProLiant Gen9 and later servers.

SPP can be used in an online mode on a Windows or Linux hosted operating system, or in an offline mode where the server is booted to an operating system included in the ISO file so that the server can be updated automatically with no user interaction or updated in interactive mode.

For more information or to download SPP, see the Service Pack for ProLiant page at **http://www.hpe.com/servers/spp**.

SPP release naming overview

SPP versions are named by the year and month that the SPP was released, followed by an identifier. For example, `SPP2015.10.0` was the first SPP released in October 2015.

Check the SPP release notes for information on the support policy. For more information, see the website at **http://www.hpe.com/info/spp/documentation**.

Adding or removing components from SPP

Each SPP contains a baseline set of components that have been tested together and are supported for one year from the release of the SPP, or for five SPP releases, whichever comes first. You can create a custom baseline by adding or removing components from the SPP to:

- Incorporate a hot fix that was released after the SPP was released.
- Ensure that only necessary files are loaded onto the system, which can make tracking changes easier if troubleshooting is required.
- Match the compatibility list with third-party products. For example, if Hewlett Packard Enterprise releases an update to your FC HBA, but the vendor of your external switch does not support the Hewlett Packard Enterprise version, you can remove this update to continue to receive support from the switch vendor.
- Make the baseline smaller so fewer system resources are required.

For more information on creating a custom ISO, see **Creating a custom ISO or baseline overview** on page 21.

NOTE:

SUM 7.x and higher supports creating custom baselines and bootable ISOs. For more information on creating custom baselines and ISOs, see the *Smart Update Manager User Guide* available at **http://www.hpe.com/info/sum-docs**.

You can download the latest version of SUM from: **http://www.hpe.com/servers/sum**.

Downloading the SPP

Procedure

1. In a web browser, go to the SPP website at **http://www.hpe.com/servers/spp/download**.
2. Click the version of the SPP you want to download.
3. Click **Download** next to the SPP ISO you want to download.
4. Click **Obtain Software**. Downloading the software requires an active warranty, HPE Care Pack, or support agreement linked to your HPE Passport.

Integrity firmware bundles overview

The Integrity website includes updates for servers as specific system downloadable bundles. For more information on the bundles, see the Integrity website at **http://www.hpe.com/info/integrity**. On the support page for each server, there are two bundles for each firmware release. Use the bundle for the operating system of the management station where you run SUM. Both bundles can update Integrity servers running any operating system because updates are performed through the management interfaces. Use one bundle when you run SUM on a Windows management server to update Integrity servers on the network. Use the other bundle when you run SUM on a Linux management server to update Integrity servers on that network. Both bundles contain the same target server firmware.

You can download the latest version of SUM from: **http://www.hpe.com/servers/sum**.

After you download a bundle, extract the file into empty directory. If you need to update using multiple Integrity bundles, download and extract each bundle into its own empty directory. Run SUM from the latest bundle you downloaded. In SUM, add all bundles to the Baseline Library screen. For more information, see the *Smart Update Manager Online Help* or *Smart Update Manager User Guide*.

SUM provides installation logic and version control that automatically checks for dependencies, and installs only the correct updates for optimal configuration.

Downloading Integrity bundles

Procedure

1. In a web browser, go to **http://www.hpe.com**.
2. Click **Support & Drivers**.
3. Click **Drivers & Software**.
4. Enter your product name or number, and then press **Enter**.
5. Select your product from the list.
6. Click **Cross operating system (BIOS, Firmware, Diagnostic, etc.)**.
7. Choose the firmware, and then click **Download**.

Moonshot Component Pack

Moonshot Component Pack is a comprehensive firmware solution tested on the Moonshot System and delivered as a compressed file. The compressed file includes all the component files needed to update a Moonshot System. Users deploy the firmware updates contained in the Moonshot Component Pack via the iLO Chassis Manager CLI or Moonshot-45G/180G Switch Module CLI. This can be accomplished using SUM, which is included with the files, or manually.

Downloading the Moonshot Component Pack

Procedure

1. In a web browser, go to the Moonshot website at **http://www.hpe.com/servers/moonshot/download**.
2. Click the Full Component Pack version.
3. Follow the instructions on-screen.

Creating a custom ISO or baseline overview

Instructions and reasons to create a custom ISO.

SUM 7.0.0 and later supports creating custom baseline and bootable ISOs with components that you select. Custom baselines and ISOs allow you to:

- Minimize the size of the baseline you are deploying.
- Create a standardized baseline for specific environments.
- Minimize the required system resources required to deploy updates.

