Smart Update Manager 20.1.0 User Guide

Part Number: 30-FE14CFC7-001
Published: October 2026
Edition: 1

Smart Update Manager 20.1.0 User Guide

Abstract

This document explains how to install, configure, and use SUM to perform firmware updates on supported HPE server solutions. Before using the solution, you must understand the supported environments and be aware of potential risks, such as service interruptions during firmware updates.

Part Number: 30-FE14CFC7-001
Published: October 2026
Edition: 1

© Copyright 2026 Hewlett Packard Enterprise Development LP

Notices

The information provided here is subject to change without notice. Hewlett Packard Enterprise's products and services are covered only by the express warranty statements that come with them. This document does not constitute an additional warranty. Hewlett Packard Enterprise is not responsible for any technical or editorial errors or omissions in this document.

Confidential computer software. You must have a valid license from Hewlett Packard Enterprise to possess, use, or copy the software. In accordance 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 the vendor's standard commercial license.

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

Acknowledgments

Adobe, the Adobe logo, Acrobat, and the Adobe PDF logo are either registered trademarks or trademarks of Adobe in the United States and/or other countries.

Google™ and the Google Logo are registered trademarks of Google LLC.

Intel Inside®, the Intel Inside logo, Intel®, the Intel logo, Itanium®, Itanium® 2-based, and Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

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

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

Mozilla® and Firefox® are trademarks of Mozilla Incorporated.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, LLC in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates.

VMware®, VMware ESXi™, and VMware vSAN™ are registered trademarks or trademarks of VMware by Broadcom, Inc. and its subsidiaries in the United States and other jurisdictions.

All third-party marks are property of their respective owners.

Table of contents

Smart Update Manager....7
Capabilities of SUM....8
Management interfaces for SUM....10
SUM 12.x and 20.x CLI compatibility and REST API workflow mapping....11
Getting started with Smart Update Manager....17
Prerequisites for deploying and using SUM....17
Getting SUM from the SPP....20
Downloading SUM from HPE website....20
Installing and using Smart Update Manager....21
Installing standalone SUM on Windows....21
Installing standalone SUM on Linux....22
Launching SUM from SPP for Windows....23
Launching SUM from SPP for Linux....25
Logging in to SUM....26
Handling browser security certificates....27
Importing the security certificate into Mozilla Firefox....27
Importing the security certificate into Google Chrome....28
Importing the security certificate into Microsoft Edge....29
Switching between legacy SUM and next-generation SUM from SPP....30
Starting, stopping, and verifying the SUM service....31
Remote access to SUM....33
Opening the SUM firewall port for remote access....34
Managing servers....35
Adding servers through remote iLO....35
Localhost server discovery and onboarding....37
Verifying localhost server added automatically....37
Adding localhost server by providing iLO credentials....38
Removing servers....39
Managing firmware baselines....40
Downloading Service pack for HPE ProLiant from HPE website....40
Adding firmware baseline....41
Removing firmware baselines....42
Adding component packages....43
Removing component packages....44

Managing custom baselines..... 44
Creating a custom firmware baseline..... 45
Downloading a custom firmware baseline..... 47
Updating firmware 48
Prerequisites to update firmware..... 48
Updating firmware remotely using iLO..... 50
Updating firmware using localhost..... 53
Smart Update Manager CLI..... 55
About SUM user.yaml configuration file..... 61
Modify SUM user.yaml settings..... 61
SUM user.yaml configuration parameters..... 62
Reports..... 67
Viewing the last analysis operation report and reviewing analysis preconditions 68
Viewing the last update operation report..... 69
Last update operation status..... 69
Smart Update Manager API 70
Log files and directory locations..... 70
Default file and directory locations..... 70
Local database..... 72
Firmware baseline storage..... 72
Configuration notes..... 73
Application logs and log locations..... 74
Audit logs and logging configuration..... 74
GatherLogs utility..... 76
Troubleshooting..... 78
Localhost record created with incomplete details..... 79
Localhost onboarding skipped..... 80
Service does not start because port 63002 is already in use..... 80
Custom baseline service does not start because port 63003 is already in use... 81
Service does not start or exits immediately..... 81
Browser displays a certificate warning during HTTPS access..... 82
Cannot log in with valid credentials..... 82
Firmware upload does not complete successfully..... 83
Target iLO endpoints are not discovered or onboarding fails..... 84
Custom SPP creation or component package operations are unavailable..... 84
User account is temporarily locked after repeated login attempts..... 85

API requests return authentication errors after token expiration..... 86
ZIP firmware baseline upload is rejected..... 86
Firmware baseline is marked invalid after startup verification..... 87
Browser displays old SUM UI content after upgrade..... 87
SUM next-generation page does not open..... 88
HPE Compute Software and Firmware Product Documentation Quick Links..... 89
Websites..... 90
Support and other resources..... 90
Accessing Hewlett Packard Enterprise Support..... 91
HPE product registration..... 91
Accessing updates..... 92
Remote support..... 92
Warranty information..... 93
Regulatory information..... 93
Documentation feedback..... 94
Documentation feedback..... 94

Smart Update Manager

Smart Update Manager (SUM) is an on-premises firmware management solution that orchestrates firmware updates across managed HPE servers. It provides a scalable, automated framework for managing firmware lifecycle operations across multiple servers.

