

Hewlett Packard
Enterprise

Smart Update Manager 8.5.0 User Guide

Abstract

This guide describes how to use SUM to apply firmware, driver, and system software updates to HPE ProLiant, HPE BladeSystem, HPE Synergy, and HPE Apollo servers and infrastructure and is intended for individuals who understand the configuration and operations of Microsoft Windows, Linux, VMware, smart components, and the risk of data loss from performing updates.

Part Number: 881504-008
Published: December 2019
Edition: 1

© Copyright 2009, 2019 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

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

UNIX® is a registered trademark of The Open Group.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Introduction 7
- Smart Update Manager 7
- Scaling SUM updates in your environment 7
- About the GUI 7
- Status icon descriptions 9

Downloading SUM 10
- Files included in the SUM download 10
- Downloading SUM from the Hewlett Packard Enterprise website 10
- Downloading an SPP Custom Download 10
- Downloading SUM from the SDR website 11
- Migrating node information to the current SUM version 11
- SUM and SPP boot environments 11

SUM modes 13
- SUM modes 13
- Deployment modes 13
- Deployment scenarios 14
- Deploying firmware for ProLiant servers using the SPP 15
- Deploying HPE Synergy with SUM 15

Log files and changing directory locations 16
- Collecting log files in SUM Online mode 16
- Collecting log files in SUM Offline mode 16
- SUM log file locations 16
- SUM log locations 17
- GatherLogs 18
- Using the `sum.ini` file 18
  - Editing the default `sum.ini` file 19
  - Creating a `sum.ini` file 19
  - Changing the temporary directory 19
  - `sum.ini` file parameters 19

Launching SUM 21
- About web browser security certificate 21
- Importing the security certificate to Firefox 21
- Importing the security certificate to Google Chrome 21
- Importing the security certificate to Internet Explorer 21
- Launching SUM 22
  - Launching SUM in GUI mode from an ISO 23
  - Launching SUM from the RPM 23
  - Using a PXE server to deploy updates 23
  - HPE Firmware Pack for ProLiant 25
- Using a different version of SUM with an SPP ISO 26

Disabling BitLocker to permit firmware updates (Windows only) 26
About using SUM with BitLocker 27
Linux root credentials for remote nodes 28
Prerequisites for using Linux sudo credentials 28
Using an SSH keyfile with root credentials 29
Logging into SUM from the GUI 29

Closing SUM 30
Logging out of the SUM GUI 30
Clearing the SUM cache 30

Using the SUM GUI 31
SUM Home screen 31
SUM Activity screen 31
SUM Localhost Guided Update 31
Using Localhost Guided Update in Interactive mode 31
Using Localhost Guided Update 32
SUM Baseline Library screen 33
About SUM baselines 34
Adding a baseline 34
Creating a custom baseline and ISO 35
Generating baseline reports 39
Validating a baseline 39
Re-validating baseline components 39
Deleting a baseline 40
Baseline addition or inventory cancellation 40
Component configuration 40
Configuring components 41
Configuring and Exporting Components 41
Importing component configuration settings 42
SUM Nodes screen 42
About node status 43
Viewing LiveLog information 43
Adding a node 43
Adding a single node by IP or DNS name 44
Adding a node by searching a range of addresses 45
Adding nodes with an input file 46
Associated nodes deployment behavior 46
Node-specific additional details 48
Editing a node 50
Performing node inventory 51
Deploying a node 51
Absaroka vs online update through OS 54
Auto-retry component update failures 54
Server updates through iLO 5 54
iLO Repository 55
Install sets 55
System Recovery Set 55
Creating a system recovery set 55
iLO 5 Gen10 security states 56
Deploying to and managing iLO Repository with SUM 56
Generating node reports 57
Deleting a node 58

Server overview....58
Node Groups screen....58
Adding a node group....58
Editing a node group....59
Performing node group inventory....59
Deploying a node group....60
Generating node group reports....60
Deleting a node group....61

Updating SUM from command lines....62

Deploying firmware components....63
Installing VMware software Smart Components on Gen10 using SUM and iSUT....64

Advanced topics....66
Using SUM with IPv6 networks....66
SUM network ports used....66
Changing the port address in the `.ini` file....67

SUM engine troubleshooting....69
SUM stops responding....69
SUM unexpectedly logs off users....70
SUM displays component failed validation error....70
SUM displays zero free space on a drive....71
Text is not translated....71
SUM restricts multiple connections to a server or shared resource by the same user....71
SUM reports port errors....72
Browser closes connection with SUM....72
SUM does not allow user to log off as expected....72

Baseline troubleshooting....73
SUM displays a dependency error for self-inventory components....73
SUM does not validate a component....73
SUM displays multiple versions of the same component....73
Custom baseline screen does not display node types....74
SUM does not save baselines after a Remote Desktop session....74
SUM does not validate HTTP baselines....74
SUM screens display outdated information....75
SUM refreshes the browser when adding a baseline....75
Baseline inventory does not respond for SPP ISO....75

Node troubleshooting....76
Google Chrome crashes frequently on the Nodes page....76
SUM dependency issues....76
Unable to add a node in High Security mode....77
SUM does not add an SMB-enabled Linux node with Unknown node type....77
SUM has an issue with sudo user....77
The SUM **Deploy** button is disabled....78
SUM node inventory fails....78

SUM does not detect a component 79
Linux hosts do not add Windows nodes 79
SUM cannot connect to a node 80
No component version information displayed 80
Command `open_firewall` does not work 81
Firewall error on a remote node error 81
Determining which HPCISSS2 and HPCISSS3 drivers to install 81
SUM skips Broadcom ports 82
SUM reports OA update incorrectly 82
SUM does not deploy to Windows cluster nodes 82
SUM does not process encryption keys included in node input file details 83
SUM does not delete install sets from the Nodes page in IE 11.44 83
Linux firmware RPM mode does not support setting attributes containing string value with parenthesis 83

VMware troubleshooting 85
RPM updates do not deploy to VMware nodes 85
Unsupported Windows ROM components list on Gen10 VMware OS instead of VMware components 85

Reports troubleshooting 86
SUM does not generate reports 86

Deploying firmware RPMs 87
About the SUM RPM tool 87
About SPP ISO and RPMs 87
Accessing firmware RPMs 87
Prerequisites 87
Using YUM and ZYPPER distributions 87
Deploying firmware components 88
Other RPM commands 89
info 89
requires 89
list 89
query 90
erase 91
RPM downloads are blocked 91
`smartupdate upgrade` returns an error 91
RPM mode does not correctly handle Smart Array firmware 92

iLO Repository component install types 93

Websites and support 94
Websites 94
Support and other resources 94
Accessing Hewlett Packard Enterprise Support 94
Accessing updates 95
Customer self repair 95
Remote support 95
Warranty information 96
Regulatory information 96
Documentation feedback 97

Introduction

Smart Update Manager

SUM is an innovative tool for maintaining and updating the firmware, drivers, and system software of HPE ProLiant, HPE BladeSystem, HPE Synergy, and HPE Apollo servers, infrastructure, and associated options.

SUM identifies associated nodes you can update at the same time to avoid interdependency issues.

Key features of SUM include:

- Discovery engine that finds installed versions of hardware, firmware, and software on nodes.
- SUM deploys updates in the correct order and ensures that all dependencies are met before deploying an update.
- Interdependency checking.
- Automatic and step-by-step Localhost Guided Update process.
- Web browser-based user interface.
- Ability to create custom baselines and ISOs.
- Support for iLO Repository (Gen10 iLO 5 nodes only).
- Simultaneous firmware and software deployment for multiple remote nodes.
- Local offline firmware deployments with SPP deliverables.
- Extensive logging in all modes.

NOTE: SUM does not support third-party controllers, including flashing hard drives behind the controllers.

Scaling SUM updates in your environment

SUM supports deploying up to 50 nodes at a time in all SUM modes. Deployment times depend on system and server environment variables.

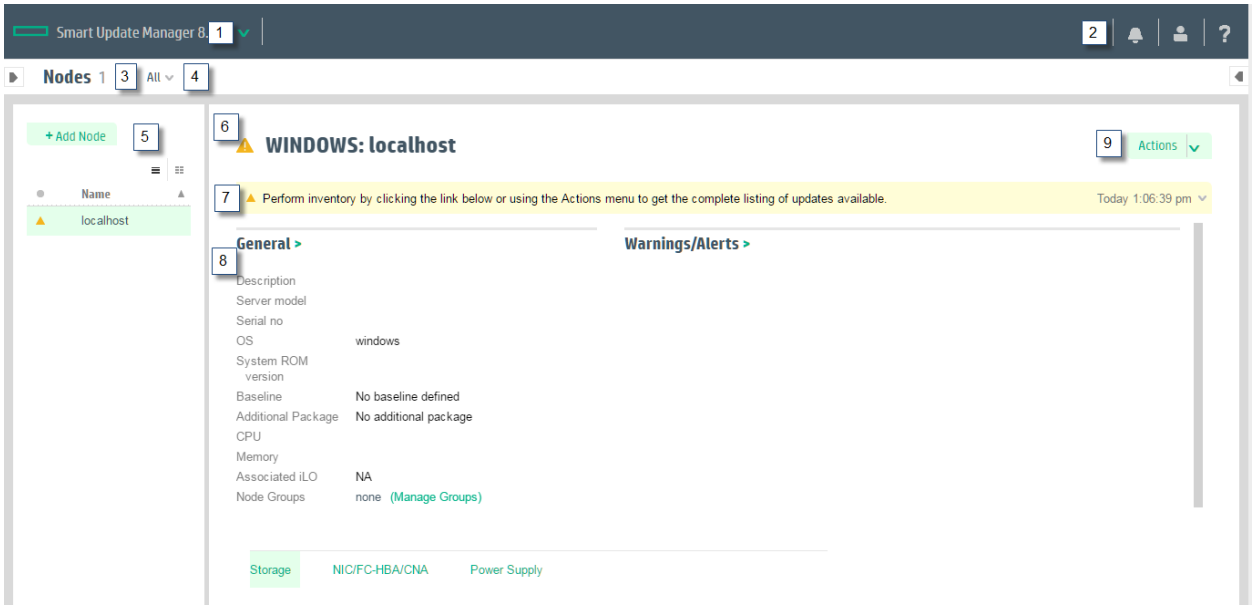
NOTE: Update a maximum of 20 VMware nodes at a time.

About the GUI

SUM is a web browser-based application. When you launch the GUI, the system uses the default web browser.

NOTE: Do not use the **Back** button in your browser window.

The following image explains the major areas of the GUI. Screens options vary based on the node type.



Item	Description
1	Main menu—Provides links to all application screens.
2	• Activity list—Status updates appear briefly, and the activity icon displays the status of recent activities. To open the Activity panel, click the **Activities** icon. • Login information—Displays the currently logged-in user and offers a logout function. • Help—Opens the help panel.
3	Screen name—Displays the name of the screen.
4	Screen filters—Filters screen objects.
5	Screen list—Displays a list of items on the screen. Add Node—Add button changes based on the screen.
6	Baseline or Node name—Lists the baseline or node that you selected in the screen list. This example shows the name of the selected baseline.
7	Informational highlight—Highlights information that you might need to perform or know about for the selected item. Click to expand this box for all information.
8	Item details—Provides full details about the selected item.
9	Actions—Lists the available actions. **NOTE:** Screen options vary based on the screen you are viewing.

Status icon descriptions

SUM uses icons to represent the status of resources and alerts and to control the display.

Table 1: Status icons

Large icon	Small icon	Description
		Critical issue / Interrupted / Dependency issue
		Warning
		OK / Successful
		Disabled
		Unknown
		A change is being applied or a task is running.

Downloading SUM

Files included in the SUM download

Download SUM from the Hewlett Packard Enterprise website or from the Software Delivery Repository as a standalone application. The standalone application does not include updates for your environment. You can obtain update components from the SPP, SPP Custom Download, or from the SDR.

The SUM download includes the following:

`smartupdate`

SUM runs in either GUI, interactive CLI, CLI, input file CLI, or Linux RPM mode. By default, SUM opens in the GUI version. If you enter `smartupdate /s`, SUM runs in the CLI mode. If you enter `smartupdate` and one of the interactive CLI commands, SUM opens in interactive CLI mode.

`clean-cache`

Removes the files in the temp directory associated with SUM that contain cached information about nodes and baselines. Logs are still maintained.

`gatherlogs`

Collects all logs for SUM. The logs are useful when debugging or troubleshooting issues for SUM.

`sum_migration`

Migrates node data from earlier versions of SUM to the current version of SUM.

Downloading SUM from the Hewlett Packard Enterprise website

Procedure

1. Launch a web browser.
2. Go to **https://support.hpe.com/hpesc/public/home/productHome?sp4ts.oid=1008862656**.
3. Click the file that you want to download:
   a. **Smart Update Manager zip**—The zip file contains the files for running SUM on supported Windows and Linux operating systems.
   b. **Smart Update Manager RPM**—The RPM is a native package for Linux and is also available on the Software Delivery Repository at **https://www.hpe.com/support/SDR-SUM**.

Downloading an SPP Custom Download

You can:

- Create a custom SPP.
- Download any of the files available.
- Delete a custom SPP. You cannot delete a default SPP from the page.

For help with the SPP Custom Download page, see the **SPP Custom Download FAQ** page.

Procedure

1. Open a web browser and go to **https://spp.hpe.com/custom**.
2. Access to the SPP requires validation through the HPE Support Center. An active warranty or HPE support agreement is required to download the SPP. For more information, please view the **SPP Warranty/Support Agreement Validation document**; an HPE Passport login is required.
3. If necessary, click **HPE Passport Sign-in**, and then provide your HPE Passport user credentials.
4. Select an SPP from the left side of the page.

Downloading SUM from the SDR website

You can download SUM as an RPM from the Software Delivery Repository at **https://www.hpe.com/support/SDR-SUM**. The SDR contains a version of the SUM RPM for each supported operating system and architecture type. Instructions on how to set up your `yum` configuration are available on the SDR website.

You can use `yum` commands to search for and download SUM to your system. You can also use a web browser to navigate the SDR and download the rpm.

Use the following commands to search, download, or install SUM from the SDR:

`yum search sum`

Search for SUM with yum.

`yum install sum`

Install SUM with yum.

`rpm -Uvh sum-<version>.<os>-<os_version>.x86_64.rpm`

Download SUM from the SDR with a web browser, and then install the RPM.

For more information on using the SDR, see the Getting Started and FAQ sections on the Software Delivery Repository website at **https://www.hpe.com/support/SDR-SUM**.

For more information on using SUM with the SDR, see the Linux best practices document at **https://www.hpe.com/servers/sdr**.

Migrating node information to the current SUM version

SUM stores node information in a database that is specific to each version of SUM. If you have used SUM to manage a node, migrate the node database information to the current version of SUM before launching SUM.

Procedure

1. From the SUM directory, launch `sum_migration.bat` (Windows) or `sum_migration.sh` (Linux).
2. Follow the on-screen instructions, and then select the version you want to migrate to the version of SUM you are using.

SUM and SPP boot environments

The USB Key Utility does not support multiboot setups on a single device. The SUM and SPP ISOs contain signed parts to work with the UEFI bootloader. The signed parts do not allow for multiboot setups on a single device, such as a USB key. You can download the SPP at **https://www.hpe.com/servers/spp/download**.

The following sections discuss deployment from SUM. For more information on planning an update, see the SUM Best Practices Guides available on the Hewlett Packard Enterprise website.

SUM modes

SUM supports local and remote deployments. SUM runs in Windows and Linux in Online and Offline modes.

GUI

An easy-to-use browser-based GUI that enables deployment and maintenance of system software and firmware components to multiple systems in a single session.

CLI

The CLI enables you to script custom installations. This mode might not support all functions of the GUI and interactive CLI. For more information, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide* at **https://www.hpe.com/info/sum-docs**.

Inputfile CLI

You can call a text file that contains all the SUM parameters you want to use. For more information, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide* at **https://www.hpe.com/info/sum-docs**.

Interactive CLI

The interactive CLI allows you to script most of the commands that are available in the SUM GUI. Functionality available from the interactive CLI includes adding nodes and baselines, deploying nodes, collecting log files, and generating reports. For more information, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide* at **https://www.hpe.com/info/sum-docs**.

Linux firmware RPM

The Linux firmware RPM mode offers a simplified command-line deployment mode for Linux nodes.

Running from an ISO

If your ISO contains updates, you can copy the ISO to a DVD or USB key. From the DVD or USB key, you can run SUM in Offline interactive or Automatic mode.