Custom SPP downloads overview

The SPP website allows you to generate filtered SPP ISOs that include only the components you want to deploy. Similar to the creating a custom baseline in SUM, this function allows you to generate downloads that do not include components that don't apply to your environment. To create a custom SPP download, go to the SPP website at **http://www.hpe.com/servers/spp/download** and then click **SPP Custom Download**.

Update tools

SUM overview

SUM is included in many update bundles for installing and updating firmware and software on ProLiant servers, and firmware on Integrity and Moonshot servers.

SUM provides a web-based GUI, interactive command-line, and a command-line scriptable interface for:

- Deployment of firmware for single or one-to-many ProLiant and Integrity servers and network-based targets such as iLO, OA, and VC Ethernet and Fibre Channel modules.
- Deployment of software for single or one-to-many ProLiant servers (supported in Windows and Linux environments).

SUM has an integrated hardware and software discovery engine that finds the installed hardware and current versions of firmware and software in use on nodes you identify. SUM installs updates in the correct order and ensures that all dependencies are met before deploying an update. SUM prevents an installation if there are version-based dependencies that it cannot resolve.

Key features of SUM include:

- Dependency checking, which ensures appropriate installation order and component readiness.
- Automatic and wizard-like Localhost Guided Update process.
- Web browser based application.
- Create custom baselines and ISOs.
- Download updates from the web.
- Intelligent deployment of only required updates.
- Simultaneous firmware and software deployment for multiple remote nodes in GUI, interactive CLI, and CLI modes.
- Improved deployment performance.
- Local online deployment of ProLiant servers and enclosures.
- Remote (one-to-many) online deployment of ProLiant and Integrity servers and enclosures directly to each server or using Scalable Update powered by iLO Federation.
- Local offline firmware deployments with Service Pack for ProLiant deliverables.
- Remote offline deployment when used with Scalable Update powered by iLO Federation, the SmartStart Scripting Toolkit (ProLiant G7 and earlier servers), Scripting Toolkit (ProLiant Gen8 and later), iLO Virtual Media, or PXE booted media.
- Support for deploying firmware updates to supported Integrity servers and Superdome 2 enclosures.
- Support for updating VC modules on Integrity servers.

  NOTE:

  SUM does not support third-party controllers. This includes flashing hard drives behind these controllers.

- Remote online deployment of I/O Card firmware on ProLiant and Integrity targets running HP-UX

For information about SUM, see *Smart Update Manager User Guide*, available on the SUM documentation website at **http://www.hpe.com/info/sum-docs**.

HPE SIM and Version Control Agent overview

HPE SIM enables system administrators to manage their systems. It provides hardware level management for ProLiant, Integrity, and 9000, BladeSystem servers, and MSA, EVA, and XP storage arrays. HPE SIM enables

you to quickly determine if a server is in alignment with a given baseline. With the HPE SIM built-in report generation capabilities, you can quickly generate reports that show which servers are out of date.

For more information, see the HPE SIM website at **http://www.hpe.com/info/hpesim**.

NOTE:

An MDS600 firmware update requires that all blades, except the blade performing the update, be powered off before you begin the firmware update.

OneView overview

Optimized for collaboration, productivity, and reliability, the OneView application is designed to provide simple, unified lifecycle management for the complex aspects of enterprise IT—servers, networking, software, power and cooling, and storage.

Architecture

OneView is delivered as a virtual application running in a VMware vSphere or Microsoft Hyper-V virtual machine.

In contrast to management environments that require predefined serialized workflows and different tools for different tasks, OneView is a scalable resource-oriented solution focused on the entire life cycle—from initial configuration to on-going monitoring and maintenance—of both logical and physical resources:

- Logical resources are items such as networks, server profiles, and connections.
- Physical resources are items you can touch, such as server hardware, interconnects, and enclosures.

Software-defined flexibility—your experts design configurations for efficient and consistent deployment

The application provides several software-defined resources, such as groups and server profiles, to enable you to capture the best practices of your experts across a variety of disciplines, including networking, storage, hardware configuration, and operating system build and configuration. By having your experts define the server profiles and the networking groups and resources, you can eliminate cross-silo disconnects. By using role-based access control (RBAC) and the groups, sets, and server profiles established by your experts, you can enable system administrators to provision and manage thousands of servers without requiring that your experts be involved with every server deployment.

One tool and one data set

OneView combines complex and interdependent data center provisioning and management into one simplified and unified interface. You use one tool and one model to:

- Provision the data center.
- Manage and maintain firmware and configuration changes.
- Monitor the data center and respond to issues.