By integrating proven capabilities from HPE Compute Ops Management and HPE OneView, SUM enhances the firmware update experience and delivers a consistent, extensible firmware management platform.

The solution is built on a modular architecture that standardizes firmware update workflows, provides a consistent firmware management experience across HPE solutions, and simplifies integration and operational management. As a result, SUM helps minimize operational risks associated with inconsistent firmware deployments, firmware states, and update outcomes across different environments.

To further improve operational reliability, the solution employs standardized processes, validation steps, and controlled orchestration to deliver predictable updates at scale.

Legacy and Next-Generation SUM

SUM 20.x and later releases represent the next-generation SUM, while SUM 12.x and earlier releases represent legacy SUM. In this guide, the term next-generation SUM is used only when it is necessary to distinguish SUM 20.x from the legacy SUM. Otherwise, the product is referred to as Smart Update Manager (SUM).

Considerations

SUM uses TCP port 63002. Earlier versions of SUM also use this port. As only one application can use the port at a time, next-generation SUM and legacy SUM versions cannot run simultaneously on the same system.

Before launching next-generation SUM, stop any legacy SUM instance and verify that TCP port 63002 is available.

> **NOTE**
>
> Click the **Help** icon to access the user guide on the appliance, even when there is no internet connectivity.

Subtopics

Capabilities of SUM
Management interfaces for SUM
SUM 12.x and 20.x CLI compatibility and REST API workflow mapping

Capabilities of SUM

The solution provides on-premises firmware lifecycle management for HPE server environments. It uses web UI, REST API, and CLI to manage firmware update workflows from a centralized host.

- **Server discovery and onboarding**
  - Discovers servers using single, multiple, or range-based HPE iLO IP addresses.
  - Supports simple onboarding of servers for firmware lifecycle operations.
  - Maintains a local inventory of managed servers.
- **Firmware baseline management**
  - Supports uploading of Service pack for HPE ProLiant (SPP) ISO or ZIP files as firmware baselines.
  - Supports adding, managing, and removing standard and customized baselines.
  - Processes multiple baselines to support scalable firmware management operations.
  - Validates and processes firmware baseline metadata before update operations.
- **iLO update methods**
  - Local and remote iLO update.
- **Firmware analysis and updates**
  - Supports remote and localhost firmware updates.
  - Performs preflight checks to improve the firmware update experience and verify compliance.
  - Applies firmware baselines to servers through HPE iLO.
- **Activity tracking and monitoring**
  - Tracks long-running operations through jobs and activity records.
  - Monitors and records long-running operations such as onboarding, baseline processing, and firmware updates through activity messages.
- **API and automation support**
  - Provides REST APIs for lifecycle management of servers, baselines and bundles, custom SPPs, and firmware updates, including discovery, onboarding, provisioning, update, and removal operations.

- Supports API-driven automation and integration with external tools and workflows.

- **Security and access control**
  - Authenticates users with host OS credentials.
  - Protects stored iLO credentials using AES-256-GCM encryption.
  - Enables HTTPS to secure communications for the web UI and REST API.
  - Uses OS authentication with bearer-token-based sessions.
- **Upgrade support**
  - Supports upgrades to future releases while preserving server and baseline configurations.
  - Stores server, firmware bundle, job, and activity data in a local SQLite database.
- **Diagnostics and usability**
  - Collects logs and diagnostic data through the gatherlogs support bundle utility.
  - Provides an intuitive UI that simplifies firmware management operations and provides a consistent user experience.
- **Reports**
  - Generates firmware analysis reports that show the expected impact of applying a selected firmware baseline, including affected components, update classifications, and recommendations.
  - Generates firmware update reports that summarize update results, including component-level status, firmware versions, update options, and post-update results.
  - Enables you to export report data for troubleshooting, support, and audit activities.
- **Custom baseline management**
  - Supports downloading the custom baseline in ISO and ZIP formats.
  - Provides component package management capabilities for custom SPPs, including adding packages to the repository, replacing existing SPP components, and removing components from the repository.
- **Localization**
  - Supports localized API error messages and activity messages.

- Supports English, Japanese, and Simplified Chinese through standard language headers.

Management interfaces for SUM

The solution supports the following management interfaces:

- **Web UI** for interactive server management, firmware baseline management, firmware update workflows, activity tracking, and job monitoring. The UI follows HPE Compute Ops Management workflow patterns to deliver a consistent user experience. For Web UI workflows, see the corresponding procedures in this guide.
- **CLI** through the `smartupdate` compatibility command for scripted firmware update operations. Key commands are compatible with earlier SUM releases. For CLI syntax, options, and examples, see Smart Update Manager CLI.
- **REST API** over HTTPS to enable automation and integration with external tools and workflows. API clients authenticate and include a bearer token when accessing protected resources. Where applicable, the API request and response models align with HPE Compute Ops Management APIs. For REST API workflows and endpoint details, see the **Smart Update Manager API Reference**.