- **Automatic mode**—Firmware components update without interaction. To launch Automatic mode:
  1. Install the DVD or USB key into the server, boot the server to the DVD or USB key.
  2. SUM launches and deploys updates after a short period.
- **Interactive offline mode**—Allows you to use the GUI mode to deploy updates. To launch Offline Interactive mode:
  1. Install the DVD or USB key into the server, boot the server to the DVD or USB key.
  2. After SUM is launched, select Interactive mode and then proceed.

NOTE: If you run SUM on a virtual machine running a supported operating system, do not deploy updates to the localhost system. Only deploy updates to remote nodes.

Deployment modes

The following key terms apply when using SUM to deploy updates. You can combine the terms to reflect an environment, for example, local-online or remote-online.

Local

The installation runs on the physical hardware you are updating. For example, running on a server to update the system ROM of the server.

Remote

SUM runs on one system, but updates other physical nodes. For example, updating the OA/VC or server firmware across a network.

Online

The installation occurs while the host processor is running in the normal server environment. For example, if the server runs Microsoft Windows Server 2012, the update occurs under this environment. The update does not require you to boot to a special environment to update the firmware. You might need to reboot the node to activate the firmware.

Offline

In Offline mode, SUM boots a small SUSE Linux Enterprise Server 12 boot kernel and enables updates to occur on a single server.

- Only updates the local system.
- Only uses a single baseline to update firmware.

In Offline mode, SUM does not support some features that require the regular local host operating systems.

Deployment scenarios

SUM deploys updates from the machine running SUM, the localhost, to one or more remote hosts. If the host running SUM uses Windows, you can update Windows, Linux, or VMware nodes. If the host running SUM uses Linux, you can update Linux or VMware nodes. You can also update remote ProLiant, Synergy, Edgeline, Superdome Flex, and Superdome X Onboard Administrators from Windows or Linux systems.

SUM deployment scenarios

Graphical deployment on a local host

- You are not familiar with command-line tools.
- You are deploying components on a local, single host.
- Updates do not require scripting.

Scripted deployment on a local host

- You are familiar with command-line tools.
- You are deploying components on a local, single host.
- Updates require a customized, scripted deployment.

Graphical deployment to a remote host

- You are not familiar with command-line tools.
- You are deploying components on one or more remote hosts.
- Updates do not require scripting.

Scripted deployment to a remote host

- You are familiar with command-line tools.
- You are deploying components on one or more hosts.
- Updates require a customized, scripted deployment to one, or more host systems.

NOTE: Do not launch SUM from a virtual machine created on the same host machine for upgrading a VMware host. It is strictly not recommended.

Deploying firmware for ProLiant servers using the SPP

The SPP contains smart components for HPE ProLiant servers and enclosure systems.

SUM deploys components to supported Windows, Linux, and VMware operating systems. The single SPP image contains a comprehensive collection of firmware and system software components including drivers, agents, tools, utilities. These components are tested, managed, and deployed together as a single solution.

NOTE: SUM supports deploying RPM components to Linux nodes.

Each SPP release includes a version of SUM you can use to deploy the SPP components. You can download the latest version of SUM from the SUM website at **https://www.hpe.com/servers/sum-download**.

For a complete list of systems and software supported by SPP, and updates available in an SPP release, see the release notes for that SPP at **https://www.hpe.com/info/sum-docs**.

Deploying HPE Synergy with SUM

The SPP and SUM can deploy updates to some HPE Synergy servers. SUM cannot deploy updates to the HPE Synergy Frame Link Module, use HPE OneView.

Log files and changing directory locations

Collecting log files in SUM Online mode

SUM generates a set of debug log files that contains internal process and debug information which can be useful in determining issues with SUM. Log files are stored in the `%LOCALAPPDATA%\sum` (Windows) and `/var/tmp/sum` (Linux) directories. SUM creates log files for each function and node that SUM updates.

Additionally, SUM does audit logging to the Windows Event Log and the syslogs on Linux and VMware. Follow the procedures outlined for each operating system to export the OS log.

SUM includes a utility named `gatherlogs.bat` (Windows) or `gatherlogs.sh` (Linux) to create a compressed .zip (Windows) or tar.gz (Linux) file with all the logs. To review the log files, you can run this utility to gather all the logs in one file.

Procedure

1. Open the `/packages` directory that contains SUM and then launch `gatherlogs.bat` (Windows) or `gatherlogs.sh` (Linux).
2. Use the command `gatherlogs -s` to run the logs without a pause.

Collecting log files in SUM Offline mode

Procedure

1. Boot an SPP or SUM in Offline mode.
2. Launch the log collection utility from the SUM GUI by pressing **CTRL+ALT+D+B+G**.
3. Select a directory where you want to save the logs. You can save the logs to a removable media to view them on another computer.

SUM log file locations

SUM stores log files in the following locations:

User logs

Windows directory: `C:\cpqsystem\sum\log`

Linux directory: `/var/log/sum`

Debug logs

Local Windows directory: `%LOCALAPPDATA%\sum`.

Remote Windows directory: `Admin$\Temp\sum`.

Linux directory: `/var/tmp/sum`

Local copy of SUM binaries when needed

Windows directory: `%LOCALAPPDATA%\localsum`

Linux directory: `/var/tmp/localsum`

SUM makes a local copy of binaries and support files when SUM is launched from a network-mounted share or read-only location. This provides SUM uninterrupted access during updates.

Remote node files

Windows directory: `Admin$\temp\sum`

Linux directory: `/var/tmp/sum`

NOTE: If you do not find logs in the locations listed on Linux systems, check the directory `/var/cpq/Component.log`.

SUM also creates audit logs in the operating system event logs as follows:

- Windows: Windows Event log
- Linux and VMware: sys logs

Audit logs track activities such as SUM logins and component installs.

SUM log locations

- SUM log
  - Windows location: `C:\cpqsystem\sum\log\<ip>\sum_log.txt`
  - Linux location: `/var/log/sum/<ip>/sum_log.txt`
  - Top-level user log for the node at the given IP address.
  - Multiple sessions of SUM are included in the same log file.
  - Includes the summary of steps performed and components installed on the system.
  - Includes return codes for the node.
- SUM detail log
  - Windows location: `C:\cpqsystem\sum\log\<ip>\sum_detail_log.txt`
  - Linux location: `/var/log/sum/<ip>/sum_detail_log.txt`
  - Detailed level user log for node at the IP address.
  - Multiple sessions of SUM are included in the same log file.
  - Includes full output from each component run on the node.
  - Includes return codes for each component and that node.
- SUM install details XML file
  - Windows location: `C:\cpqsystem\sum\log\<ip>\SUM_InstallDetails.xml`
  - Linux location: `/var/log/sum/<ip>/SUM_InstallDetails.xml`
  - XML version of status for user of the last installation.
  - Includes overall status details.
  - Includes details for each component installed.
- SUM execution details XML file

- Windows location: `C:\cpqsystem\sum\log\SUM_ExecutionDetails.xml`
- Linux location: `/var/log/sum/<ip>/SUM_ExecutionDetails.xml`
- Includes details of the baseline and nodes added and operations performed during a session.
- The file is not specific to any node but common for a SUM session
- If SUM is restarted, a new file is created with a date-time stamp, which contains only the information from the new session.

- `cpqsetup` log
  - Windows location: `C:\cpqsystem\log\cqpsetup.log`
  - Linux location: `/var/log/sum/Component.log`
  - Includes details of each component self-discovery and installation deployed.
- Other logs created by individual components
  - Windows location: `C:\cpqsystem\log\*.log`
  - Linux location: `/var/cpq/*.log`
  - `Flash.debug.log`
  - `Verbose.log`
  - `Cpxxxxxx.log`

GatherLogs

SUM provides a tool that collects all log files in to one file. If you are troubleshooting an issue, run `gatherlogs`. The script is available in the same directory that holds SUM.

NOTE: Always shut down SUM before running the GatherLogs utility.

If the GatherLogs utility is executed while SUM is running, it might report an error such as *CNodeData table is not present*. Databases do not flush all the transactions into the file for performance reasons. The transactions are in the cache of the process and the content is flushed onto the file system based on several criteria. However, all the tables are available to SUM for all operations from its cache. When SUM is shut down, the contents of the cache will be flushed to the file system. Therefore, the GatherLogs utility executed while SUM is running will not be able to access all the data/tables. As a result, it might report the error.

When using the `/debuglogdir` (Windows) or `--debuglogdir` (Linux) parameter to launch SUM, also provide the parameter when you launch the `gatherlogs` script so that it can collect the log files from `debug log directory`.

Using the `sum.ini` file

When you launch SUM, it creates the `sum.ini` file in a temporary directory. The `sum.ini` file is a plain-text file that configures multiple settings for the SUM session. You can save or create the `sum.ini` file in the directory where SUM is and it will be used instead of the file in the temporary directory.

Editing the default `sum.ini` file

Procedure

1. Navigate to the temp directory for SUM. The default location for the temp directory is `/var/tmp/sum` (Linux) or `%LOCALAPPDATA%\sum` (Windows).

   NOTE: If there is no directory or `sum.ini` file, launch SUM, and then shut down the application to create the default `sum.ini` file.

2. Open the `sum.ini` file in a text editor.
3. Edit the parameters you want to change.
4. Save the file.
5. You can launch SUM and use these parameters.

More information

sum.ini file parameters

Creating a `sum.ini` file

You can create the `sum.ini` file before you launch SUM and assign the parameters you want to use. Use a text editor to create the file, and save it in your chosen directory.

Procedure

1. Open a text editor and create a document.
2. Populate the document with the parameters you want SUM to use.
3. Optional: Override the SUM RPM (Linux-only) default temp directory by creating `/opt/sum/bin/sum.ini`.

More information

sum.ini file parameters

Changing the temporary directory

Use the following command to launch SUM and change the temporary directory.

Procedure

Type `smartupdate /debuglogdir <log_path> /s`.

`sum.ini` file parameters

Define the following SUM parameters based on your environment.

`[FTP]`

`port=disabled`

`[HTTP]`

`port=63001`: SUM uses this port for nodes that require an HTTP connection. You can also use the parameter `/port` when you launch SUM.

`ssl_port=63002`: Used for internal SUM HTTPS server. You can also use the parameter `/ssl_port` when you launch SUM.

`num_threads=200`: Number of concurrently running HTTP/HTTPS threads SUM allows. The suggested minimum is four threads per remote node.

[Engine]

`temp_dir=<path>`

NOTE: This parameter is one method for changing the temp directory where SUM stores the log files and the nodes and the baseline database.

`mode=<release/debug>`: The debug parameters adds more details to the log files.

Launching SUM

About web browser security certificate

When you launch SUM in GUI mode, you might see a statement that the URL `localhost:63002` is a potential security risk. The error statement differs based on the browser.

You can do the following to continue:

- Select the option to continue despite the risk.
- Import the Hewlett Packard Enterprise security certificate to the web browser.

Importing the security certificate to Firefox

Procedure

1. Open **Settings**, select **Advanced** > **Certificates** > **View Certificates**.
2. Click **Import**, and then navigate to the SUM directory **packages\assets\certificates**. Select the **CA.crt** file.
3. Select **Trust CA to identify websites**.
4. Clear the browser cache, and then close the browser.
5. Launch the browser.

Importing the security certificate to Google Chrome

Procedure

1. Open Chrome settings, and then click **Show advanced settings**.
2. Click **Manage certificates** in the **HTTPS/SSL** section.
3. Click **Import**, and then navigate to the SUM directory **packages\assets\certificates**. Select the **CA.crt** file. Place the certificate in the **Trusted Root Certification Authorities** store.
4. Clear the browser cache, and then close the browser.
5. Launch the browser.

Importing the security certificate to Internet Explorer

Procedure

1. Click **Internet options**, select **Content**, and then select **Certificates** or **View Certificates**, based on the version of Internet Explorer.
2. Click **Import**, and then navigate to the SUM directory **packages\assets\certificates**. Select the **CA.crt** file. Place the certificate in the **Trusted Root Certification Authorities** store.

3. Clear the browser cache, and then close the browser.
4. Launch the browser.

Launching SUM

If you downloaded SUM as a standalone application, the ISO, zip, or RPM does not include software, driver, or firmware components. You can download components from **https://www.hpe.com**. If you downloaded SUM as part of an SPP bundle release, the download includes component updates.

When you launch SUM from a mounted ISO, such as iLO Virtual Media, SUM creates a local copy of the SUM binaries. `%LOCALAPPDATA%\localsum` (Windows) or `/var/tmp/localsum` (Linux) directory. Delete the temporary `localsum` files manually because the `clean-cache` command does not clean these files. SUM displays messages about copying files to the drive specified. If you run SUM on a fileshare directory, SUM does not need to copy the files if you run.

NOTE: When you launch SUM on a Windows node, the CHIF driver is installed automatically. To skip installing the CHIF driver, use the `/skip_prereqs` parameter.

Gen10 servers require the CHIF driver. Gen9 and older servers do not require the CHIF driver, but the CHIF driver allows SUM to determine all component versions.

Windows 2012 and later: Add the system to the domain and use the Domain Admin group user.

IMPORTANT: SUM does not support multiple users logging in to SUM at the same time. All users must have administrator privileges, or the equivalent, for all nodes you are updating.

Each time you launch SUM it determines the state of each node that it manages. SUM determines changes that might have happened between sessions.

Procedure

1. Navigate to the directory where you saved SUM.
2. Do one of the following:

   GUI mode

   Navigate to the directory where you saved SUM.

   To launch SUM on a fileshare directory, enter the command `smartupdate.bat` (Windows) or `smartupdate.sh` (Linux).

   To launch with a specific debug directory, use `smartupdate /debuglogdir <debug_directory_path>`

   Text-based console mode (interactive CLI)

   Navigate to the directory where you saved SUM. From the command line, type `smartupdate` and a console parameter. For a full list of parameters, type `smartupdate -h` (Linux) or `smartupdate /h` (Windows).

   CLI mode and Input file mode

   Navigate to the directory where you saved SUM. Type `smartupdate /inputfile <filename>` for Windows and `smartupdate --inputfile <filename>` for Linux with full list of parameters. If you are using an input file, include the directory path to the input file.

   For full details on using SUM in CLI mode, see the *Smart Update Manager CLI Guide*.

Launching SUM in GUI mode from an ISO

Run SUM on a Windows or Linux operating system.

NOTE: If there is no CHIF driver on a Windows node when you launch SUM, SUM automatically installs the CHIF driver. To skip installing the CHIF driver, use the parameter `/skip_prereqs`.

Procedure

1. Copy the files from the ISO to your local host.
2. Run `launch_sum.bat` (Windows) or `launch_sum.sh` (Linux) from the directory that contains the ISO.

NOTE: If you are using Gnome Virtual file system, manually extract the ISO and save them in a directory. Then launch SUM.

Launching SUM from the RPM

Procedure

From any directory, type `smartupdate`.

Using a PXE server to deploy updates

Use these steps to set up a PXE server on a Linux system.

Procedure

1. Install the following packages:
   a. `tftp-server`
   b. `dhcp`
   c. `httpd`
   d. `syslinux`
2. Set up a DNS server on your network. Although not required, Hewlett Packard Enterprise recommends setting up a DNS server.
3. Activate `TFTP` within `XINETD`.
   a. Change
      `disable=yes`
      to
      `disable=no`
      in
      `/etc/xinet.d/tftp`
   b. Restart
      `XINETD`

4. Set up the PXE server to use a static IP:

   a. Create the file `/etc/sysconfig/network-scripts/ifcfg-eth0.static`

   b. Set the contents to the file as:

   ```
   DEVICE=eth0
   BOOTPROTO=STATIC
   ONBOOT=no
   TYPE=Ethernet
   IPADDR=<IP>
   NETMASK=<IPMASK>
   GATEWAY=<GATEWAYIP>
   ```

5. Set up the PXE boot environment:

   a. Copy `initrd.img` and `vmlinuz` from the `/system` directory of the SPP ISO to `/tftpboot` directory of the PXE system.

   b. Copy `pxelinux.0` (PXE boot Linux kernel) to the `/tftpboot` directory.

   c. Ensure the files copied to `/tftpboot` are world readable.

6. Configure `PXELINUX`

   a. Create directory `/tftpboot/pxelinux.cfg`.

   b. Create files representing the hex value of the static IP address in the `/tftpboot/pxelinux.cfg` directory. For example, if the static IP address used is 192.168.0.254, the hex value is C0A800FE and the files to be created would be:

   - `C`
   - `C0`
   - `C0A`
   - `C0A8`
   - `C0A80`
   - `C0A800`
   - `C0A800F`
   - `C0A800FE`

   c. Create a zero-sized file (using touch) representing the MAC address of the NIC of the boot PXE boot client (pre-pended with 01 and replacing ':' with '-') in the `/tftpboot/pxelinux.cfg` directory. For example, if the NIC MAC address were 00:01:02:03:04:05, a file name would be 01-00-01-02-03-04-05.