The solution also provides core enterprise management capabilities, including:

- Availability features.
- Security features.
- Graphical and programmatic interfaces.
- Integration with other Hewlett Packard Enterprise management software.

BladeSystem c-Class VCSU overview

BladeSystem c-Class VCSU enables administrators to perform the following tasks:

- Upgrade VC Ethernet and VC-Fibre Channel module firmware.
- Perform other maintenance tasks remotely on VC Ethernet and Fibre Channel modules installed in both the BladeSystem c-Class c7000 and c3000 enclosures using a standalone Windows or Linux-based CLI.

Sometimes you must use VCSU instead of SUM to update a VC module.

When VCSU initiates a firmware upgrade process, all modules can be updated at the same time, or the updates can be alternated between left and right modules so that network and SAN connectivity is not disrupted during the upgrades. The utility displays a message indicating that an update is in progress and the percentage completed. After the module firmware updates are complete, the utility activates all modules. VCSU minimizes outage time in the network fabric and can eliminate an outage if the VC modules are installed in redundant pairs.

To locate the latest version of VCSU:

1. Open a web browser and go to **http://www.hpe.com**.
2. Click **Support and Drivers**.
3. Select **Download drivers and software (and firmware)**.
4. Enter BladeSystem c-Class VCSU and press **Enter**.
5. Select the VC module type.
6. Select the operating system for updating the VC module. Always perform a health check of the VC modules you are going to update before initiating the firmware update process.

NOTE:

SUM leverages VCSU included in the VC firmware component to deploy VC firmware updates.

When to use BladeSystem c-Class VCSU

Use VCSU if one of the following applies to a VC module:

- Unhealthy state—SUM reports a module as unhealthy during discovery on the Select Targets screen.
- Force the same version—SUM does not allow you to force rewrite the same firmware version.
- Downgrade VCM—SUM does not allow you to force downgrade VC firmware.
- Update single module—SUM does not allow you to update only a single module.
- Non-redundant configuration—If SUM detects that the VC module is non-redundant, it will not allow you to perform any updates. This prevents an accidental server outage.
- Not part of a domain—SUM alerts you if the VC module is not part of a domain. SUM requires the VC module to be part of a domain to perform discovery.
- Change activation order—If you want to change the activation order, insert time delay for VC modules, or choose other non-default options.
- The VC modules are managed by VCEM—If VC module is managed by VCEM, you need to put the VC module into maintenance mode. After changing to maintenance mode, rescan the VC module in SUM and continue with the update.
- Do not use VCSU on enclosures managed by OneView. OneView manages VC firmware updates.

Microsoft SCCM 2007 overview

Microsoft SCCM 2007 enables customers to use SCCM for update management and distribution of ProLiant server system software and PSPs. See the documentation that comes with SCCM for instructions on how to manage updates with SCCM.

HPE has developed an Updates Catalog cabinet file (`ProLiant.cab`) containing an XML file that conforms to the Microsoft update format to describe updates available from Hewlett Packard Enterprise. This cabinet file enables SCCM to understand and interpret the update status for ProLiant servers. You can monitor ProLiant server update status and authorize and deploy software updates to servers. Deployment of PSPs is comprehensive. You receive the benefit of deploying PSPs, which are tested together to ensure a smooth installation. Using the SCUP tool, the catalog can be imported into the SCCM server. The SCCM server can

deploy software from the imported catalog to client servers. SCUP works with the WSUS and SCCM. It is a separate installation by the administrator.

Managing and deploying ProLiant SmartStart components and ProLiant Support Packs only requires SCCM 2007, WSUS, and SCUP installation. SCCM, WSUS, and SCUP must be installed and verified before managing updates. See the documentation for detailed SCCM, WSUS, and SCUP setup information on the Microsoft website at **http://www.microsoft.com**.

The Server Updates Catalog should be used for monitoring and deploying software and firmware upgrades, as well as new and upgrade installations of the SPP. Initial installations for individual software and firmware are not supported due to the complexity of inter-component dependency. Deployment of PSP is recommended for newly-configured ProLiant servers to ensure all relevant software is installed.

SCCM 2007 uses the WSUS infrastructure for delivering software updates to managed devices. Though some of the user experience is similar to SMS 2003, the architecture is different and uses a custom HP-provided scan tool along with standard packages and advertisements. The new SCCM infrastructure does not support the SMS 2003 Inventory Tool for ProLiant and Integrity Update.

Use SCCM to update SPPs, software updates, and specific firmware updates. If you have SCCM, you need additional tools to complete firmware updates.