Supported operations by management interface

Operation	Web UI	CLI	REST API
Firmware update of a single server	✓	✓	✓
Firmware update of a single server with automatic reboot	✓	✓	✓
Generating the last update operation report	✓	✓	✗
Firmware update of multiple servers against a single baseline	✓	✓	✓
Generate the last analysis operation report	✓	✓	✗
Firmware update with power off after update	✓	✓	✓
Firmware update of the localhost server	✓	✓	✓

SUM 12.x and 20.x CLI compatibility and REST API workflow mapping

Smart Update Manager (SUM) 20.x maintains compatibility with key CLI commands from SUM 12.x. The following table maps commonly used operations to the corresponding SUM CLI commands and SUM 20.x REST APIs. The high-level flow summarizes how each CLI operation maps the API workflow.

- For more information on CLI, see Smart Update Manager CLI.

> **TIP**
>
> There are no command changes to the operations listed in this table. The same CLI syntax is supported in both SUM 12.x and SUM 20.x versions.

- For REST API implementation details, see **SUM API reference Guide**.

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow
Firmware update of Single Server	`smartupdate --s --target <ip_address> --user <userid> --passwd <password> --use_location <baseline_directory_path>`	`POST /compute-ops-mgmt/v1/auth/login`	Authenticate to SUM and get access token
		`GET /compute-ops-mgmt/v1/servers`	Check whether the target server is already registered
		`POST /compute-ops-mgmt/v1/jobs`	Discover target server if it is not already registered
		`POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard`	Register/onboard the target server using iLO credentials
		`GET /compute-ops-mgmt/v1/firmware-bundles`	Check whether the firmware baseline already exists
		`POST /compute-ops-mgmt/v1/firmware-bundles`	Import/upload firmware baseline from --use_location
		`POST /compute-ops-mgmt/v1/analyze-firmware-update`	Run firmware analysis and dependency check

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow
		`POST /compute-ops-mgmt/v1/jobs`	Start firmware update job
		`GET /compute-ops-mgmt/v1/jobs/{jobId}`	Monitor discovery, onboard, baseline import, analysis, and update jobs
		`GET /compute-ops-mgmt/v1/servers/{serverId}?include-all-data=true`	Read final firmware analysis/update result
Firmware update of Single Server with ability to specify Reboot option	`smartupdate --s --target <ip_address> --user <userid> --passwd <password> --use_location <baseline_directory_path> --reboot`	Same API path as Firmware update of Single Server	The --reboot option is handled through the firmware update job payload sent to POST /compute-ops-mgmt/v1/jobs, using template fd54a96c-cabc-42e3-aee3-374a2d009dba with jobParams.manual_reboot_required: false.
Firmware update of Single Server with dry run	`smartupdate --s --target <ip_address> --user <userid> --passwd <password> --use_location <baseline_directory_pa`	`POST /compute-ops-mgmt/v1/auth/login`	Authenticate to SUM and get access token
		`GET /compute-ops-mgmt/v1/servers`	Check whether the target server is already registered
		`POST /compute-ops-mgmt/v1/jobs`	Discover target server if it is not already registered
		`POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard`	Register/onboard the target server using iLO credentials
		`GET /compute-ops-mgmt/v1/firmware-bundles`	Check whether the firmware baseline already exists

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow
	th> --dryrun	POST /compute-ops-mgmt/v1/firmware-bundles	Import/upload firmware baseline from --use_location
		POST /compute-ops-mgmt/v1/analyze-firmware-update	Run dry-run firmware analysis. No firmware update is applied
		GET /compute-ops-mgmt/v1/jobs/{jobId}	Monitor discovery, onboard, baseline import and dry-run analysis jobs
		GET /compute-ops-mgmt/v1/servers/{serverId}?include-all-data=true	Read dry-run analysis result
Firmware update of multiple Server's against a single baseline	smartupdate --s --target <ip_address_1> --user <userid_1> --passwd <password_1> --target <ip_address_2> --user <userid_2> --passwd <password_2> --use_location <baseline_directory_path>	POST /compute-ops-mgmt/v1/auth/login	Authenticate to SUM and get access token
		GET /compute-ops-mgmt/v1/firmware-bundles	Check whether the single firmware baseline already exists
		POST /compute-ops-mgmt/v1/firmware-bundles	Import/upload the single baseline from --use_location, if not already present
		GET /compute-ops-mgmt/v1/jobs/{jobId}	Monitor baseline import job
		GET /compute-ops-mgmt/v1/servers	Check whether each target server is already registered
		POST /compute-ops-mgmt/v1/jobs	Discover each target server if not already registered
		POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard	Register/onboard each target server using its credentials
		GET /compute-ops-mgmt/v1/jobs/{jobId}	Monitor discovery and onboard jobs for each server
		POST /compute-ops-mgmt/v1/analyze-firmware-update	Run firmware analysis/dependency check for each server against the same baseline
		POST /compute-ops-mgmt/v1/jobs	
		GET /compute-ops-mgmt/v1/jobs/{jobId}	