7. Create a default `pxelinux` configuration.

   a. Create a file name default in the `/tftpboot/pxelinux.cfg` directory.

   b. Set the contents of the default file to:

```
prompt 1
default Linux
timeout 100
label Linux
kernel vmlinux
append initrd=initrd.img ramdisk_size=9216 noapic acpi=off
```

8. Copy the entire contents of the SPP ISO to a directory named `/tftpboot/SPP*`, where '*' represents the version of the SPP.
9. Add the following to `/ect/httpd/conf/httpd/conf` where "*" represents the version of the SPP.

```
<Directory /tftpboot/SPP*>
Options Indexes
AllowOverride None
</Directory>
Alias /linux /tftpboot/SPP*
```

10. Start the `dhcpd` and apache services and activate `tftp`.

```
service dhcpd start
service xinetd restart
service httpd start
```

11. PXE boot the servers to begin the update process.

HPE Firmware Pack for ProLiant

Updating with the Python script requires access to the Firmware Pack for ProLiant repository. Before using the commands listed below, install the SUM RPM. For more information on setting up a repository, see **https://www.hpe.com/support/SDR-FWPP**.

`smartupdate requires`

Lists PCI devices currently installed on components.

`smartupdate list`

Shows firmware currently installed on the system.

`smartupdate upgrade`

Initiates flash engine for firmware packages.

`smartupdate info`

Provides detailed description of installed firmware.

After establishing a Firmware Pack for ProLiant repository, use the following instructions to download and install the firmware RPMs:

- `yum install $(smartupdate requires)`
- Press **Y** when prompted to install applicable RPMs.
- After the RPMs are installed, type:
- `smartupdate upgrade`
- Press **Y** when prompted to begin flashing the firmware update to the system.

More information

About the SUM RPM tool

Using a different version of SUM with an SPP ISO

To use a different version of SUM than the version that was packaged in an SPP, use the Custom Baseline function in SUM. Replacing the SUM files in an SPP ISO manually might create issues with deployments.

NOTE: SUM can create a custom baseline or ISO with components from SPP 2016.10.0 and older, but it cannot include SUM versions earlier than SUM 8.0.0.

NOTE: Component signature checking is available in SUM 8.3.1 and later.

Procedure

1. Download a copy of the SUM ZIP you want to use and save it in an empty directory, and then unpack the ZIP.
2. Download a copy of the SPP ISO and save it locally, and then mount the ISO.
3. Open the version of SUM you want to use with the SPP components.
4. Add a baseline to the SUM session. For more information, see **Adding a baseline**.
5. Create a custom baseline using the SPP components, and then select the version of SUM you want to use as the version to include in the custom ISO. For more information, see **Creating a custom baseline and ISO**.

More information

Adding a baseline
Creating a custom baseline and ISO

Disabling BitLocker to permit firmware updates (Windows only)

To allow firmware updates, temporarily disable BitLocker support.

Procedure

1. Click **Start**, and then search for `gpedit.msc` in the Search Text box.
2. When the Local Group Policy Editor starts, click **Local Computer Policy**.
3. Click **Computer Configuration** > **Administrative Templates** > **Windows Components** > **BitLocker Drive Encryption**.
4. When the BitLocker settings are displayed, double-click **Control Panel Setup: Enable Advanced startup options**.
5. When the dialog box appears, click **Disable**.
6. Close all windows, and then start the firmware update.

To enable advanced startup options:

- Enter: `cscript manage-bde.wsf -protectors -disable c:`
- When the firmware update process is completed, the BitLocker Drive Encryption support can be re-enabled by following steps 1 through 4 but clicking **Enabled** in step 5 instead. The following command can be used to re-enable BitLocker Drive Encryption after firmware deployment has completed.
- Enter: `cscript manage-bde.wsf -protectors -enable c:`

The following table describes TPM detection scenarios that you might encounter.

Scenario	Result
TPM is detected and enabled, using GUI mode, and a system ROM must be updated.	SUM displays a warning message indicating that it detected TPM. SUM offers an option to **Ignore Warnings**. You can only deploy the updates if you select **Ignore Warnings**.
TPM is detected and enabled, using CLI or Input file mode, the `/tpmbypass` switch is not given, and firmware must be applied to the server. GUI mode does not support `/tpmbypass`.	No warning appears. Because the installation is silent, the installation is terminated and cannot continue. The SUM user log for the node will indicate that TPM was present but no /tpmbypass or /ignore_warnings was passed.
TPM is detected and enabled with Option ROM Measuring, using GUI mode, and a system ROM must be updated.	A warning message appears. You can only deploy the updates if you select **Ignore Warnings**.
TPM is detected and enabled with Option ROM Measuring, using CLI or Input file mode, the `/tpmbypass` switch is not given, and any firmware updated must be applied to the server.	No warning appears. Because the installation is silent, the installation is terminated and cannot continue. The SUM user log for the node will indicate that TPM was present but no /tpmbypass or /ignore_warnings was passed.
TPM is detected and enabled, using CLI or Input file mode, the installation occurs, and the `/tpmbypass` switch or /ignore_warnings switch is supplied.	The installation occurs.

In the SUM GUI, you can ignore TPM on the Deploy screen. You can also ignore TPM in CLI or interactive CLI mode.

About using SUM with BitLocker

The TPM, when used with BitLocker, measures a system state. Upon detection of a changed ROM image, it restricts access to the Windows file system if the user cannot provide the recovery key. SUM detects if a TPM is enabled on a node. For some newer models of ProLiant servers, if a TPM is detected in your system or with any remote server selected as a target, SUM utilities for iLO, HDD, NIC, PowerPIC, and BIOS warn users prior to a flash. If the user does not temporarily disable BitLocker and does not cancel the flash, the BitLocker recovery key is needed to access the user data upon reboot.

A recovery event is triggered in the following situations:

- You do not temporarily disable BitLocker before flashing the system BIOS when using the Microsoft BitLocker Drive Encryption.
- You have optionally selected to measure iLO, Smart Array, and NIC firmware.

If SUM detects a TPM, it displays a message.

To enable firmware updates without the need to enter in the TPM password on each server, temporarily disable BitLocker Drive Encryption. Disabling the BitLocker Drive Encryption keeps the hard drive data encrypted. However, BitLocker uses

a plain text decryption key that is stored on the hard drive to read the information. After the firmware updates have been completed, re-enable BitLocker Drive Encryption. Re-enabling BitLocker Drive Encryption removes the plain text key and BitLocker secures the drive.

CAUTION: Temporarily disabling BitLocker Drive Encryption can compromise drive security and only attempt to disable it in a secure environment. If you are unable to provide a secure environment, Hewlett Packard Enterprise recommends providing the boot password and leaving BitLocker Drive Encryption enabled throughout the firmware update process. This requires setting the `/tpmbypass` parameter for SUM or the firmware update is blocked.

Linux root credentials for remote nodes

You can provide root credentials, a user with sudo permissions, or provide nonroot with root credentials for remote nodes.

To use super user functionality, configure the user as a super user with all root privileges. You can also use nonroot user with a root user to update components.

Prerequisites for using Linux sudo credentials

- Provide one of the following:
  - Username and password
  - Username and SSH key file path (in PEM format)
- Give the sudo users write access to the `/var/tmp` directory.
- For sudo users, add the user to the */etc/sudoers* file. The following shows the privileges and specifications for users.
  - User: `<Sudo_user>` (the actual name of the user account)
  - Privilege: `ALL`
  - Specification: `ALL`
- Edit the entry in the `/etc/sudoers` file so the system asks for the sudo user password instead of root user password when you run the sudo command.
- The following shows the privileges to comment or remove from `/etc/sudoers`.
  - User: `ALL`
  - Privilege: `ALL`
  - Specification: `ALL`

  NOTE: Only use this option with `Defaults targetpw` on all systems.
- When using SSH keys for login credentials combined with sudo, edit the entry in the `/etc/sudoers` file so that the system does not ask for the user password as follows:
  - User: `sudo_user`
  - Privilege: `ALL`
  - Specification: `NOPASSWD:ALL`

Using an SSH keyfile with root credentials

SUM allows you to log in with a password or by providing an SSH key.

Procedure

1. On the node that is running SUM, type `ssh-keygen -t rsa`. SUM also supports DSA encryption key format. To create a DSA encryption key, type `ssh-keygen -t dsa`. A passphrase is optional.
2. Save the key in the directory `.ssh/id_rsa.pub`. Root users, use the directory `/root/.ssh`.
3. Verify that the private key is in PEM format by opening the key and viewing the top of the key for the following text:

   `---- BEGIN RSA PRIVATE KEY ----`
4. If necessary, on the node you want to update, create an `.ssh` directory at the root level. Set the permissions level on the directory to 700.
5. Determine if the node you want to update has the filename `.ssh/authorized_keys`. If this file is not present, create or append this file. Set the permissions on the `authorized_keys` file to 640.

   NOTE: If you append the file, more users are authorized to use the private key.
6. Copy the contents of `.ssh/id_rsa.pub` on the host node, and then paste them into the filename `.ssh/authorized_keys` on the remote node.
7. Open an SSH path between the host node and the node you want to update.
   a. Type `ssh root@10.0.0.1`. This parameter opens a shell path.
   b. Type `ssh root@10.0.0.1 uname`. This parameter executes the command and returns.
8. SUM requires access to `id_rsa` (private key file), and the optional passphrase.

   NOTE: If other applications require the public key in PEM format, you can convert it by typing `ssh-keygen -e -f id_rsa.pub > id_rsa_pub.pem`. Open the key, and look at the PEM format for `---- BEGIN SSH2 PUBLIC KEY ----`.

To create a private key on a Windows system, you can use an application like PuTTY or PuTTY Key Generator (PuTTYGen). For more information, see **https://www.digitalocean.com/community/tutorials/how-to-create-ssh-keys-with-putty-to-connect-to-a-vps**.

To export the file to PEM format, select **Conversion** > **Export OpenSSH key**.

Logging into SUM from the GUI

Procedure

If SUM is already running and you are prompted for login credentials when opening the GUI, use the current user credentials from the system running SUM.

Closing SUM

Logging out of the SUM GUI

Procedure

1. Click the user icon in the top right corner, and then click **Logout**.
2. Select one of the following:
   - **Log Off - Current user.**
   - **Shutdown - This option will shut down SUM engine.**
3. Click **OK**.

If you close the browser window without shutting down SUM, the SUM engine continues to run in the background. Issue an interactive CLI command that shuts down the engine.

- Navigate to the directory that holds the SUM application.
- From a command line, type `smartupdate shutdownengine`.

Clearing the SUM cache

SUM stores node information between sessions, including user credentials for nodes, in a database file. The `clean-cache` removes the database information. The command does not delete the log directories or files.

Procedure

1. Shut down the SUM engine.
2. From a command-line window, navigate to the directory that contains SUM.
3. Type `clean-cache.bat` (Windows) or `clean-cache.sh` (Linux).

NOTE: If you are using a GUI, you can navigate to the directory that holds SUM and run `clean-cache` to clear the cache. Running the clean-cache command erases all nodes, baselines, and other information entered in SUM.

Using the SUM GUI

SUM Home screen

When you launch SUM, the GUI displays the Home screen. From this screen, you can click **Localhost Guided Update**, **Baseline Library**, or **Nodes**. To navigate to other screens, use the navigation menu in the upper-left corner.

SUM Activity screen

The Activity screen provides a list of the activities that SUM is performing or has recently performed. The table displays the source and message related to activities SUM performs. SUM does not refresh this screen when you are viewing the screen. If you want to view the latest activity status, click **Refresh**.

SUM Localhost Guided Update

Use the Localhost Guided Update function to update the localhost that is running SUM. You can use a baseline you have added to the Baseline Library. If you do not specify a baseline, SUM uses the updates in the directory from which SUM is run. If you want to configure components before deploying updates, make the configuration changes from the Baseline Library before running Localhost Guided Update.

Localhost Guided Update modes

- **Interactive**: SUM uses the default baseline or other baseline to update the localhost. You can choose the updates that SUM applies to the localhost.
- **Automatic**: SUM automatically updates the localhost and using the default baseline or other baseline that you select. After you click **OK**, SUM begins updating the node.

Using Localhost Guided Update in Interactive mode

Procedure

1. In the navigation menu, click **Localhost Guided Update**.
2. Click **Interactive**.

   NOTE: If the iLO of the server is configured in one of the High Security modes or if `Require Host Authentication` is enabled, you will be prompted to enter iLO Administrator credentials.

3. SUM displays the current baseline selected for the Localhost.
   a. To use the currently selected baseline, continue to the next step.
   b. To use a different baseline, click the **X** next to the baseline. Select **Assign different baseline** to select another **Baseline** or **Additional package**.
4. Click **OK**. SUM begins inventory on the baseline and Localhost.
5. Click **Next** after SUM finishes the inventory.
6. Recommended updates that are ready to deploy are highlighted in pale green and SUM displays a green icon in the **Ready to proceed** column. If a component has a red icon in the **Ready to proceed** column, it means that there is a

dependency to resolve before SUM can deploy that component. Click the red icon to get details on the dependency. Clear the item if you want to deploy the other updates and come back later to perform this update.

7. If you selected **Deploy all updates**, select a duration of time before SUM reboots.
8. Click **Deploy**.

NOTE: Items that are up-to-date or optional are not highlighted. Click **Force** to deploy these updates. To globally select all components to rewrite or downgrade, select **Actions** > **Advanced Options** and select the **Rewrite** and **Downgrade** options, and the **Reboot** options. To view the component details, double-click an update. If you want to view the information in the new update, click the link.

The global select options are as follows: Upgrade Firmware and Software, Upgrade Firmware, Upgrade Software, Downgrade & Rewrite Firmware, Downgrade & Rewrite Software, Downgrade & Rewrite Both, Downgrade Firmware, Downgrade Software, Downgrade Both, Rewrite Firmware, Rewrite Software, and Rewrite Both.

9. SUM performs component analysis before deploying updates.
10. Review the installation log files.

NOTE: In offline mode, if SUM failed to deploy updates, click the **Reboot** to exit SUM and reboot the node to the host operating system.

You can deploy updates in an iLO task queue, or save install sets and update the existing recovery set on iLO Repository. SUM does not support deleting any install sets on iLO Repository from the Localhost Guided Update function.

More information

Deploying a node

Using Localhost Guided Update

Procedure

1. In the navigation menu, click **Localhost Guided Update**.
2. Click **Automatic**.

NOTE: If the iLO of the server is configured in one of the High security modes or if `Require Host Authentication` is enabled, SUM prompts for iLO administrator credentials. To continue with the update, either provide the credentials or disable the High security mode in iLO.

3. SUM displays the current baseline selected for the Localhost.
   a. To use the currently selected baseline, continue to the next step.
   b. To use a different baseline, click the **X** next to the baseline. To select a different **Baseline** or **Additional package**, select **Assign different baseline**.
4. Click **OK**.

NOTE: SUM begins to deploy updates after you click **OK**. SUM cannot interrupt updates in the Localhost Guided Update Automatic mode. SUM cannot install SNMP and WBEM Providers components in Automatic mode. Use Interactive mode if you want to install these components.

SUM Baseline Library screen

The Baseline Library screen displays the baselines and additional packages you will use to update your nodes. Baselines include an SPP, or custom baseline that includes updates that you select from other baselines or additional packages. Additional packages are directories that hold updates that are not included in a named update package, for example a Hot Fix. SUM saves baseline information between sessions.

SUM displays each added baseline in the left pane. Select a baseline, and SUM displays the following information for each baseline and additional package.

- Languages
- Operating systems
- Enhancements
- Components—SUM includes a search box for finding updates that meet the search parameters. You can search on file name, description, and update type. Double-click an update to view its details.
- Component errors—Components that are specified in the baseline but are missing, and components that are present but fail signature validation.

  The Baseline inventory checks for the component signature and if the signature is invalid or not signed, the component is marked as an invalid component and an error message is displayed.
  The following table displays the signature error messages and compsig file error messages for various components.

Component type	Signature error messages	Compsig file error messages
Gen10 Windows exe	Component not signed Component signature invalid	Component signature file missing. [Warning]
Gen10 RPMs	Component not signed Component signature invalid	Component signature file missing. [Warning]
Gen10 VMware component		1. Component signature file missing. [Error] 2. Failed to verify component signature file.
Gen9 and below Windows exe	Component not signed Component signature invalid	
Gen9 and below RPMs	Component not signed Component signature invalid	
Gen9 and below VMware components		1. Component signature file missing. [Error] 2. Failed to verify component signature file.