NOTE:

SCCM cannot be used to update firmware on non-server targets, for example, OA, VC, and other enclosure interconnects.

VMware ESXi firmware updates

VMware ESXi 5.0 and later firmware updates

SUM 7.1.0 and later supports online firmware and driver updates for VMware ESXi 5.x and later targets. Run SUM on a Windows or Linux host system, and update your VMware targets over a network. VMware updates are available in the SPP. For more information on released components, see the *Support Pack for ProLiant Release Notes*. A recommended list of drivers and firmware for ProLiant servers running VMware ESXi 5.x and later is available in, the VMware Firmware and Software Recipe at **http://vibsdepot.hpe.com**.

SUM requires the WBEM Providers for VMware ESXi to update the VMware targets. For information on using SUM to update VMware targets, see the *Smart Update Manager User Guide*.

Collecting current server or enclosure configurations

Creating a database or spreadsheet of your current server or enclosure configurations before and after an update will help you to audit your systems, or troubleshoot if you run into problems after an update.

SUM includes functions that enable you to create reports automatically from the command line or the SUM GUI. For more information, see the *Smart Update Manager User Guide* on the SUM documentation website at **http://www.hpe.com/info/sum-docs**.

Support and other resources

Websites

General websites

Hewlett Packard Enterprise Information Library	**www.hpe.com/info/EIL**
Smart Update Manager	**www.hpe.com/servers/sum**
Smart Update Manager Downloads	**www.hpe.com/servers/sum-download**
Smart Update Manager Information Library	**www.hpe.com/info/sum-docs**
Smart Update Tools	**www.hpe.com/servers/sut**
Smart Update Tools Information Library	**www.hpe.com/info/sut-docs**
Service Pack for ProLiant	**www.hpe.com/servers/spp**
Service Pack for ProLiant documentation	**www.hpe.com/info/spp/documentation**
Service Pack for ProLiant downloads	**www.hpe.com/servers/spp/download**
Service Pack for ProLiant custom downloads	**www.hpe.com/servers/spp/custom**
HPE SDR site	**downloads.linux.hpe.com**

For additional websites, see **Support and other resources**.

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

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

Accessing updates

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

Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Hewlett Packard Enterprise Support Center: Software downloads	**www.hpe.com/support/downloads**
Software Depot	**www.hpe.com/support/softwaredepot**

- To subscribe to eNewsletters and alerts:

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

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected	**www.hpe.com/services/getconnected**
HPE Proactive Care services	**www.hpe.com/services/proactivecare**
HPE Proactive Care service: Supported products list	**www.hpe.com/services/proactivecaresupportedproducts**
HPE Proactive Care advanced service: Supported products list	**www.hpe.com/services/proactivecareadvancedsupportedproducts**

Proactive Care customer information

Proactive Care central	**www.hpe.com/services/proactivecarecentral**

Proactive Care service activation	**www.hpe.com/services/proactivecarecentralgetstarted**

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options	**www.hpe.com/support/ProLiantServers-Warranties**
HPE Enterprise Servers	**www.hpe.com/support/EnterpriseServers-Warranties**
HPE Storage Products	**www.hpe.com/support/Storage-Warranties**
HPE Networking Products	**www.hpe.com/support/Networking-Warranties**

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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

Acronyms and abbreviations

CNA	Converged Network Adaptor
CPLD	Complex Programmable Logic Device
DHCP	Dynamic Host Configuration Protocol
DNS	domain name system
EFM	Enclosure Firmware Management
HBA	host bus adapter
HPE SIM	HPE Systems Insight Manager
iLO	Integrated Lights-Out
ISO	International Organization for Standardization
KVM	keyboard, video, monitor
MSA	Modular Smart Array
NVRAM	non-volatile random access memory
OA	Onboard Administrator
PXE	Preboot Execution Environment
PXE BOOT	Preboot eXecution Environment Enable/Disable utility
RIBCL	Remote Insight Board Command Language
RPM	Red Hat Package Manager
SAS	serial attached SCSI
SATA	serial ATA
SCCM	System Center Configuration Manager
SCP	secure copy
SOAP	Simple Object Access Protocol
SPP	Service Pack for ProLiant
SUV	serial, USB, video
TPM	Trusted Platform Module
UID	unit identification light
USB	universal serial bus
VC	Virtual Connect
VCA	Version Control Agent
VCRM	Version Control Repository Manager
VCSU	Virtual Connect Support Utility
VM	Virtual Machine
VSM	Virtual SAS Manager

Table Continued

WBEM	Web Based Enterprise Management
WMI	Windows Management Instrumentation