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow
		`GET /compute-ops-mgmt/v1/servers/{serverId}?include-all-data=true`	Start firmware update job for each server using the same bundle_id Monitor each firmware update job Read final firmware update result for each server

Generate a deploy preview report	`smartupdate --s --target <ip_address> --user <userid> --passwd <password> --use_location <baseline_directory_path> --report --reportdir <report_directory_path>`	`POST /compute-ops-mgmt/v1/auth/login`
		`GET /compute-ops-mgmt/v1/servers`
		`POST /compute-ops-mgmt/v1/jobs`
		`POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard`
		`GET /compute-ops-mgmt/v1/firmware-bundles`
		`POST /compute-ops-mgmt/v1/firmware-bundles`
		`POST /compute-ops-mgmt/v1/analyze-firmware-update`
		`GET /compute-ops-mgmt/v1/jobs/{jobId}`
		`GET /compute-ops-mgmt/v1/servers/{serverId}?include-all-data=true`
			Authenticate to SUM and get access token
			Check whether the target server is already registered
			Discover target server if it is not already registered
			Register/onboard the target server using iLO credentials
			Check whether the firmware baseline already exists
			Import/upload firmware baseline from --use_location
			Generate deploy preview analysis. No firmware update is applied
			Monitor discovery, onboard, baseline import, and deploy-preview analysis jobs
			Read deploy preview data from lastAnalysisOperation

Generate installed updates report	`smartupdate --s --target <ip_address> --user`	`POST /compute-ops-mgmt/v1/auth/login`
		`GET /compute-ops-mgmt/v1/servers`
		`POST /compute-ops-mgmt/v1/jobs`
			Authenticate to CFM and get access token
			Check whether the target server is already registered

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow

	`<userid> --passwd <password> -- use_location <baseline_directory_path> -- installed_report -- reportdir <report_directory_path>`	`POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard`
		`GET /compute-ops-mgmt/v1/firmware-bundles`
		`POST /compute-ops-mgmt/v1/firmware-bundles`
		`POST /compute-ops-mgmt/v1/analyze-firmware-update`
		`POST /compute-ops-mgmt/v1/jobs`
		`GET /compute-ops-mgmt/v1/jobs/{jobId}`
		GET /compute-ops-mgmt /v1/servers/{serverId}?include-all-data=true
			Discover target server if it is not already registered
			Register/onboard the target server using iLO credentials
			Check whether the firmware baseline already exists
			Import/upload firmware baseline from --use_location
			Run firmware analysis and dependency check before update
			Start firmware update job
			Monitor discovery, onboard, baseline import, analysis, and firmware update jobs
			Read installed update result from lastFirmwareUpdate

Firmware update of server with Power off the server after an update	`smartupdate --s --target <ip_address> --user <userid> --passwd <password> -- use_location <baseline_directory_path> --`	Same APIs as Firmware update of Single Server	The only difference is in the firmware update job payload sent to POST /compute-ops-mgmt/v1/jobs, where jobParams.power_off is set to true.

Functionality	SUM 12.x and 20.x CLI command	SUM 20.x API	High level flow
	`power_off --reboot` **NOTE** Not applicable for SUM 12.x.		

Firmware update of localhost server	`smartupdate --s --target localhost --user <userid> --passwd <password> --use_location <baseline_directory_path>`	`POST /compute-ops-mgmt/v1/auth/login`
		
		`GET /compute-ops-mgmt/v1/servers`
		
		`POST /compute-ops-mgmt/v1/discovered-servers/actions/onboard`
		
		`GET /compute-ops-mgmt/v1/firmware-bundles`
		
		`POST /compute-ops-mgmt/v1/firmware-bundles`
		
		`POST /compute-ops-mgmt/v1/analyze-firmware-update`
		
		`POST /compute-ops-mgmt/v1/jobs`
		
		`GET /compute-ops-mgmt/v1/jobs/{jobId}`
		
		`GET /compute-ops-mgmt/v1/servers/{serverId}?include-all-data=true`
			Authenticate to SUM and get access token
			
			Check whether localhost is already registered
			
			Register/onboard localhost if credentials are required
			
			Check whether the firmware baseline already exists
			
			Import/upload firmware baseline from --use_location
			
			Run firmware analysis and dependency check for localhost
			
			Start firmware update job for localhost
			
			Monitor onboarding, baseline import, analysis, and firmware update jobs
			
			Read final firmware update result for localhost

Getting started with Smart Update Manager

This section describes how to get started with the solution. It explains the prerequisites for deploying and using the application, and provides instructions for obtaining and downloading the software from the supported distribution sources.