- Component Warnings—Components that are present but are missing optional signature files used with iLO Repository.
- Component configuration—Some components support optional configuration parameters that can be set before deployment.

NOTE: If you created a custom ISO, mount the ISO on the system so SUM can detect the files, and then add the directory as a baseline.

More information

Component configuration
Adding a baseline

About SUM baselines

Baselines are directories that contain update components SUM can apply to local and remote nodes. Some baselines include:

- SPP
- Custom SPP downloads
- Maintenance Supplement Bundle
- Custom baselines/ISOs created by SUM

When you add a baseline, SUM searches for the following files:

- `bpxxxx.xml` file: Lists the name, version, history, and components in the baseline. SUM treats any components in the directory that are not listed in the `bpxxxx.xml` file as an Additional Package, not as the main baseline. The SPP, Maintenance Supplement Bundle, and custom baselines include the `bpxxxx.xml` file.
- `..\manifest` directory: This directory contains details about all components contained in the baseline. Included in the manifest directory are:
  - `meta.xml`: Contains most of the component xml file data.
  - `primary.xml`: Contains details about RPMs in the baseline.
  - `system.xml`: Contains mapping information between ROM family and system model.
  - `revision_history.xml`: Contains history information for the component.
- `\db\BaselineDB.pdb`: This is a prepopulated database that SUM uses if there is no other database from other baselines. This file contains all details for the components when the baseline was generated. SPPs and custom baselines include prepopulated databases.

More information

Component configuration
Adding a baseline

Adding a baseline

Procedure

1. On the Baseline Library screen, click **Add Baseline**.

NOTE: If you want to clear the Add Baseline screen, click **Start Over**.

SUM opens the Add Baseline screen.

2. Select **Add Baseline** or **Create Custom**.
3. Select the type of baseline you want to add and include the required information:
   - **Browse SUM Server Path**
     - A directory or fileshare that the system running SUM can access.
     - Enter the directory path to the baseline, or click **Browse** and use the menu to navigate to the directory.
   - **UNC path (for example \\host\dir)**
     - This location uses UNC paths that the system can access. In the **Enter URI for the baseline** field, enter the UNC address for the source baseline. Enter the username and password.

       NOTE:

       – UNC path is only supported in Windows systems.

       – SUM does not support mapped UNC drives.
   - **Download from http share**
     - **Enter directory path**: Enter, or browse to, the directory where you want to save the baseline. If required, create a directory.
     - **Enter HTTP URL**: Enter an HTTP URL where a bundle file is saved. The server can be local or remote, and you can use an Apache, Tomcat, or IIS server. Provide the complete URL, including the bundle XML. The components must reside in the same directory as the bundle XML. Make sure that you have enough local free space for the baseline.

       If you want to download components only for specific operating systems, select the operating systems in the **OS Filter Options**.

       NOTE: SUM adds all baselines it finds in a directory.
4. Click **Add**.

   To see the status of the baseline, check the activity log. If the baseline does not appear in the baseline list, make sure that there are updates in the directory.

NOTE: SUM begins to inventory a baseline as soon as you finish adding the baseline. Wait until the baseline inventory finishes before adding another baseline.

More information

Component configuration
Adding a baseline

Creating a custom baseline and ISO

Creating a custom baseline allows you to:

- Deploy specific updates from SPP releases.
- Minimize the size of baselines or ISOs.
- Standardize the updates that you deploy in your environment.

NOTE: Before creating a custom bootable ISO, make sure that an unpacked ISO is available in a local directory. SUM uses the ISO as a source for the boot environment. For example, a recent SPP ISO. Do not unpack more than one ISO in a directory.

NOTE: SUM does not support creating a custom SPP from another custom SPP.

You can create and download a custom SPP from the SPP Custom Download website at **https://www.hpe.com/servers/spp/custom/**.

Prerequisites

- Add the directories that contain updates as baselines to the Baseline Library screen.
- Make sure that each baseline directory only contains one baseline. For example, do not put an SPP ISO and hot fixes in the same directory.

Procedure

1. Click **+Add**, and then select **Create Custom**.
2. In the **Description** text box, enter a description for the baseline. The maximum length for the description is 50 characters.
3. Select a date for the **Version**, and enter a 1-character or 2-character identifier, for example, **1** or **1a**.

   The **Baseline Name** is automatically generated by combining the description and version.
4. In the **Output Location** field, click **Browse** to navigate to an empty directory where you want to save the baseline. SUM does not allow using a directory that is not empty.
5. To create a bootable ISO with your baseline, select **Make Bootable ISO file**.

   To create a custom bootable ISO, you must have a bootable SPP extracted in a local directory.

   In the **Extracted Source ISO Location** field, click **Browse** and choose the root directory where SUM can find the extracted bootable ISO. For example:

   ```
   C:\SUM\Baselines\spp_july2017
   ```

   NOTE: Do not store more than one bootable ISO in a directory.
6. In the **SUM Source Location**, select one of the following:

   Current Working Directory

   Copies the version of SUM you are currently using.

   Custom Directory

   Copies a version of SUM from another directory.

   Do Not Include

   Does not include a copy of SUM in the baseline.

In **SUM path** field, enter the directory path, or click **Browse** and then choose a directory that contains the version of SUM you want to use.

NOTE: If you select Bootable ISO, **Do Not Include** is replaced with **Extracted Source ISO location**, which displays the location of the ISO with SUM.

7. In the **Baseline Sources** section, select the baselines that contain the components you want to include in the custom baseline.

NOTE: If the same component is included in more than one source baseline, SUM lists the component multiple times. If you select the component from multiple baselines, SUM displays the component multiple times, but the baseline only includes one copy of the component file.

NOTE: SUM versions earlier than SUM 8.3.5 do not support processing of .fwpkg components. If you use a SUM version earlier than SUM 8.3.5 for custom baseline creation, you cannot select .fwpkg components. The minimum SUM version that supports processing of .fwpkg components is 8.3.5.

NOTE: When creating custom baseline with a hot fix bundle (additional baseline), ensure that the path of the hot fix bundle location does not include spaces.

8. In the Filters section:

   a. Select whether you want to create a baseline for Enclosure Firmware Management.

   b. Select whether you want the custom baseline to **Match CloudSystem Matrix Version**. Select this option to use a `MatrixConfig.xml` file saved on your local system. If you select this option, the **Advanced Filters** become inactive and other filters are disabled.

      If you select **Match CloudSystem Matrix Version**, do the following:

      I. Select whether you want to compare the custom baseline to a Matrix Definition XML file on the local system. You can download the latest Matrix Definition from **https://www.hpe.com/info/matrixcompatibility**.

         SUM no longer supports comparing a baseline to a Matrix Definition XML file on hpe.com.

      II. Enter a directory for the Matrix Definition file.

   c. Select the **Component Type** you want to choose, **Firmware**, **Software**, or **Firmware and Software**.

      NOTE: Select one of these options if you want to create a baseline with only firmware or software updates. To update only firmware or software for a node automatically, use the baseline with only firmware or software updates.

   d. Select each kind of update you want to include in the baseline:

      Critical Updates

      Updates that require immediate deployment.

      Recommended Updates

      Updates recommended that you deploy at your earliest convenience.

Optional Updates

Updates to this version if your system is affected by one of the documented fixes, or if you want to use any of the enhanced functionalities provided by this version.

Advanced Filters

To apply to the baseline, select this option:

Filter category	Options
Architecture	Select the system architecture to include in the baseline.
Operating System	Select the operating systems to include in the baseline. The list of options is provided by the source baseline. Custom baseline only supports creating baselines from SPP baseline sources. To create a bootable ISO that supports offline firmware update, select all Linux operating systems to include all firmware that you can deploy.
Enclosures	Select enclosure options for your environment.
Component Category	The type of updates you can deploy.
Server Model	Select the server device components to include in the baseline. The list of options is provided by the source baseline.

NOTE: SUM supports creating a baseline for node types supported by the SPP source baselines.

9. Click **Apply Filters**. SUM displays a list of available updates.
10. Select the individual component updates you want to include in your baseline. Use the search function to find specific updates in the list.
11. To create the baseline, click **Create ISO and save Baseline** or **Save Baseline**. When you click **Create ISO and save Baseline** or **Save Baseline**, SUM does not close the Create Custom Baseline screen, in case you want to create another custom baseline.

    NOTE: Install the application `xorriso` on Linux hosts to create a custom ISO that is (UEFI) bootable.
12. To close the Create Custom Baseline screen, click **Close**.

SUM saves XML files with details of the custom baseline components. SUM reads this XML file and compares the list to the contents of the directory.

More information

Component configuration
Adding a baseline

Generating baseline reports

Procedure

You can generate an Inventory report from the Baseline Library screen. This is the same Inventory report that you can generate on the Nodes screen.

More information

Component configuration
Adding a baseline
Generating node reports

Validating a baseline

SUM can validate a baseline against the following sources:

- **Bundle file**—Allows you to validate against a bundle, for example an SPP. You can use this feature after you pull an SPP from the web or copy a bundle between systems.

  If a component has been unpublished after the SPP or MSB was published, SUM does not pull the component from the web. SUM displays a message that there is a missing component when it validates the bundle. You can look up the component on the Hewlett Packard Enterprise website to see if it is available for download.

- **CloudSystem Matrix file**—Allows you to verify that a custom baseline matches a downloaded version of CloudSystem Matrix. For more information, see **https://www.hpe.com/info/matrixcompatibility**.

  SUM no longer supports validating a baseline against a CloudSystem Matrix file on hpe.com.

  After SUM validates a baseline matches a CloudSystem Matrix configuration file, you can use the baseline to inventory nodes to confirm the nodes match the configuration. Node inventory reports whether the baseline is an exact match to the installed versions, or if the node needs updates to match the CloudSystem Matrix configuration. Inventory also reports if installed components are at a later version than the HPE Helion CloudSystem configuration file.

NOTE: SUM no longer supports validating a baseline against a CloudSystem Matrix file on hpe.com.

Procedure

1. From the Baseline Library screen, select a baseline, and then select **Actions** > **Validate**.

   SUM displays the baseline and baseline bundle file location.

2. Select a validation type, **Validate against bundle file**, or **Validate against CloudSystem Matrix version** on your local system.

   a. In **Matrix Definition XML File**, select **Latest MatrixConfig.xml file from local**.

   b. Enter the path, or browse, to the Matrix XML file.

More information

Component configuration
Adding a baseline

Re-validating baseline components

If a baseline inventory displayed component errors or warnings and you corrected the errors or warnings, you can validate the baseline again.

Procedure

Click **Revalidate All**.

SUM verifies whether the components with errors and warnings have been fixed.

More information

Component configuration
Adding a baseline
SUM does not validate a component

Deleting a baseline

Before deleting a baseline, assign a different baseline to each node that uses the selected baseline. The Baseline screen lists how many nodes use each baseline. Click the hyperlink to display the nodes that use the baseline.

Procedure

1. On the Baseline Library screen, select a baseline.
2. Select **Actions** > **Delete**.

   NOTE: If the baseline is associated with one or more nodes, SUM displays a list of the nodes. Edit the nodes to change the associated baseline, or delete the node.

3. Confirm that you want to delete the baseline.

More information

Component configuration
Adding a baseline
Editing a node
Deleting a node

Baseline addition or inventory cancellation

SUM does not support canceling a baseline addition or inventory. Wait for the procedure to end and then delete the baseline.

More information

Component configuration
Adding a baseline

Component configuration

Some components might have optional configuration settings. Configuration parameters include information necessary to set up the component correctly or passwords required for software installed by the component. From the Baseline Library screen, click on the **Configure** or **Configured** link next to the component in order to change component options, import options, and export options.

You can also configure components if you use an input file. For more information about input files, see *Smart Update Manager CLI Guide*. If you copy the configuration directory into a baseline, when you add that baseline to the SUM session, SUM imports the configuration settings during the inventory process.

You will need to reconfigure component settings if you:

- Run the `clean-cache` utility and did not export the configuration to the baseline directory.
- Copy the component files to a remote server after configuring components settings on a local host and not exporting the configuration to the baseline directory after configuring it in SUM.

More information

Component configuration
Adding a baseline

Configuring components

Procedure

1. On the Baseline Library screen, select the baseline you want to use, select **Components**, and then select **Configuration State** until the components that offer configuration settings are filtered to the top.
2. Select **Configurable** or **Configured** for each a component you want to configure.

   NOTE: Components that display **Configured** have had the default configuration settings changed.
3. Enter the configuration settings, and then click **Save in SUM** to store the component settings in the current SUM database.

   Repeat these steps for each component you want to configure.

   NOTE: Configuration options vary based on the component.

More information

Component configuration
Adding a baseline

Configuring and Exporting Components

Configure components and export the component configurations to a location of your choice. You can then import these configuration settings into another SUM session or use these exported configuration parameters to configure the components as you deploy them outside of SUM or with SUM on remote nodes. This allows you to configure components once and reuse the configurations.

The exported configuration file or script is stored in a directory name `<component filename>_conf`. The directory contains the configuration file or script and a `README` file with the instructions on how to deploy the component with the configuration outside of SUM. SUM stores the configuration file or script separately from the component to not break the component security signing.

Procedure

1. On the Baseline Library screen, select the baseline you want to use, select **Components**, and then select **Configuration State** until the components that offer configuration settings are filtered to the top.
2. Select **Configurable** or **Configured** for each a component you want to configure.

   NOTE: Components that display **Configured** have had the default configuration settings changed.
3. Enter the configuration settings, and then click **Save in SUM** to store the component settings in the current SUM database.

Repeat these steps for each component you want to configure.

NOTE: Configuration options vary based on the component.

4. Click **Save and Export**, and then select a directory where you want to save the component configuration. Select whether you want to include user credentials in the configuration file. SUM creates a directory named after the component you exported. The name is `<component_name>_conf`. The Activity screen displays the address where it saved the configuration file.
5. SUM includes a `README` file that provides instructions on how to deploy the component in standalone mode.

   IMPORTANT: SUM stores configuration settings, possibly including user credentials, in a plain-text file format that the component can use.

6. Click **Save**. The configuration data is saved in the SUM database and written to the appropriate file.
7. Repeat these steps for each component you want to configure.

More information

Component configuration
Adding a baseline

Importing component configuration settings

If you have configured components in another SUM session, or in a baseline copied from another server, you can import these settings into the GUI.

NOTE: If you saved the baseline configuration directory in the same directory as the baseline, SUM automatically imports the configuration settings when you add the baseline to the baseline library.

Procedure

1. On the Baseline Library screen, select the baseline you want to use, select **Components**, and then click **Configuration** until the components that offer configuration settings are filtered to the top.
2. Scroll down the list of components, and then select **Configurable** for each component configuration file.
3. Click **Import**.
4. Select the directory where you saved the configuration file, and then click **Open**.

   IMPORTANT: SUM overwrites any existing component configuration as it automatically saves the imported configuration data.

5. Repeat these steps for each component you want to configure.

More information

Component configuration
Adding a baseline

SUM Nodes screen

Nodes are servers or devices that SUM can independently update. The Nodes screen displays the nodes and associated nodes that you have added to SUM and SUM can manage. The node details that SUM displays varies based on the node type.

The yellow status bar under the node name gives a brief description of the status or action you can perform next on the node. For full details, click the **Actions** arrow. For example, after you add a node, the status bar might give a link to Inventory the node. Or, after you inventory a node, the status bar will provide a link to review and deploy updates.

About node status

SUM assigns the following statuses to nodes after you add the node and deploy updates:

- **Scouting**: SUM verifies the node address and user credentials. If required, scouting also installs a CHIF driver. For Gen10 iLO 5 nodes, scouting retrieves the iLO Repository details.
- **Preinventory** (remote Windows and Linux nodes only): SUM runs commands on the remote node to determine operating system details, installed hardware, and installed RPMs (Linux nodes).
- **Inventory**: SUM gathers information from the node and determines which updates apply, and if there are any dependency issues. For remote Windows and Linux nodes, SUM copies a version of itself along with required the baseline components required to determine applicability.
    - **Deploy/install updates**: SUM deploys updates to the node. For remote Windows and Linux nodes, all components required for deployment are copied to the remote node and SUM runs on the remote node. For iLO 5 nodes, SUM uploads components to the iLO Repository, and saves components for install sets. iLO 5 saves the components as install set on the iLO Repository. However, it can be disabled by clearing the option **Save Components as an Install Set on iLO Repository**.

      NOTE: For Gen10 Windows/Linux, if you select the option to save components as install set to iLO NAND, SUM uploads components along with their configuration and creates an install set in iLO NAND. This install set will be initiated and the resultant task queue will be processed.
- **Complete installation**: SUM finishes updates and, if necessary, reboots the node.