Subtopics

Prerequisites for deploying and using SUM
Getting SUM from the SPP
Downloading SUM from HPE website

Prerequisites for deploying and using SUM

System requirements

- Minimum 2 virtual CPUs (vCPUs) or 2 physical CPU cores. For production deployments and environments with concurrent operations, 4 vCPUs or 4 physical CPU cores are recommended.
- Minimum 8 GB RAM is recommended normal operations and for firmware bundle uploads, custom baseline or custom SPP creation, report generation, and multiple simultaneous firmware updates.
- The local OS user account has administrative or root privileges on the SUM host.

Disk space requirements

- **Installation and runtime requirements**

Requirement	Minimum free space
Installation, configuration data, database, logs, and runtime operations	10 GB

Supported storage volumes include D:, E:, or F: depending on your system configuration.

- **Firmware depot volume requirements**

Allocate additional free space on the firmware depot volume for firmware bundle uploads and processing.

Firmware bundle size	Required free space
5 GB SPP ISO or ZIP	Approximately 14.5 GB
10 GB SPP ISO or ZIP	Approximately 27 GB

Calculation: Required free space = (2.5 × SPP size) + 2 GB

- **Concurrent firmware baseline uploads**

Requirement	Required free space
Multiple firmware baselines uploaded co ncurrently	Required free space = 2 × ((2.5 × largest S PP size) + 2 GB)

- **Custom baseline and custom SPP creation requirements**

  Additional depot volume capacity is required to accommodate:

  - Base SPP baseline
  - Extracted baseline content
  - Uploaded component packages
  - Custom SPP build staging files
  - Generated ISO or ZIP artifacts
  - Log files
  - Temporary processing files

NOTE

For systems that use custom baseline creation or custom SPP creation, Hewlett Packard Enterprise recommends a minimum of 50 GB of free space on the depot volume.

Network requirements

- Ensure that TCP port 63002 is available on the SUM host for HTTPS access to the SUM web UI, REST APIs, and local CLI communication.
- Allow inbound TCP port 63002 to the SUM host for remote browser and API access.
- Ensure that TCP port 443 is available between the SUM host and target HPE iLO addresses for Redfish communication, inventory collection, server onboarding, and firmware update operations.

Internal service ports

SUM uses the following ports for local inter-service communication. These ports must remain available on the SUM host and should not be exposed externally unless directed by HPE Support.

Port	Service	Purpose
TCP 63003	Custom Baseline Service	Manages component package operations and custom SPP creation.
TCP 63005	Baseline Manager Service	Handles firmware baseline uploads, processing, registration, and deletion.
TCP 5030	DSE Service	Performs install set calculations, compliance checks, custom baseline filtering, and dependency resolution.

Supported OS

- Red Hat Enterprise Linux 9 or later
- SUSE Linux Enterprise Server 15 or later
- Windows Server 2019 or later

Supported platforms

- HPE ProLiant Gen10, Gen10 Plus, Gen11, and Gen12 servers

Supported browsers

- **Windows:** Google Chrome, Mozilla Firefox, and Microsoft Edge
- **Linux:** Google Chrome and Mozilla Firefox

Getting SUM from the SPP

Prerequisites

- Valid user credentials for accessing the website.

About this task

You can get Smart Update Manager (SUM) from the Service pack for HPE ProLiant (SPP).

Procedure

1. Open a web browser.
2. Navigate to the SPP download page: **https://spp.hpe.com/**
3. If prompted, click **Sign in here**.
4. Enter your HPE user credentials and sign in.
5. Click **Download Software** and save the file to the desired location.
6. Depending on your OS, follow the instructions in Launching SUM from SPP for Windows or Launching SUM from SPP for Linux.

Downloading SUM from HPE website

Procedure

1. Launch a web browser.
2. Go to the Hewlett Packard Enterprise website: **https://support.hpe.com/connect/s/product?language=en_US&sp4ts.oid=1008862656&kmpmoid=5182020&actTab=all&tab=driversAndSoftware&driversAndSoftwareFilter=8000114**.
3. Select the required package:
   - **Smart Update Manager**
   - **Smart Update Manager for Linux**
4. Download the selected package and save it to the desired location.

Installing and using Smart Update Manager

This chapter describes how to install and launch Smart Update Manager (SUM) on the supported OS.

Subtopics

Installing standalone SUM on Windows
Installing standalone SUM on Linux
Launching SUM from SPP for Windows
Launching SUM from SPP for Linux
Logging in to SUM
Handling browser security certificates
Switching between legacy SUM and next-generation SUM from SPP
Starting, stopping, and verifying the SUM service

Installing standalone SUM on Windows

Prerequisites

- Ensure that you have met the OS, network port, and system requirements described in Prerequisites for deploying and using SUM.

About this task

Follow this procedure to install Smart Update Manager (SUM) on a Windows system using the MSI installer. The installation configures the solution as a managed service and allows access through a web browser.

Procedure

1. Download the SUM MSI installer.
2. Double-click the `.msi` file to start the installation wizard.
3. Review and accept the EULA.
4. Specify the installation path or accept the default location.
5. Click **Install**.
6. Complete the installation and optionally enable auto-launch.