Viewing LiveLog information

The **LiveLog** allows you to view the status of an active deployment. If SUM is deploying multiple components, search the list to view the status of specific components. After SUM finishes the deployment, SUM displays a **View Log** button.

Procedure

On the Nodes screen, select a node, and then click **Live Log**.

Adding a node

You can add a node using a specific IP address or by searching an IP address range.

Prerequisites

1. Know the IP address or DNS name of the node.
2. User login credentials for the node.
3. If you are planning to assign a baseline to a node when adding it, add the baseline first.
4. When you add a node, SUM installs the prerequisite inventory components by default. If you do not want the components to be installed, clear the **Install Prerequisite components if not already installed** check box.
5. If the iLO of the server is configured in one of the high security modes or if `Require Host Authentication` is enabled, iLO Administrator credentials are required.

NOTE: Use this option only for **Windows**, **Linux**, and **Unknown** node types.

Procedure

1. **Adding a single node by IP or DNS name**
2. **Adding a node by searching a range of addresses**
3. **Adding nodes by input file**

Adding a single node by IP or DNS name

Procedure

1. From the Nodes screen, click **+Add Node**.
2. Select **Add a single node or known range of nodes** from the **Selection operation** drop-down list.
3. Enter the IP address, DNS name, range of IP addresses, or multiple addresses separated by commas. For example, entering 10.0.1.1–10.0.1.20 adds 20 nodes. 10.0.1.1, 10.0.1.2, 10.0.1.7 adds three nodes. If the nodes use the same credentials, SUM adds the nodes.

   NOTE:

   - The supported DNS character set is ASCII only—A-Z, a-z, underscore, dot, and 0-9 with hyphen.

     You can add a maximum of 50 nodes.
   - If you are adding a VC node, use the IP address of the primary Enet module. All VC modules installed, including FC modules, are updated through the primary Enet module.

4. Enter a description for the node.
5. In the **Node type** field, select the node type. If you do not know the node type, select **Unknown**. During the inventory process, SUM determines the node type.

   Some nodes allow SUM to discover and add associated nodes automatically.

   NOTE: Selecting the correct node type might help SUM complete adding the node faster.

6. Optional: To skip the installation of the prerequisite inventory components, clear the **Install Prerequisite components if not already installed** check box.

   IMPORTANT: Performing this action may result in scenarios where SUM may not perform a complete inventory. Two sessions may be required to complete the update in such a case.

7. Optional: Select the baseline, additional package, or both to apply to this node.
8. Optional: Select a group from the list.
9. Select one of the following:

- **Use current credentials (requires existing trust relationship with the node)**: This option is for Windows nodes only.
- **Enter administrator credentials**: Enter the username and password for a user with administrator privileges on the node. If Windows users have administrator privileges, use `domain\username`.

10. Linux nodes allow you to use sudo credentials to deploy updates without logging in to the node with root credentials. To use sudo commands, you have to install sudo capabilities on the node.

    NOTE: Super user and sudo are not available for all nodes.

    If you want to use an account that lacks direct root privileges, in the **Access Level** field, select one of the following:

    - Click **Use sudo with credentials entered above** if you want to use sudo credentials.
    - Click **Enter super user credentials to update components** if you want to enter super user credentials.

    NOTE: If you are using super user credentials, enter normal user credentials in the **Credentials** field, and then add super user credentials in the **Access Level** field. SUM first logs in using the normal user credentials, and then uses the super user credentials to log in to the super user account.

11. If the iLO of the server is configured in one of the High Security modes or if `Require Host Authentication` is enabled, enter the iLO Administrator credentials in the provided iLO Credentials section.
12. Click **Add**.

    In the **Added Nodes** section, SUM displays the nodes you selected.

More information

Node-specific additional details

Adding a node by searching a range of addresses

Procedure

1. From the Nodes screen, click **+Add Node**.
2. Select **Find nodes on network** from the **Selection operation** drop down.
3. Click **Find Nodes**.
4. Select **IP Address Range** or **Port Address**.

   NOTE: SUM can search a port in the range of 0–65535.

5. Enter a range of IP addresses for SUM to search, select one of the default ports or select **Other** and enter the port, and then click **Search**.

   NOTE: SUM only searches one subnet/octet, the final four digits of an IPv4 address.

   SUM displays the nodes it finds in the **Available Nodes** field.
6. Select the nodes you want to add from the **Available Nodes** section, and then click **Add Nodes**.
7. If you want to assign a baseline, select **Baseline**, **Additional Packages** in the **Baseline to Apply** field.

8. In the **Credentials** section, select whether to **Use current user credentials (requires existing trust relationship with the node)**, **Enter administrator credentials**, or **Enter SSH Key Credentials** (not available for all nodes).
9. If the iLO of the server is configured in one of the High Security modes or if `Require Host Authentication` is enabled, enter the iLO Administrator credentials in the provided iLO Credentials section.
10. If you choose to enter administrator credentials, enter the **Username** and **Password**.
11. Click **Add**.
12. In the **Added Nodes** section, SUM displays the nodes you selected.
13. Click **Cancel** to go back to the Nodes screen.

Adding nodes with an input file

You can use a CLI with Input File script to add many nodes that you can deploy in the GUI.

Procedure

1. Create an input file with the node details. For example:

```
#Input file sample
SILENT = YES
SOURCEPATH = C:\SPP
DRYRUN = TRUE

[TARGETS_USER_1]
HOST = 192.168.1.1
HOST = 192.168.1.3
HOST = 192.168.1.2
UID = user1
PWD = user_password1
ILO_USERNAME=ilo username
ILO_PASSWORD=ilo password
[END]

[TARGETS_USER_2]
HOST = 192.168.1.4
HOST = 192.168.1.5
HOST = 192.168.1.6
UID = user2
PWD = user_password2
[END]
```

2. Open a terminal window, navigate to the directory where SUM is located, and then issue the command:

   `smartupdate /inputfile <path:\inputfile.txt>` (Windows)

   `./smartupdate --inputfile <path:/inputfile.txt>` (Linux)

3. Launch the GUI and manage the nodes. If the nodes were not added, verify that there are no issues with the Input File.

For more information, see **https://www.hpe.com/support/SUM-CLI-en**.

Associated nodes deployment behavior

The following describes which nodes SUM can automatically add and the order in which SUM deploys the nodes:

Onboard Administrator

Types of associated nodes:

- iLO
- Virtual Connect
- SAS Switches

Deployment behavior:

Deploys the OA first and then other nodes.

Virtual Connect

Types of associated nodes:

Onboard Administrator

Deployment behavior:

Deploys the VC first and then the OA.

FC Switch

Types of associated nodes:

Partner FC Switches

Deployment behavior:

Deploys to the selected switch first and then to associated switches.

6 Gb SAS BL Switches

Types of associated nodes:

Onboard Administrator

Deployment behavior:

Deploys to the selected switch first and then to the OA.

iLO

Types of associated nodes:

- Onboard Administrator
- Server

Deployment behavior:

Deploys to the iLO first and then the OA and servers.

NOTE: SUM adds associated server only for iLO 4 nodes, not for iLO 5.

Server

Types of associated nodes:

None

Superdome X

Types of associated nodes:

None

Superdome Flex

Types of associated nodes:

None

NOTE: If you are running a mixed IPv4 and IPv6 environment, SUM might display the following issues:

- If you add an IPv6 iLO with associated nodes and the associated nodes are only configured with IPv4, SUM displays IPv6 nodes.
- SUM does not support IPv6 for SAS and FC switches.

Node-specific additional details

Some nodes have node-specific information required when you add a node.

Windows

Additional details:

Enter what you want to do if SUM detects an update process on the node:

- **Leave the update running and bypass the node**
- **Stop any currently running update process on the node and replace it with updates from this session**

Linux

Additional details:

- You can use SSH key credentials for Linux nodes. Enter the **Username**, **Private Keyfile** location, and **Password** (if required). The private key file must use the PEM format.
- Enter what you want to do if SUM detects an update process on the node:
  - **Leave the update running and bypass the node**
  - **Stop any currently running update process on the node and replace it with updates from this session**
- Select the access level for this node:

- None
- Use sudo with credentials entered previously
- Enter super user credentials

VMware Host

Additional details:

Select whether to use administrator credentials or open an authentication ticket with the VMware host of the vCenter. A ticket allows you to update the node regardless of the lockdown mode status.

If you select **Enter vCenter details to get ticket (for authentication to host)**, enter the **IP/DNS**, **Username**, and **Password** for the host.

NOTE: SUM does not automatically migrate VMware nodes if DRS or HA is enabled. For more information on migrating VMware nodes, see the documentation for HPE OneView for VMware vCenter at **https://www.hpe.com/info/ovvcenter/docs**.

NOTE: For Gen10 servers running VMware ESXi, iSUT must be installed before adding the node in SUM. Such servers cannot be added in SUM with the host IP address. Instead, the iLO IP address must be used and added as an iLO node type.

Onboard Administrator

Additional details:

- Select whether you want to automatically add associated nodes. This adds all nodes in the chassis.
  - If you are updating OAs and iLOs at the same time, select this for OA nodes so SUM detects associated iLO nodes. SUM can determine the proper deployment order when you deploy updates to the OA.
  - If you do not provide credentials, SUM uses the credentials you provide for the OA for associated VCs.

NOTE: If the OA is in FIPS mode, SUM does not support downgrading or rewriting firmware. SUM displays a message and turns off the downgrade and rewrite options.

Superdome X Onboard Administrator

Additional details:

No node-specific settings.

Superdome Flex RMC

Additional details:

No additional details.

SAS B/L Interconnect Switch

Additional details:

Select whether you want to automatically add associated nodes.

Fibre Channel Switch

Additional details:

Select whether you want to automatically add associated nodes.

iLO

Additional details:

Select whether you want to automatically add associated nodes.

Virtual Connect

Additional details:

Some VC options, such as VC Activation order, can be set from the Edit Node or Review/Deploy Node screen.

NOTE: SUM cannot deploy updates to a Virtual Connect node managed by HPE OneView.

Select whether you want to automatically add associated nodes.

- Add the Associated Onboard Administrator credentials.
  - **Use credentials above**: Uses the same credentials you entered previously.
  - **Enter administrator credentials**: Enter the credentials if they differ from the credentials you entered earlier.

More information

Associated nodes deployment behavior

Editing a node

Nodes are changed using the **Edit** option on the Nodes screen. Make sure SUM has completed all functions, for example, node inventory or deployment, before you edit a node. Options you can edit vary based on the node. For information on specific node options, see **Node-specific additional details**.

NOTE: SUM uses the same function to edit all node types.

Procedure

1. From the Nodes screen, highlight the node, and then select **Actions** > **Edit**.
2. The following are some of the fields you can edit:
   a. **Description**
   b. **Type**
   c. Selected **Baseline** and **Additional Package**.

      NOTE: If a node is part of a group, the group baseline and additional package settings override the node. Remove the node from the group to change the baseline or additional package.

   d. **Credentials**

      NOTE: If the iLO of the server is configured in one of the High Security modes or if `Require Host Authentication` is enabled, enter the iLO Administrator credentials in the provided section.

3. Click **OK** to accept the changes and return to the Nodes screen.

Performing node inventory

The node inventory collects information about the node, and the firmware, software, and driver versions installed on the node. SUM detects when a component has a missing dependency.

SUM must perform a node inventory during each new session to determine the firmware and software on a node.

SUM cannot inventory a node if the credentials are not valid. If the credentials are not valid for the node, edit the node credentials.

NOTE: If you perform inventory on an OA node, SUM can automatically add and inventory the associated nodes. To add associated nodes, select the check box on the Add Nodes screen. Add VC credentials separately. If you perform inventory on a blade iLO or VC, SUM does not find an associated OA until the end of the inventory process. Add credentials to the OA and then perform inventory on the OA node.

Procedure

1. From the Nodes screen, highlight the node, and then select **Actions** > **Inventory**.
2. SUM displays the baseline associated with the node. If you want to reassign the baseline that SUM will use for inventory, select a baseline, additional package, or both.

   For Gen10 servers, you can select a saved install set as a baseline in the **Inventory** page.
3. Click **Inventory**. SUM displays errors to resolve before you can deploy updates.

More information

Associated nodes deployment behavior

Deploying a node

The Deploy screen allows you to change the settings for the node you are deploying. You can change the following:

- Installation options.
- Reboot options.
- iLO Repository options (Gen10 iLO 5, Windows, and Linux nodes only).
- Components to deploy and configure components from the Baseline Library screen.

IMPORTANT:

- If you run SUM on a virtual machine running a supported operating system, do not deploy updates to the localhost system. Deploy updates to the host OS on remote nodes, or to the iLO on those nodes.
- When SUM activates the Deploy button, do not manually update or downgrade a component that SUM manages. Updating the component manually will cause SUM to skip the component and report an error.
- SUM 8.5.0 blocks the flashing of firmware version 4.80 on the HPE VC Flex-20 Enet Module.
- SUM flashes iLO 5 firmware v1.40 prior to updating to v2.10 because it is a prerequisite for flashing firmware v2.10.

Procedure

1. From the Nodes screen, select a node to update, and then select **Actions** > **Review/Deploy**.
2. Select the **Installation Options** tab to change:

NOTE: If the baseline has multiple versions of the same product, only one can be selected from the different versions of the same components. If you select other component of the same version, the already selected component gets cleared automatically. The component that has the higher version gets selected by default if:

- The Downgrade and Rewrite option is set.
- The higher version of the component is not installed.

- Installation options

  Upgrade Firmware and Software

  Upgrades firmware and software components.

  Upgrade Firmware

  Upgrades only firmware components.

  Upgrade Software

  Upgrades only software components.

  Downgrade and Rewrite both

  Upgrades, downgrades, and rewrites firmware and software components.

  Downgrade and Rewrite Firmware

  Upgrades, downgrades, and rewrites only firmware components.

  Downgrade and Rewrite Software

  Upgrades, downgrades, and rewrites only software components.

  Downgrade both

  Upgrades and downgrades firmware and software components.

  Downgrade Firmware

  Upgrades and downgrades only firmware components.

  Downgrade Software

  Upgrades and downgrades only software components.

  Rewrite both

  Upgrades and rewrites firmware and software components.

  Rewrite Firmware

  Upgrades and rewrites only firmware components.

  Rewrite Software

  Upgrades and rewrites only software components.

- **Verbose logging or normal logging**
- **Skip Components with Dependency Failures**
- **Select whether to clean up temporary files after deployment**
- **Select whether to clean up debug logs and temporary files after deployment**

NOTE: If an OA is in FIPS mode, SUM does not support downgrading or rewriting firmware. SUM displays a message and turns off the downgrade and rewrite options.

3. On the **Reboot Options** tab, select the following:

   a. Select a system reboot option: `Never`, `If needed`, `Always`.

   b. Enter the number of minutes SUM delays before rebooting the node. Select 1–60 minutes.

   c. Enter a reboot message, up to 255 characters, to display.

   NOTE: The `reboot_message` cli parameter is not functional for SLES12 OS because the SLES12 OS image has a constraint that does not permit executing the parameter as a cli command.

4. Gen10 iLO 5 Windows and Linux and iLO 5 nodes only: To manage the iLO Repository, select the **iLO Repository Options** tab.

   a. To upload selected components to the iLO Repository and create an install set, select **Save Components as an Install set on iLO Repository**. SUM automatically creates a default name and description, but you can edit the name and description for the install set. You can use this install set to roll back the server components at a future time. The name and description are limited to 63 characters, and the only special characters allowed are – and _.

      NOTE: You can update firmware and software by using SUM either through the server operating system or through iLO. For more information on the advantages of these methods, see **Absaroka vs online update through OS**.

   b. To update the previous recovery set, select the **Update the existing recovery set with components (BIOS, iLO, CPLD) from this run** check box. SUM updates the existing recovery set in iLO Repository with new firmware versions of iLO, BIOS, and CPLD from current deployment.

   c. To set the start and end time of the deployment, click **Set Schedule**. Alternatively, select **Maintenance Windows**.

   d. Select one of the following:

   - **SUM manages iLO Repository space**: SUM automatically creates space on the iLO Repository if necessary. SUM deletes:
     - Unreferenced components first.
     - Deletes the oldest install set. iLO Repository can save a maximum eight install sets.
   - **Manually manage iLO Repository space**: You select the install sets or unreferenced components to delete to free up iLO Repository space.

5. Select the components from the **Baseline** and **Additional Packages** tabs that you want to deploy.

   If you are deploying updates to an iLO 5 node, SUM automatically selects components based on the operating system that is running on the node. If the node is off, SUM picks up all firmware components. If Agentless Management System (AMS) is not present on the system, iLO does not get OS details. In such a case, SUM picks only firmware components.

   If you are performing an Absaroka update, make sure that iSUT is installed on the system.

   NOTE: Gen10 iLO 5 nodes require all components include a component signature file. If the signature file is missing, SUM disables the Deploy button. Deselect components without signature files to deploy other updates.

6. Click **Deploy**. SUM Verifies any changes that you made are valid and then begins deploying components.

NOTE: To begin the deployment, all dependency issues must be resolved, or clear the component so it does not install.

7. In the General section of the Node screen, click **View log** for the node, and then click **View log** for the component you installed to view the details of the installation.

NOTE: On the node page, click the **Live Log** button to view the deployment status while SUM is deploying updates.

Absaroka vs online update through OS

For online firmware and software updates on Gen10 servers, you can use SUM through the server operating system or through the iLO and the iLO Repository. For iLO Repository-based updates, most of the discovery and update processes are handled using the Redfish Absaroka support from iLO 5.

The following are the advantages of using the two methods:

- **Absaroka**
  - Does not add to production network traffic.
  - Can stage in advance, install during maintenance window.
  - Includes install set creation for future rollback.
- **Online update through OS**

  Unlike Absaroka, online updates through the operating system do not need iSUT installed to ensure all drivers and some firmware components are installed.

NOTE: You can also perform an offline upgrade using either the USB key utility or iLO virtual media. This upgrade method does not require the server operating system and is useful for provisioning.

Auto-retry component update failures

SUM performs an auto retry of the component installation in the following scenarios:

- SUM performs installation of pre-requisite components during scouting and inventory for OS nodes. If the component installation fails with `GENERAL_FAILURE (-1)` and `COMPONENT_EXECUTION_FAILED (-3)`, SUM performs the installation of the pre-requisite components once during scouting and inventory.
- SUM runs self-discovery components in discovery mode during inventory for OS nodes. If the component fails to generate the discovery xml, SUM retries the self-discovery once for the failed self-discover components during inventory.
- For OS based updates, If the component installation fails with `GENERAL_FAILURE (-1)` and `COMPONENT_EXECUTION_FAILED (-3)`, SUM retries the installation of the failed components once during deployment.
- For iLO Repository-based updates on OS nodes If the component installation fails with `GENERAL_FAILURE (-1)` and `COMPONENT_EXECUTION_FAILED (-3)`, SUM retries the installation of failed Type D components once during deployment.

Server updates through iLO 5

Gen10 servers with iLO 5 allow you to update the servers two ways:

- Deploy updates through the operating system with SUM.
- Deploy updates through the iLO 5. SUM loads the updates to the iLO 5. Integrated Smart Update Tools (iSUT) deploys the updates based on the iSUT mode. This requires:
  - iSUT 2.0.0.0 or later
  - AMS management tools

  NOTE: For Windows Server 2019, you must install AMS version 1.30.0.0(B) or later.

For more information about iSUT, see **www.hpe.com/info/isut-docs**.

iLO Repository

The iLO Repository is a secure storage area in the nonvolatile flash memory embedded on the system board. The nonvolatile flash memory is 4 gigabytes in size and is called the iLO NAND. Use SUM or iLO to manage signed software and firmware components in the iLO Repository.

iLO, the UEFI BIOS, SUM, and other client software can retrieve these components and apply them to supported servers. Use SUM to organize the stored components into install sets and SUM or iLO to manage the installation queue.

Install sets

An install set is a group of components that can be applied to supported servers with a single command. SUM determines what to install on a server and creates an install set that is copied to iLO. You can view existing install sets on the **Install Sets** page in the iLO web interface.

Saving an install set when you deploy from SUM keeps all the components on the iLO system for later use. For example, you could use the saved components to restore or roll back a component version without needing to find the original SPP.

System Recovery Set

By default, a System Recovery Set is included with every server. User accounts with the **Recovery Set** privilege can configure this install set. Only one System Recovery Set can exist at a time.

The following firmware components are included in the default System Recovery Set for Intel servers:

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

If the default System Recovery Set is deleted:

- A user with the **Recovery Set** privilege can use the iLO RESTful API and the RESTful Interface Tool to create a System Recovery Set from components stored in the iLO Repository.
- A user with the **Recovery Set** privilege can use SUM to create an install set, and then designate it as the System Recovery Set by using the iLO RESTful API.

Creating a system recovery set

Use update tools to save an install set to the iLO Repository, for example SUM.

Prerequisites

- Recovery set permissions on the iLO.
- Install set saved in the iLO Repository.
- iLO RESTful API.

Procedure

1. Open iLO RESTful API.
2. If there is an install set defined as a recovery set, use the `PATCH` command to define the `IsRecovery` parameter to `false`.

```
PATCH /redfish/v1/UpdateService/InstallSets/[install_set_ID]/

{
  "IsRecovery": false
}
```

3. Use the `PROMOTE` command to change the `IsRecovery` parameter to `true` on a saved install set.

```
PROMOTE /redfish/v1/UpdateService/InstallSets/[install_set_ID]/

{
  "IsRecovery": true
}
```

More information

Deploying a node

iLO 5 Gen10 security states

When you add a Gen10 node to SUM, communication between the iLO and host operating system occurs over the CHIF interface. Depending on the iLO security state, the communication operates in the following modes:

Production state

iLO credentials are not required for localhost access.

Secure mode

In secure mode, such as High security, CNSA SuiteB, and FIPS, communication between the iLO and host operating system is encrypted, authorized, and authenticated.

Provide iLO administrator credentials for SUM while adding Windows/Linux nodes (Gen10) if its iLO is in High security, CNSA or FIPS mode. SUM uses these credentials to perform scouting, inventory or deployment of updates to these nodes.

NOTE: iLO credentials are required in addition to host OS credentials when the iLO for a server is configured in one of the high security modes or if `Require Host Authentication` is enabled.

For more information about Gen10 server security settings, see *HPE Gen10 recommended security settings* in the *HPE Gen10 Servers and Embedded Server Management Security Reference Guide* at **https://www.hpe.com/info/sum-docs**.

Deploying to and managing iLO Repository with SUM

On the Deploy screen, when you deploy updates to an iLO 5 node, SUM creates the installation queue for the iLO 5 to deploy. You can select whether you want to save the components in the iLO Repository.

- **Inventory** screen: Use this screen to inventory the baseline contents or a saved install set and additional baseline.
- **Review/Deploy** screen: Use this screen to deploy the selected baseline or install set. This screen performs like the Review/Deploy screen for other nodes.

The iLO Repository allows you to deploy firmware with the following methods:

- iLO and SUM: SUM works with the iLO to deploy the updates to the targets, for example, the operating system and iLO node.
- iLO and iSUT: The iLO and iSUT work together to deploy updates to the target nodes, for example, the operating system and the iLO node.

Generating node reports

You can generate reports with detailed information about your SUM session, including details on a node, components you can install, and failed dependencies.

The reports for a node enable you to generate HTML, XML, and CSV reports. On the Reports screen, SUM includes a **Reports Center** that displays previous reports you have generated.

NOTE: SUM uses the same function to generate reports for all node types.

Procedure

1. From the Nodes screen, select a node, and then select **Actions** > **Reports**.
2. Select the reports you want to generate:

   Firmware details

   Displays firmware versions that are currently installed on the node.

   Deploy preview

   Displays components that SUM can install on the node.

   Failed dependency details

   Displays any failed dependencies on the node.

   Deploy details

   Displays details about what SUM installed on a node.

   Inventory

   Displays details about what components are in the baselines.

   Combined report

   Generates one of each report type.

   NOTE: If you cannot select a report, SUM might not have enough information to generate the report.

3. Click the report format you want SUM to generate: **HTML**, **CSV**, or **XML**.

   NOTE: You can view HTML and XML reports in java-script enabled browsers.

4. In the **Advanced Report Options**, you can:

   a. Select a directory to save the reports. SUM creates a directory if it does not exist.

NOTE: The default location for Windows clients is `C:\cpqsystem\sum\log`.

b. Select whether to run the report in the background.

5. Click **Generate**.

Deleting a node

Procedure

1. From the Nodes screen, highlight the node, and then select **Actions** > **Delete**.

NOTE: You cannot delete a node if the inventory or deployment of the node is active.

2. Click **Yes, Delete** to confirm that you want to delete the node.

Server overview

When you select a node, the Overview screen displays a progress bar for inventory and deployment of the node, and information about the node. For example, SUM does not deploy updates to HPE Synergy Frame Link Modules.

The information SUM displays varies based on the node type. Some information includes:

- Node type
- Node address
- NIC information
- FC HBA information
- Baseline and Additional Package
- Warnings/alerts
- Install sets available on the iLO Repository (Gen10 iLO5 nodes only)
- iLO Repository details (Gen10 iLO5 nodes only)

During the inventory and deploy process, SUM displays a progress bar for current tasks.

Node Groups screen

Node groups allow you to combine nodes and perform tasks as a group instead of individually. You can assign baselines, perform inventory, and review and deploy updates to all nodes in the groups that share these settings. The settings you assign on a group screen, for example a baseline, overrides what you applied to the node when you added the node to SUM.

Adding a node group

Procedure

1. On the Groups screen, click **+Create New Group**.

2. Enter a **Node Group Name**.

3. Enter a **Node Group Description**.
4. In the **Assign existing Node(s) to Node Group** section, select the nodes that you want to add to the group.
5. In the **Baseline** section, select a **Baseline** and **Additional Packages** (optional) for the group if you want all the nodes to use the same baseline.

   NOTE: The baseline or additional package you select overrides the baseline or additional package you selected on the Nodes screen.

6. Click **Add**.

   NOTE: On the Add node page, you can either select a baseline or an existing ready to inventory node group. After you select a node group. the baseline applied on the node group is applicable to this node.

   To remove a node from a node group, click the **X** on the right side of the row for the node.

Editing a node group

Procedure

1. Select a node group from the list.
2. Select **Actions** > **Edit**.
3. Enter a new **Node Group Name** if you want to change it.
4. Enter a new **Node Group Description** if you want to change it.
5. In the **Assign existing Node(s) to Node Group** section, select the nodes you want to add to the node group.
6. In the **Remove Node(s) from Node Group** section, select the nodes you want to remove from the node group.
7. Select the baseline and additional package if you want to change them for all the nodes in the node group.
8. Enter new user credentials if you want to change them. The credentials override the credentials on the nodes in the group.

   NOTE: If the iLO of the server is configured in one of the High Security modes or if `Require Host Authentication` is enabled, enter the iLO Administrator credentials in the provided section.

9. Click **OK**.

   NOTE: When you add new nodes to an existing node group, ensure that they are in the same state as the other nodes in the node group with the same baseline assigned. If you add nodes that are not in the same state as the other nodes, all the nodes in the node group are reset to idle after displaying a warning.

Performing node group inventory

Procedure

1. Select a node group from the list.

   NOTE: You can add nodes that have a common applicable source as repository in the same node group.

2. Select **Actions** > **Inventory**.

3. Assign a baseline and additional package, if required.

   NOTE: You can also assign install sets as node group baseline.

4. Click **Inventory**.

   NOTE:

   - You can add the iLO save install set selected in the inventory to the Task queue by clearing the Task queue. You can also select a common saved iLO install set displayed under the baseline selection.
   - You can view the logs stored in the iLO Task queue on the View log page. However, you cannot view live logs when the iLO and UEFI components are updated.

Deploying a node group

If all the server nodes in the group are at ready to inventory state, you can use the Review/Deploy action menu to direct deploy a common baseline.

Procedure

1. Select a node group from the list.
2. Select **Actions** > **Review/Deploy**.
3. Select the **Installation Options** you want to deploy.
4. Select **Component verbose log** if you want more detailed log files.
5. Select the **Reboot options**.
6. Review and correct if SUM displays any warnings or alerts. SUM does not deploy updates to the group unless you select **Ignore Warnings**.
7. Select whether to skip components that report dependency failures or missing component signatures.
8. In the **Baseline Library** section, select the components you want to deploy.
9. Click **Deploy**.
10. If you make changes, SUM verifies that there are no dependency errors, and then deploys the components. SUM does not begin deployment until failed dependencies are resolved. Either resolve the dependency, or clear the component.

Generating node group reports

Procedure

1. Select a node group from the list.
2. Select **Actions** > **Reports**.
3. Select the reports you want to generate and where you want SUM to save reports.
4. SUM generates the same reports for node groups and for nodes.

More information

Generating node reports

Deleting a node group

Procedure

1. Select a node group from the list.
2. Select **Actions** > **Delete**.
3. Confirm that you want to delete the node group.

Updating SUM from command lines

SUM provides methods to run system commands outside the GUI.

- **CLI**: Allows you to add all parameters in one command line, and then use the silent parameter to execute the entire sequence on multiple nodes without any user interaction. You can update one or more nodes using this method. For more information about using CLI, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide*.
- **CLI with Input Files**: Allows you to add all parameters to a text file, and then call SUM using the inputfile command with the text filename as the parameter. Using the input file method allows you to provide a larger number of nodes to update. For more information about using CLI with Input Files, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide*.
- **Interactive CLI**: Provides an interactive method for each step of a process. This method is similar to using the GUI but you provide individual commands instead. SUM interactive CLI runs a single command at a time. Using this method allows you to have nodes a different stage of update. For example, you can have one node in the inventory phase, one node in the deployment phase, and another node that you are adding. For more information about using Interactive CLI, see the *Smart Update Manager 8.4.0 CLI and Interactive CLI Guide*.
- **RPMs**: The SUM RPM deployment is a method for deploying firmware RPMs. For more information on deploying firmware RPMs, see **Deploying firmware RPMs**.
- **iSUT**: iSUT allows you to run scripts that can deploy updates to your nodes. Before running iSUT, configure the component. For more information on using iSUT, see the *Integrated Smart Update Tools User Guide*.

The SUM binary executable maintains state information as needed on a per-session basis. SUM saves this information in the `sum.ini` file. This file is in the `%localappdata%\sum\` location (Windows) and `/var/tmp/sum/`(Linux). SUM stores the user, session ID, host, and port information. This information enables you to log in and run SUM using different credentials.

Deploying firmware components

The primary function of SUM firmware commands is to flash or upgrade the firmware from the packaged contents to the device on the target host by using the `smartupdate upgrade` command.

NOTE:

- On Linux, two hyphens (--) are used before each argument.
- On Windows, a slash (/), hyphen (-), or two hyphens (--) can be used before each argument.

Procedure

1. Launch the firmware flash engine using the `smartupdate [GLOBAL OPTIONS] upgrade [OPTIONS]` command.

   Global options:

   - `-y`, `--yes`: Assume `YES` to all options (non-interactive).
   - `-v`, `--verbose`: Display verbose information.

   Other upgrade options:

   - `-h`, `--help`: Show this help message and exit.
   - `--ignore-warnings`: Ignores warnings SUM returns and proceeds with the installation.
   - `--dry-run`: Test that upgrade runs without issues. Does not deploy upgrades.
   - `-d`, `--downgrade`: Downgrade components.
   - `-r`, `--rewrite`: Rewrite components.
   - `--debuglogdir`: Defines the directory where SUM saves log files.
   - `--cleanup_onexit`: Cleans up the following:
     - FWRPMS copied to the IP folder.
     - Extracted FWRPM directory and files in the IP folder.
     - Unpacked components in the baseline.
     - All temporary directories the firmware wrapper generates.
   - `--cleanupall_onexit`: Cleans up everything, including the debug logs, generated by the firmware wrapper. This command does not delete the user logs.

For information on return codes from Linux and Windows smart components, see *Return Codes* in the *Smart Update Manager CLI and Interactive CLI Guide* at **www.hpe.com/info/sum-docs**.

Installing VMware software Smart Components on Gen10 using SUM and iSUT

To install the VMware ESXi software bundle Smart Components on Gen10 servers, you must configure the ESXi host with iSUT.

Starting Configuration

Install the HPE custom image for the required version of VMware ESXi.

Set up the ESXi host with iSUT

1. Install the appropriate vSphere Installation Bundle (VIB) for iSUT.

   NOTE: Currently, the iSUT products are smart components that do not unzip correctly on the ESXi platform. Unzip the Smart Component in Linux or uncompress them on Windows.

2. After you unzip the smart component to extract the sut-esxi<esxi OS version>-bundle-<iSUT Version>.zip file, copy the sut-esxi<esxi OS version>-bundle-<iSUT Version>.zip file to the ESXi platform, and then install the VIB:

   ```
   esxcli software vib install –d <sut-esxi**-bundle-***.zip>
   ```

3. Reboot the server.
4. If you want iSUT to run in Automode, change the mode to one of the auto modes. For example, `sut –set mode=autodeployreboot`.