7. Access the SUM UI using `https://localhost:63002`.

> **TIP**
>
> For more information about importing certificates into a web browser, see Handling browser security certificate.

Results

The application is installed and runs as a background service.

More information

Logging in to SUM
Launching SUM from SPP for Windows
Switching between legacy SUM and next-generation SUM from SPP
Starting, stopping, and verifying the SUM service
Installing standalone SUM on Linux
Downloading SUM from HPE website

Installing standalone SUM on Linux

Prerequisites

- Ensure that you have met the OS, network port, and system requirements described in Prerequisites for deploying and using SUM.

About this task

Follow this procedure to install Smart Update Manager (SUM) on a Linux system using an RPM package. The installation configures the solution as a managed service and allows access through a web browser.

Procedure

1. Download the SUM RPM package.
2. Copy the RPM package to the target Linux system.
3. Install the RPM package using the system package manager:

`sudo rpm -ivh <sum-package-name>.rpm`

> **TIP**
>
> To upgrade, use: `sudo rpm -Uvh <sum-package-name>.rpm`

4. Verify that the installation directory exists:

   `/opt/sum/`

5. Verify the service status.

   `sudo systemctl status sum`

6. Access the SUM UI:

   `https://localhost:63002`

> **TIP**
>
> For more information about importing certificates into a web browser, see Handling browser security certificate.

Results

The application is installed and runs as a `systemd` service.

More information

Logging in to SUM
Switching between legacy SUM and next-generation SUM from SPP
Starting, stopping, and verifying the SUM service
Launching SUM from SPP for Linux
Importing the security certificate into Mozilla Firefox
Importing the security certificate into Google Chrome
Importing the security certificate into Microsoft Edge
Downloading SUM from HPE website

Launching SUM from SPP for Windows

Prerequisites

- You have access to the Service pack for HPE ProLiant (SPP) ISO image or ZIP file.

- The SPP ISO image or ZIP file is mounted on the system.

About this task

Follow this procedure to launch the solution from the SPP ISO image.

Procedure

1. Mount the SPP ISO image or ZIP file on your system.
2. Open the mounted drive. For example, D:, E:, or F: depending on your system configuration.
3. Locate and double-click launch_sum.bat to start the launcher.

   The launcher provides the following options:

   - **Option 1** launches the legacy Smart Update Manager.
   - **Option 2** launches Smart Update Manager next Generation.
4. At the launcher prompt, use the **Up Arrow** or **Down Arrow** keys to select an option, or enter **1** or **2**, and then press **Enter** to confirm your selection. The default selection is **Option 1**, which is launched automatically after 6 seconds if no option is selected.
5. Select **2) Smart Update Manager - Install/Upgrade** by using the Up and Down Arrow keys or by entering **2**.
6. Do one of the following:

   - If SUM is not installed, wait for the installation to complete.
   - If SUM is already installed, follow the prompts to upgrade the existing installation.

Results

The SUM web interface opens in the default browser. SUM automatically registers the mounted SPP as a firmware baseline.

More information

Importing the security certificate into Mozilla Firefox
Importing the security certificate into Google Chrome
Importing the security certificate into Microsoft Edge
Getting SUM from the SPP

Launching SUM from SPP for Linux

Prerequisites

- You have permission to run shell scripts.
- You have access to the Service pack for HPE ProLiant (SPP) ISO image or ZIP file.
- The SPP ISO image or ZIP file is mounted on the Linux system.

About this task

Follow this procedure to launch the solution from the SPP ISO image.

Procedure

1. Mount the SPP ISO image or ZIP file on your system.
2. Navigate to the mounted directory containing the SPP files.
3. Change to the directory where the launch_sum.sh script is located.
4. Run the script `./launch_sum.sh`.

   The launcher provides the following options:

   - **Option 1** launches the legacy Smart Update Manager.
   - **Option 2** launches Smart Update Manager next Generation.
5. At the launcher prompt, use the **Up Arrow** or **Down Arrow** keys to select an option, or enter **1** or **2**, and then press **Enter** to confirm your selection. The default selection is **Option 1**, which is launched automatically after 6 seconds if no option is selected.
6. Select **2) Smart Update Manager - Install/Upgrade** by using the Up and Down Arrow keys or by entering **2**.
7. Do one of the following:

   - If SUM is not installed, wait for the installation to complete.
   - If SUM is already installed, follow the prompts to upgrade the existing installation.
8. Optional. Manually open a supported browser and navigate to the SUM interface, if your current shell environment does not support opening the GUI or web browser automatically.

Results

The SUM web interface opens in the default browser. SUM automatically registers the mounted SPP as a firmware baseline.

More information

Importing the security certificate into Mozilla Firefox
Importing the security certificate into Google Chrome
Importing the security certificate into Microsoft Edge
Getting SUM from the SPP

Logging in to SUM

About this task

Follow this procedure to sign in to the application using a valid OS user account on the host machine.

> **NOTE**
> Access to the Smart Update Manager (SUM) instance is controlled through OS authentication.