Setup and execute the test using SUM

1. Get the appropriate SPP file.
2. If you are hosting the SPP on a Windows 10 environment, right-click the file, and then mount the *.iso.

   NOTE: If you are not hosting the SPP on a Windows 10 environment, use Virtual Clone Drive to mount ISOs.

3. Navigate to the folder that has the SPP files mounted, and then click **launch_sum.bat**. The SUM GUI screen appears.
4. Click **Baseline Library** at the upper-left corner of the SUM GUI.
5. To add an additional baseline package, click **Add Baseline** in the top-left pane. The Add Baseline Options screen appears.
6. Click **Add Baseline** in the pop-up window. The Add Baseline screen appears.

   NOTE: You must have both the cp*.zip and cp*.compsig files for the smart component available in the same location as the smart components.

7. Click **Add**. The “Additional package” gets added with a list of the smart components found at the location you specified.

NOTE: Use the “Additional package” as your baseline if you want to test the installation of the new components. You can test the installation by adding nodes.

For Gen10 servers, add an iLO node (use iLO IP for requested IP address).

8. Select Smart Update Manger in the top-left corner of the GUI, and then click **Nodes**. SUM starts performing “discovery” actions.

After adding a node, you can perform an inventory, and then deploy the smart components.

NOTE: For more information, see the SUM, HPE iLO Amplifier Pack, and HPE OneView documentation.

- Smart Update Manager User Guide: **www.hpe.com/info/sum-docs**
- HPE iLO Amplifier Pack User Guide: **www.hpe.com/support/ilo-ap-docs**
- HPE OneView 5.0 User Guide: **www.hpe.com/info/oneview/docs**

Advanced topics

- **About using SUM with IPv6 networks**
- **SUM network ports used**

Using SUM with IPv6 networks

You can deploy to remote nodes in IPv6-based networks for Windows and Linux node servers.

For Windows-based servers to communicate with remote node servers, SUM uses either existing credentials or the user-provided user name and password to connect to the admin$ share. This share is an automatic share provided by Windows Server. After SUM connects to the admin$ share, it copies a version of the engine to the node server for the duration of the installation. After this engine starts, SUM uses this engine to communicate between the local and remote node server.

Open the firewall ports SUM needs for communication. After the installation is completed or canceled, SUM stops the remote engine, removes it from the node, closes the port on the Windows firewall, and then releases the share between the node and the local system.

For Linux-based servers to communicate to remote node servers, SUM starts by using the user-provided user name and password to create an SSH connection to the node server. After it connects, SUM copies the engine to the node server for the duration of the installation. After this engine starts, SUM uses this engine to communicate between the local and remote node server.

During this process, SUM opens ports in the iptables firewall to enable SUM to communicate with the SUM engine over SSL to pass data between the local and remote systems. When the installation is completed or canceled, SUM stops the remote engine, removes it from the target server, closes the port in the iptables firewall, and then closes the SSH connection to the node server.

To set up IPv6 networking, refer the documentation for your operating system.

SUM network ports used

SUM requires that certain network ports are available. If you lock down network ports, make sure that the ports listed in the network port tables are open so that SUM works correctly when connecting to remote node servers and hosts. If you are unable to unlock these network ports, you must run SUM locally and update network-based hosts through their web interfaces (for example, the OA, iLO, and VC modules).

NOTE: Use the `open_firewall` parameter for SUM to automatically open the required firewall ports on the local host and any remote servers.

Updates for most node types require network traffic in both directions between the server running SUM and the node. The server running SUM creates a local HTTP server, which is used to serve firmware binaries to the node and to communicate node status. The remote node issues HTTP requests and posts status updates to the server running SUM during the update process. If there is a routing problem or firewall blocking traffic back from the remote node to the system running SUM, firmware updates might be blocked, status updates blocked or delayed, or both.

After creating the initial communication binds to one of the available ports, SUM traffic can move to a dedicated high-number port number (greater than 1024). This frees up the initial port for new requests.

System running SUM	Target node type	Inventory phase		Deployment phase	
		To target	From target (SUM 7.3.0 and later)	To target	From target (SUM 7.3.0 and later)
Windows	Windows	445, 135, 137, 138, 139	None	445, 135, 137, 138, 139	None
Windows or Linux	Linux	22	None	22	None
Windows or Linux	VMware: Only on Gen9 and previous generation servers	443, 5989	63001	443, 5989	63001
Windows or Linux	OA	22, (80), 443	None	22, (80), 443	None
Windows or Linux	Superdome X	22, (80), 443	None	22, (80), 443	63001, 63002
Windows or Linux	iLO, VC, FC switch, SAS switch	22, (80), 443	None	22, (80), 443	63001
Windows or Linux	Superdome Flex	443	None	443	63002

SUM uses port 63002 to communicate between the `sum_binary` and `sum_service` applications on both Windows and Linux systems. If ports are listed in both columns, SUM communicates bidirectionally.

NOTE:

- Windows to Windows traffic uses WMI, a standard DCOM-In port 135 and Async-in and WMI-in.
- To use the iLO Repository, iLO must be used as the 'target node type.'

Use the parameters `/port` and `/ssl_port` to change from ports 63001 and 63002 if there are firewall conflicts. Use `/open_firewall` to open the HTTP and HTTPS ports used by SUM for external access. Open these ports for remote node functionality and for remote browser access. For example:

```
smartupdate /port 80 /ssl_port 443
```

You can use the parameter `/ftp_port` to assign which port to use for FTP service. By default the FTP port is disabled. Use this option to enable the service.

Changing the port address in the `.ini` file

You can change the network ports SUM uses by editing the `sum.ini` file or using the `/port` or `/ssl_port` CLI parameters. For more information on using SUM CLI mode, see the *Smart Update Manager CLI Guide*.

The following commonly used alternate network ports are:

Procedure

1. `port=63001` edit to `port=80`.
2. `ssl_port=63002` edit to `ssl_port=443`.

SUM engine troubleshooting

SUM stops responding

Symptom

- SUM takes more time to deploy updates than expected.
- SUM stops responding when performing inventory on a baseline.
- SUM shuts down unexpectedly.
- SUM does not generate any dependency and fails to install when downgrading from iLO 5 1.15 to iLO 5 1.10.

Solution 1

Action

1. Try the following actions.
   - Launch SUM.
   - Run `clean-cache`, and then launch SUM.
   - Shut down the SUM engine. Use the command `smartupdate shutdownengine` from the SUM directory.
   - Restart the computer and run SUM again.

Solution 2

Cause

SUM might not have system or network resources.

Action

Do not deploy more than the 50 nodes at a time, or 10 VMware nodes at a time.

Solution 3

Cause

Performing inventory on more than one baseline might use too many system resources.

Action

Perform inventory on one SPP baseline at a time.

Solution 4

Cause

SUM does not show any dependency and fails to install because SUM 8.5 does not support iLO downgrade.

Action

Perform the downgrade outside of SUM. Extract iLO 5 Smart Component to a directory and then upload the firmware binary file directly using the iLO 5 interface.

SUM unexpectedly logs off users

Symptom

SUM logs out a user after an extended inactive period.

Cause

This is intentional. After an extended period of no activity, SUM logs out users.

Action

Log in to SUM with your user credentials.

SUM displays component failed validation error

Symptom

When SUM is run on a Windows system to deploy SPP, the Windows components install might fail with the error: `Signature validation failed on this component`.

Cause

The issue is caused due to the missing root and CA certificates in the system. To resolve this issue, perform the following steps and retry the update.

Action

1. Download the following two certificates:
   a. **https://secure.globalsign.net/cacert/Root-R1.crt**
   b. **https://support.comodo.com/index.php?/Knowledgebase/Article/View/945/96/root-addtrust-external-ca-root**
2. Right-click a certificate and select **Install Certificate**.
   A Windows wizard appears.
3. On the Welcome screen of the wizard, click **Next**.
4. On the Certificate store page of the wizard, select **Place all certificates in the following store**.
5. On the Certificate store page of the wizard, click the **Browse** button.
6. In the Select Certificate Store dialog box, select **Third Party Root Certification Authorities**, and then click **OK**.
7. On the Certificate store page of the wizard, click **Next**.

8. On the Completing the Certificate Import Wizard page of the wizard, click **Finish**.
9. Repeat steps 2-8 for the other certificate.

SUM displays zero free space on a drive

Symptom

SUM displays a warning that there is no free disk space when an available disk has more than 4 TB available.

Action

1. In GUI mode, select **Ignore Warnings** on the Deploy screen.
2. In CLI mode, include the `/ignore_warnings` parameter.
3. In Input file mode, include the parameter `IGNOREWARNINGS=YES`.
4. In iCLI mode, include the parameter `ignore_warnings=true`.

   Example: "`smartupdate setattributes --nodes <IP> ignore_warnings=true`"

Text is not translated

Symptom

Some text on screens is not translated.

Action

No action. This is a known issue that will be fixed in a future version.

SUM restricts multiple connections to a server or shared resource by the same user

Symptom

An error occurs when multiple connections to a server or shared resource is used by the same user.

Cause

SUM uses the **admin$ share** function on Windows-based servers to copy files and perform required operations on remote node servers. If multiple connections to the remote Windows node is detected, the system will display an error message, as SUM will not allow more than one user name. In such instances, disconnect all previous connections to the server or shared resource, and try again.

If SUM displays the error, check for open `<filepath>admin$</filepath>` shares on the remote node you want to update, and remove the connections. Use the following commands to check for open shares and delete them:

Action

1. Open a command prompt window.
2. Type **`net use`**.
3. If open connections on the remote node are found, type **`net use <node_admin_share> /delete`**.
4. Attempt the operation in SUM that caused SUM to display the error.

SUM reports port errors

Symptom

SUM reports errors with blocked ports or does not disconnect from ports.

Action

1. Close SUM, and then reboot the system.
2. Clear the ports used in `sum.ini`.
3. Launch SUM.

   If you have intentionally blocked a port, rebooting the system will not unblock the port. Unblock the port manually and then launch SUM.

Browser closes connection with SUM

Symptom

The Chrome or Internet Explorer browser closes the connection with SUM, but leaves SUM running.

Cause

The browsers Internet Explorer and Chrome might disconnect from a SUM connection session.

Action

1. Open a terminal window, and then navigate to the directory from where SUM was launched.
2. Type the command `smartupdate /shutdownengine` (Windows).
3. Relaunch SUM.

SUM does not allow user to log off as expected

Symptom

While running a process, users cannot log off as expected.

Action

Wait until SUM ends all inventory and deploy processes before attempting to log off.

Baseline troubleshooting

SUM displays a dependency error for self-inventory components

Symptom

On the Baseline Library screen, SUM displays a dependency error for components that perform a self-inventory.

Cause

Users deployed a server while using a root user account and are using sudo permissions to run SUM.

Action

Delete the following directory.

`/var/tmp/sum`

SUM does not validate a component

Symptom

The Baseline Library screen does not validate a component.

Cause

A compsig file is missing. Gen10 server and VMware nodes require compsig files before you can deploy the update.

Action

1. Delete the component from the baseline directory.
2. Download a new copy of the component to the baseline directory.
3. Download the compsig file for the component.
4. Validate the baseline.

More information

Re-validating baseline components

SUM displays multiple versions of the same component

Symptom

When you are creating a custom baseline, SUM displays multiple versions of a component.

Cause

Multiple source baselines contain the same component.

Action

Select one copy of the component.

Custom baseline screen does not display node types

Symptom

SUM does not display a node type when filtering source for a custom baseline.

Solution 1

Cause

The source baselines might not contain components for that node type.

Action

Make sure that the baseline includes components for the node type.

Solution 2

Cause

A node type might be clear.

Action

Deselect all node types in **Advanced filters** to see all components in baseline sources, and then select the components you want to add to the baseline.

SUM does not save baselines after a Remote Desktop session

Symptom

SUM does not save baseline or node information between Remote Desktop sessions.

Cause

Remote Desktop does not save the temporary folders between sessions.

Action

For more information, see the article on the Microsoft website **https://technet.microsoft.com/en-us/library/cc755098.aspx**.

SUM does not validate HTTP baselines

Symptom

SUM cannot validate a baseline downloaded from an HTTP repository.

Cause

SUM does not validate a baseline it downloads through HTTP. The .exe files downloaded are not compared against a manifest file.

Action

This is the expected behavior of SUM.

SUM screens display outdated information

Symptom

The information SUM displays on a screen is outdated and incorrect.

Cause

The web browser has saved a cached version of the SUM screen.

Action

Clear the web browser cache.

SUM refreshes the browser when adding a baseline

Symptom

SUM refreshes the browser window when you click **Retrieve List** when adding a baseline pulled from the web.

Cause

This is an issue that happens with Internet Explorer 11.

Action

Use a different web browser.

Baseline inventory does not respond for SPP ISO

Symptom

Performing SUM inventory when an SPP ISO is mounted via Gnome Virtual file system does not respond.

Cause

Gnome Virtual file system does not apply the read and execute permissions for the files.

Action

Manually extract the SPP to a directory, and then launch SUM.

Node troubleshooting

Google Chrome crashes frequently on the Nodes page

Symptom

Google Chrome version 54 crashes while adding a node on the Nodes page.

Cause

The computer might not have enough memory available to support Google Chrome version 54.

Action

1. Update the Chrome version.
2. Relaunch the browser.
3. In Settings, disable all third-party extensions.
4. Reload the webpage.

SUM dependency issues

Symptom

1. SUM displays the component error: `Missing 32 lib depend.`
2. SUM lists SUSE Enterprise Linux dependencies for Red Hat Enterprise Linux systems.

Solution 1

Cause

Your systems might not have all 32–bit dependencies installed.

Action

Make sure that you have all the 32-bit libraries installed on your system. View the component release notes for details on required libraries.

Solution 2

Cause

SUM incorrectly lists the SUSE components instead of Red Hat components.

Action

No action.

Unable to add a node in High Security mode

Symptom

When you add a node, a message displays that the iLO has been configured in High Security mode.

Cause

iLO has been configured in one of the High Security modes that requires iLO Administrator credentials while adding a node.

Action

1. SUM provides a link to Enter iLO Credentials. Click the link to open a dialog box.
2. Enter the iLO Administrator Username and Password in the required field.

SUM does not add an SMB-enabled Linux node with Unknown node type

Symptom

When the SMB service is running on a Linux server, it provides access to the path `\\<ip>\admin$` or mimics the existence of this path. Therefore, if you add such a Linux node to SUM in CLI, iCLI, IPF, or GUI modes without providing the node type, the node is identified as a Windows node. As a result, SUM displays the error message `Invalid username or password.`

Action

Do not add an SMB-enabled Linux node without specifying the node type.

SUM has an issue with sudo user

Symptom

SUM does not respond when editing a node with sudo.

Browser will not invoke if SUM is launched from a sudo user.

Solution 1

Cause

The user credentials might not have administrator privileges on the remote node.

Action

Make sure the user that is logged in to SUM is part of the administrator group for the system.

Solution 2

Cause

When SUM is launched as a sudo user from a Linux node, the browser will not invoke.

Action

The following command should be used from sudo user login to get the GUI in the browser window:
`sudo -H env DISPLAY=:0 ./smartupdate`

The SUM Deploy button is disabled

Symptom

SUM disables the **Deploy** button on the Deploy Nodes screen.

Cause

SUM discovered a failed dependency.

Action

Make sure that SUM has resolved all dependencies before attempting to deploy updates.

SUM node inventory fails

Symptom

- Inventory does not respond on remote Windows nodes. The node logs display error message regarding the status of `RegOpenEx`.
- SUM displays an inventory error on a VMware node.

Solution 1

Cause

Other processes, such as a backup or process that accesses the registry might be running on the remote Windows node.

Action

Shut down the remote process that is accessing the registry, or run SUM locally on the node to perform inventory and deploy updates.

Solution 2

Cause

The VMware service might not be running.

Action

1. Make sure the VMware service is running. Log in to the VMware ESXi shell.
2. Check the provider version, and then enter `esxcli software vib list | grep smx`.
3. Verify if the provider service is running, and then enter `/etc/init.d/sfcbd-watchdog status`.
4. Verify if the provider responds to queries, and then enter `enum_instances SMX_SCInstallationService root/hpq`.
5. To restart the service, enter `/etc/init.d/sfcbd-watchdog restart; /etc/init.d/sfcbd-watchdog status;`.

SUM does not detect a component

Symptom

SUM might not detect some components, for example, a solid-state hard drive.

Cause

Information that SUM gathers from the component might not match information from the node.