Procedure

1. Open a supported web browser.
2. Navigate to https://localhost:63002.
3. Enter the OS **`Username`** and **`Password`** for the SUM host.

   For a Windows domain account, specify the username in one of the following formats:

   - `domain_name\user_name`
   - `user_name@example.com`

   If you enter only **`user_name`**, SUM interprets the account as a local OS account, which might result in an invalid credentials message.
4. Click **Sign In**. SUM establishes a secure session and displays the dashboard.

More information

Adding servers through remote iLO
Removing servers
Adding firmware baseline
Removing firmware baselines

Updating firmware remotely using iLO
Installing standalone SUM on Windows
Installing standalone SUM on Linux
Importing the security certificate into Mozilla Firefox
Importing the security certificate into Google Chrome
Importing the security certificate into Microsoft Edge

Handling browser security certificates

When you launch Smart Update Manager (SUM) in UI mode, the browser might display a security warning indicating that `https://localhost:63002` presents a potential security risk. The message varies by web browser.

This warning occurs because the browser does not automatically trust the security certificate used by SUM. Once the certificate is trusted, the warning is no longer displayed when accessing the web interface.

To continue, do one of the following:

- Continue to the web interface despite the security warning.
- Import and trust the Hewlett Packard Enterprise security certificate in the web browser.

Subtopics

Importing the security certificate into Mozilla Firefox
Importing the security certificate into Google Chrome
Importing the security certificate into Microsoft Edge

Importing the security certificate into Mozilla Firefox

Procedure

1. Open **Settings**.
2. Select **Advanced > Certificates > View Certificates**.

3. Select **Import**, and navigate to the Smart Update Manager (SUM) data directory.

> **TIP**
> Default data directory locations:
> - **Linux:** /opt/sum/data/
> - **Windows:** C:\Program Files\SUM\data\

4. Select the ca.crt file.
5. Select **Trust CA to identify websites**.
6. Clear the browser cache and close the browser.
7. Launch the browser.

More information

Launching SUM from SPP for Windows
Launching SUM from SPP for Linux
Logging in to SUM

Importing the security certificate into Google Chrome

Procedure

1. Open **Settings**.
2. Select **Privacy and security**.
3. Select **Security**, and then scroll down to **Manage certificates**.
4. Select **Import**, and navigate to the Smart Update Manager (SUM) data directory.

> **TIP**
> Default data directory locations:
> - **Linux:** /opt/sum/data/
> - **Windows:** C:\Program Files\SUM\data\

5. Select the ca.crt file and place the certificate in the **Trusted Root Certification Authorities** store.
6. Clear the browser cache and close the browser.
7. Launch the browser.

More information

Launching SUM from SPP for Windows
Launching SUM from SPP for Linux
Logging in to SUM

Importing the security certificate into Microsoft Edge

Procedure

1. Open **Settings**.
2. Select **Privacy, Search, and Services**, and then scroll down to **Security**.
3. Select **Manage certificates**.
4. Select **Import**, and navigate to the Smart Update Manager (SUM) data directory.

> **TIP**
> Default data directory locations:
> - **Linux:** /opt/sum/data/
> - **Windows:** C:\Program Files\SUM\data\

5. Select the ca.crt file and place the certificate in the **Trusted Root Certification Authorities** store.
6. Clear the browser cache and close the browser.
7. Launch the browser.

More information

Launching SUM from SPP for Windows
Launching SUM from SPP for Linux

Switching between legacy SUM and next-generation SUM from SPP

About this task

Use this procedure to switch between legacy SUM (12.x) and next-generation SUM (20.x) from the mounted SPP. Use the launch_sum.sh for Linux or launch_sum.bat for Windows script to switch between SUM and next-generation SUM.

> **IMPORTANT**
>
> Legacy SUM and next-generation SUM maintain separate application data repository, including server inventories and firmware baseline repositories. Servers and firmware baselines added, created, or imported in one application are not available in the other.
>
> Switching between these two applications does not migrate, synchronize, or share configuration data. Any changes made in one application are not reflected in the other.

Procedure

1. Run one of the following scripts from the mounted Service pack for HPE ProLiant (SPP):
   - **For Linux:** `launch_sum.sh`
   - **For Windows:** `launch_sum.bat`
2. Select the required options:
   - **Option 1 - SUM**: To launch to legacy SUM.

     > **TIP**
     >
     > The option is available for Gen10, Gen10 Plus, Gen11, and Gen12 servers.

   - **Option 2 - SUM**: To launch to next-generation SUM.
3. Use **Up Arrow** or **Down Arrow**, or enter **1** or **2**, and then press **Enter** to confirm the selection.

4. Verify that the currently running SUM service stops automatically.
    - If next-generation SUM is running, the next-generation SUM service stops before SUM starts.
    - If SUM is running, the SUM service stops before next-generation SUM starts.
5. Optional. If the service does not stop automatically, manually stop the service.
    - For next-generation SUM, follow this procedure to stop the service.
    - For SUM, navigate to the directory from which SUM was launched, and use the command: `smartupdate shutdownengine`.
6. Verify that the selected SUM version starts successfully.