Action

If SUM does not detect a component, and the component is available in the baseline, run the component outside of SUM.

Linux hosts do not add Windows nodes

Symptom

SUM does not add a Windows node when running SUM on a Linux host.

Cause

SUM does not support deploying updates from a Linux host to a remote Windows node.

Action

Run SUM on a Windows host to add Windows nodes.

SUM cannot connect to a node

Symptom

SUM displays the message: `Unable to login or identify node as a supported device.`

Solution 1

Cause

SUM has connection issues with the remote node.

Action

1. Check the following:
   - The node is active on the network.
   - Network ports are open.
   - Make sure that Windows nodes have the $Admin share enabled.
   - Make sure that HTTP and SSH access are enabled for Linux nodes.

Solution 2

Cause

User credentials are incorrect.

Action

Verify that valid user credentials are provided.

No component version information displayed

Symptom

SUM does not display version information for a component.

Cause

SUM does not read the component contents correctly.

Action

If you know that the component is the version you want to use, run SUM in online mode and force the deployment of the component.

Command `open_firewall` does not work

Symptom

The CLI command `open_firewall` does not work on some nodes.

Cause

SUM is unable to open the firewall in all instances. These include: third-party firewall applications, Linux iptables DROP entries, and firewalls with complex rules.

Action

When the `open_firewall` command does not work, manually open the firewall and then SUM can manage the node.

Firewall error on a remote node error

Symptom

SUM reports a potential error with a firewall on a remote node.

Action

Make sure that no firewall is running, network ports are open, review the `http_proxy` parameter, `https_proxy` parameter, and review the CURL proxy settings.

You can find more information about CURL proxy settings at the website **https://curl.haxx.se/docs/manpage.html**.

You can find SUSE Linux Enterprise Server node proxy configurations in the directory `etc/sysconfig/proxy`.

Determining which HPCISSS2 and HPCISSS3 drivers to install

Symptom

Unsure which HPCISSS2 and HPCISSS3 drivers SUM installs.

Action

If you are updating the Smart Array SAS/SATA driver, use the following table to determine which driver SUM installs if you select both the HPCISSS2 and HPCISSS3 drivers on the Review/Deploy screen:

Installed driver version	CISSS2	CISSS3
HPSAMD driver	Installs if only this driver is selected.	Installs CISSS3 if both drivers were selected.
HPCISSS2 driver	Installs and updates.	
HPCISSS3 driver		Installs and updates.

SUM does not overwrite an HPCISSS3 driver with HPCISSS2, or HPCISSS2 with HPCISSS3. After an update, SUM displays that the HPCISSS3 driver overwrote the HPCISSS2 driver, or HPCISSS2 overwrote HPCISSS3. When you relaunch SUM, it displays that the driver did not install and is ready to install.

If you want to install a specific driver and SUM installs the other driver, perform an update outside of SUM to install the selected driver.

SUM skips Broadcom ports

Symptom

SUM does not update a Broadcom node.

Cause

Broadcom port is not up when SUM attempts to deploy updates.

Action

View the prerequisites of the appropriate driver for your network adapter installation to view the required port state.

SUM reports OA update incorrectly

Symptom

Fully installed OA updates are reported in SUM as failed.

Cause

There is a timing issue between SUM and the target node.

Action

Close and restart SUM, and then run inventory on the node to detect the component version details.

SUM does not deploy to Windows cluster nodes

Symptom

Unexpected issues occur when deploying updates to nodes that are part of Windows clusters.

Cause

SUM does not support Windows clustering environments.

Action

1. Remove the node from a Windows cluster.
2. Attempt the action again.

SUM does not process encryption keys included in node input file details

Symptom

When added in an input file node details, an encryption key is not processed as expected.

Action

SUM processes the `ENCRYPTION_KEY` parameter as a global parameter, not an individual parameter. If different keys are required, use multiple input files.

SUM does not delete install sets from the Nodes page in IE 11.44

Symptom

When you click the **Delete** button to delete install sets from the Nodes page, the page is refreshed and you are redirected to the SUM Home page.

Cause

This issue is seen only in Internet Explorer 11.44 on Windows Operating System 2016.

Action

This is a browser-specific issue and seen only in IE 11.44.

Linux firmware RPM mode does not support setting attributes containing string value with parenthesis

Symptom

In Linux firmware RPM mode, when setting any attributes which takes string as a value and the value contains parenthesis — "(" and ")" — the deployment fails.

Cause

Parentheses are interpreted as special characters and the shell does not support them.

Action

1. Use an escape sequence for the parentheses.

- Example1: `install_set_name='"test (installset)"'`
- Example 2: `install_set_description="test \(installset\)"`

VMware troubleshooting

RPM updates do not deploy to VMware nodes

Symptom

SUM does not deploy RPM updates to VMware ESXi nodes.

Cause

RPM packages only support Linux nodes.

Action

No action.

Unsupported Windows ROM components list on Gen10 VMware OS instead of VMware components

Symptom

During online remote flashing of VMware 6.0u3 OS on Gen10 server, unsupported Windows components list on the Review page.

Cause

SUM can pull the signed secure flash binary to upload to the iLO Repository from either firmware packages or Windows .exe smart components. If a firmware package is not available, SUM gets the signed secure flash binary image from a Windows component.

Action

Select the Windows components to proceed with the deployment.

Reports troubleshooting

SUM does not generate reports

Symptom

SUM cannot generate reports for a node.

Cause

The node is offline or SUM cannot access the node.

Action

Make sure the node is online, that the firewall is open, and that SUM can ping the node.

Deploying firmware RPMs

This section describes using SUM firmware commands to deploy ProLiant firmware in the RPM format to nodes running supported Linux operating systems.

About the SUM RPM tool

SUM firmware commands tool is available at **https://www.hpe.com/support/SDR-SUM**. For information on the prerequisites for running SUM, see the SUM release notes. Versions are available for supported Red Hat Enterprise Linux and SuSE Linux Enterprise Server operating systems.

About SPP ISO and RPMs

The SPP ISO requires an active warranty or support contract. The SDR splits the ISO content into SPP and FWPP repositories. The SPP repository provides freely-available drivers, agent software, and firmware, while the FWPP repository provides a complete set of HPE firmware that requires a warranty or support contract.

Accessing firmware RPMs

Procedure

Use normal Linux tools (for example, YUM), to pull a collection of system firmware from a centralized repository, for example the Software Delivery Repository at **https://downloads.linux.hpe.com/SDR**.

Prerequisites

Procedure

Perform these tasks on the target system, and run them with `uid=0` (root) privileges.

Using YUM and ZYPPER distributions

Using YUM and ZYPPER distributions

Install, deliver, and locally cache applicable firmware.

Procedure

1. To subscribe to a SUM repo, follow the instructions provided at **https://downloads.linux.hpe.com/SDR/project/hpsum/**.
2. Automatically find required packages:
   - Install the SUM firmware commands utility.
   - Use SUM to query the system and report which packages you need.
   - For RHEL systems, configure yum and for SLES systems, configure zypper.

- Install SUM rpm on the respective OS using the command:
  - `yum install sum`

    OR
  - `zypper install sum`
- Run the command: `smartupdate install requires`

Deploying firmware components

The primary function of SUM firmware commands is to flash or upgrade the firmware from the packaged contents to the device on the target host by using the `smartupdate upgrade` command.

NOTE:

- On Linux, two hyphens (--) are used before each argument.
- On Windows, a slash (/), hyphen (-), or two hyphens (--) can be used before each argument.

Procedure

1. Launch the firmware flash engine using the `smartupdate [GLOBAL OPTIONS] upgrade [OPTIONS]` command.

   Global options:

   - `-y, --yes`: Assume `YES` to all options (non-interactive).
   - `-v, --verbose`: Display verbose information.

   Other upgrade options:

   - `-h, --help`: Show this help message and exit.
   - `--ignore-warnings`: Ignores warnings SUM returns and proceeds with the installation.
   - `--dry-run`: Test that upgrade runs without issues. Does not deploy upgrades.
   - `-d, --downgrade`: Downgrade components.
   - `-r, --rewrite`: Rewrite components.
   - `--debuglogdir`: Defines the directory where SUM saves log files.
   - `--cleanup_onexit`: Cleans up the following:
     - FWRPMS copied to the IP folder.
     - Extracted FWRPM directory and files in the IP folder.
     - Unpacked components in the baseline.
     - All temporary directories the firmware wrapper generates.
   - `--cleanupall_onexit`: Cleans up everything, including the debug logs, generated by the firmware wrapper. This command does not delete the user logs.

For information on return codes from Linux and Windows smart components, see *Return Codes* in the *Smart Update Manager CLI and Interactive CLI Guide* at **www.hpe.com/info/sum-docs**.

Other RPM commands

info

Gather information about the firmware packages available on the target system.

Syntax

```
smartupdate info
```

requires

Gather information about the PCI devices currently installed on components.

Syntax

- `smartupdate install requires`

  Installs the firmware RPM files from the repository.

- `smartupdate remove requires`

  Removes the firmware RPM files.

list

Gather information about the firmware packages available compared to what is installed on the target host.

Syntax

```
smartupdate list
```

Example output

```
smartupdate list

Searching for firmware.
Analyzing results.

Info | NAME                        | VERSION         | INSTALLED    | TYPE   |
-------------------------------------------------------------------------------
icRU | system-p70                  | 2015.07.01      | 2015.07.0    | system |
ifrU | ilo4                        | 2.5             | 2.4          | ilo    |
```

Parameters

`I`—Installable

`1`: Yes, can be installed.

—: Cannot be installed.

`c`—Criticality

`c`: Addresses a critical issue.

`f`: Addresses an issue.

`e`: Enhanced functionality.

–: No information.

`r`—Reboot

`r`: The package requires a reboot to apply the update, but the firmware is up-to-date, no action required.

`R`: The next time the update command is run a reboot will be required.

–: No reboot required.

`version cmp`—Different between applied version and version in the package.

–: The versions are the same.

`d`: The version in the package is older than the currently applied version.

`U`: The version in the package is newer than the currently applied version.

Options

Use a filter string for most commands to work with a specific firmware package or subset.

Example filter output

```
smartupdate list '%{NAME} =~ /p70/'

Searching for firmware.
Analyzing results.

Info | NAME                | VERSION         | INSTALLED     | TYPE   |
-------------------------------------------------------------------------
icRU | system-p70          | 2015.07.01      | 2009.07.00    | system |
```

query

Extract package information in a format that you define.

Syntax

```
smartupdate query


Searching for firmware.
Analyzing results.

system-p70
-----------------------------------------------------------------------------------------------------------
%{RELEASEDATE_SECOND} 57
%{RELEASEDATE_MONTH} 9
%{FIRMWARE_STRING} smartcomponent-linux-firmware-system
%{RPMNAME} hp-firmware-system-p70
%{REBOOT_REQUIRED} yes
%{VERSIONID} 4082a4f9023d47b082a48853ff659c08
%{RELEASENUM} 1.1
%{MODEL}
%{XSL}
%{LANGUAGE} English (US)
%{FILENAME} CP027723.scexe
%{PLATFORM} red_hat_enterprise_linux_x86
%{RELEASEDATE_DAY} 3
%{UNINSTALL_SILENT}
%{UNINSTALL_COMMAND}
%{PRODUCTID} 047d8b4df70c471db61bbfce96870076
%{UNINSTALL_COMMAND_PARAMS}
%{RELEASEDATE_HOUR} 13
%{INSTALL_NEEDUSERACCT} no
%{PLATFORM_MAJOR} 6
%{FIRMWARE_ID} system-p70
%{INSTALL_COMMAND_PARAMS}
```

```
%{VERSION} 2015.07.01
%{FIRMWARE_NAME} system-p70
%{ALTNAME} HP ProLiant DL380p Gen8 (P70) Servers
%{RELEASE} 1.1
%{NAME} Online ROM Flash Component for Linux - HP ProLiant DL380p Gen8 (P70) Servers
%{TYPE_OF_CHANGE} 0
%{MANUFACTURER_NAME} Hewlett-Packard Development Company, L.P.
%{DESCRIPTION} This component provides updated system firmware that can be installed directly
on supported Operating Systems. Additionally, when used in conjunction with Smart Update
Manager (SUM), this Component allows the user to update firmware on remote servers from a
central location. This remote deployment capability eliminates the need for the user to be
physically present at the server in order to perform a firmware update.
%{INSTALL_COMMAND}
%{INSTALL_SILENT} yes
%{INSTALL_COMMAND_REBOOT_REQUIRED} yes
%{UNINSTALL_COMMAND_REBOOT_REQUIRED}
%{DEBNAME} hp-firmware-system-p70
%{RELEASEDATE_MINUTE} 49
%{TYPE_OF_CHANGE_TXT} enhancement
%{RELEASEDATE_YEAR} 2015
%{REVISION}
```

erase

Erases the components that the command `smartupdate remove requires` installs.

Syntax

Use the command for your Linux operating system.

RHEL

```
yum erase $(smartupdate remove requires)
```

SLES

```
zypper remove $(smartupdate remove requires)
```

RPM downloads are blocked

Symptom

RPM downloads are blocked.

Cause

A dependency error prevents SUM from downloading RPMs.

Action

Use the command to continue downloads when SUM encounters an error: `yum install $(smartupdate install requires) --skip-broken`

`smartupdate upgrade` returns an error

Symptom

When running the command `smartupdate upgrade`, an error is shown instead of installing the update.

Action

Run the command `smartupdate upgrade` a second time.

RPM mode does not correctly handle Smart Array firmware

Symptom

SUM commands `requires`, `upgrade`, and `list` do not accurately work with Smart Array firmware.

Action

Deploy Smart Array firmware with GUI or CLI mode.

iLO Repository component install types

The iLO Repository is a new feature in servers with iLO 5. It provides a mechanism to perform firmware, driver, and system software updates across the management network through iLO. Tools like HPE OneView, iLO Amplifier Pack, and SUM already use iLO Repository, thus reducing traffic on the production network and reducing production load downtime.

Tools upload components to the iLO Repository along with an install set, which includes instructions for installing the components to the server. The install set includes information such as component install order and information on reboot. The install set also provides details about components, including the component type that indicates how the component gets installed. Install sets are built by SUM and ordered properly to reduce the overall number of reboots during the upgrade. Install sets get copied to the iLO Repository task queue to begin the upgrade process.

NOTE: iSUT cannot install itself on remote systems. Therefore, if iSUT is in an install set, then either iSUT must be installed on the target system or SUM must be run from the target system to execute the install set.

You can run the SPP against that system the first time to get iSUT installed. Alternatively, you can install just the iSUT component manually.

Various installers monitor the task queue and operate on the top item on the queue. The various installers are as follows:

iLO

While iLO can update different firmware components types, iLO is the only mechanism for updating some components, specifically, secure flash firmware components. These components include the system ROM, Power Pic, and iLO itself. Some of these components can be installed and activated immediately, while others require a restart before activating.

UEFI

UEFI monitors the task queue during POST and installs any firmware components that it can. UEFI can upgrade most firmware components, such as ME (SPS), IE, few NICs, and Smart Array. However, it is the only mechanism to install some firmware, such as TPM and NVDIMM.

After an upgrade, UEFI performs a reboot to activate the firmware.

iSUT running in the OS/hypervisor

iLO and UEFI can update firmware components from the iLO Repository task queue, but not software and drivers. Software and drivers must be updated from the running production operating system. iSUT installed in the OS can monitor the iLO Repository task queue for firmware, drivers, or system software that can be upgraded from the OS. Some hard drive firmware can only be upgraded in the OS.

SUM can also upgrade firmware, system software, and drivers on systems with pending iLO Repository task queues.

iSUT or SUM can restart the system as necessary after a successful update to activate the components.

Websites and support

Websites

Hewlett Packard Enterprise Information Library	**www.hpe.com/info/EIL**
Smart Update Manager	**www.hpe.com/servers/sum**
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/isut-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:
  https://www.hpe.com/info/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
  https://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages

- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

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

  Hewlett Packard Enterprise Support Center

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

  Hewlett Packard Enterprise Support Center: Software downloads

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

  Software Depot

  https://www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

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

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

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

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

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

HPE Proactive Care services

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

HPE Datacenter Care services

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

HPE Proactive Care service: Supported products list

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

HPE Proactive Care advanced service: Supported products list

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

Proactive Care customer information

Proactive Care central

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

Proactive Care service activation

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

Warranty information

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

HPE ProLiant and IA-32 Servers and Options

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

HPE Enterprise and Cloudline Servers

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

HPE Storage Products

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

HPE Networking Products

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

Regulatory information

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

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

Additional regulatory information

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

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

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

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

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

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

Documentation feedback

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