    TIP

    If the selected SUM is not installed, it is installed automatically before the service starts.

7. Verify that the default web browser opens the application UI at: **https://localhost:63002**.

Results

The selected SUM version starts and is ready to use.

Starting, stopping, and verifying the SUM service

Prerequisites

- You have administrator privileges on Windows.
- You have root or sudo privileges on Linux.

About this task

Use the Smart Update Manager (SUM) service control script to start, stop, restart, or verify the status of SUM and its dependent services. The script manages dependent services in the required sequence to ensure correct service operation.

Procedure

1. Open a command prompt or terminal on the SUM host.

2. Depending on the OS running on the SUM host, use the appropriate commands to manage the SUM service:

   For Windows:

   - Start SUM and dependent services: `sum-service-control.bat start`
   - Stop SUM and dependent services: `sum-service-control.bat stop`
   - Restart SUM and dependent services: `sum-service-control.bat restart`
   - Verify the status of SUM and dependent services: `sum-service-control.bat status`

   For Linux:

   - Start SUM and dependent services: `sudo /opt/sum/bin/sum-service-control.sh start`
   - Stop SUM and dependent services: `sudo /opt/sum/bin/sum-service-control.sh stop`
   - Restart SUM and dependent services: `sudo /opt/sum/bin/sum-service-control.sh restart`
   - Verify the status of SUM and dependent services: `sudo /opt/sum/bin/sum-service-control.sh status`

3. Optional. Display command help:

   For Windows:

   - `sum-service-control.bat --help`

   For Linux:

   - `sudo /opt/sum/bin/sum-service-control.sh --help`

   NOTE

   SUM starts automatically after installation. However, it does not start automatically following an OS reboot. After the system restarts, use the SUM service control script to manually start SUM and its dependent services.

Results

The script performs the requested action and manages dependent services automatically. When starting services, the script starts dependent services before starting SUM. When stopping services, the script stops SUM before stopping the dependent services.

Subtopics

Remote access to SUM
Opening the SUM firewall port for remote access

Remote access to SUM

Smart Update Manager (SUM) uses TCP port 63002 for the SUM web UI and REST APIs.

By default, SUM is accessible locally using: `https://localhost:63002`

If you need to access SUM from a remote system, the SUM port must be allowed for inbound connections through the operating system firewall.

Use the `--open-firewall` option with the SUM service-control script to open the configured SUM TCP port in the operating system firewall.

> **NOTE**
> You do not need to open the firewall port when SUM is accessed only from the localhost.

When to use the --open-firewall option

Use the `--open-firewall` option in the following situations:

- You can access SUM locally, but the SUM web UI or REST APIs cannot be accessed from a remote system.
- You want the SUM service-control script to open the required firewall port when starting SUM.
- You changed the SUM server port in the SUM configuration and need to allow the new port through the firewall.

Opening the SUM firewall port for remote access

Prerequisites

- You have administrative privileges on Windows or root/sudo privileges on Linux.

Procedure

1. Open a command prompt or terminal.

   Log in to the system where Smart Update Manager (SUM) is installed and open a command prompt or terminal with the required administrative privileges.

2. Start SUM and open the firewall port.

   Run the appropriate command for your OS.

   - **Windows**: `sum-service-control.bat start --open-firewall`
   - **Linux**: `sudo /opt/sum/bin/sum-service-control.sh start --open-firewall`

   The service-control script starts SUM and opens the configured SUM TCP port in the operating system firewall.

3. Open the firewall port for a running SUM service.

   If SUM is already running and you only need to open or verify the configured firewall port, run:

   - **Windows**: `sum-service-control.bat status --open-firewall`
   - **Linux**: `sudo /opt/sum/bin/sum-service-control.sh status --open-firewall`

   The service-control script opens the configured SUM TCP port, if required, and verifies the SUM service status.

4. Verify remote access.

   From a supported web browser on a remote system, enter: **https://%3CSUM-hostname-or-IP-address%3E:63002**.

   For example: **https://sumserver.example.com:63002** or **https://192.168.1.100:63002**

Results

If the firewall is configured correctly and SUM is running, the SUM web UI is accessible from the remote system.

Managing servers

Smart Update Manager (SUM) supports the following server management methods:

Remote servers through HPE iLO

Use this method to discover, onboard, and manage remote HPE servers by entering a single iLO IP address or a range of iLO IP addresses in the UI. SUM communicates with the target iLO over the network and uses the provided iLO credentials to onboard the server and perform firmware lifecycle operations.

Localhost server

Use this method for the server on which SUM is installed. When the SUM service starts, it automatically attempts to discover and onboard the localhost server by using in-band communication with the local iLO. If a supported local iLO is detected and the required in-band components are available, the localhost server is automatically added to **Servers** page. The server is then available for firmware lifecycle operations directly from the host system.

NOTE

Localhost operations use in-band communication through the local iLO and do not require a network connection to the local iLO.

Subtopics

Adding servers through remote iLO
Localhost server discovery and onboarding
Verifying localhost server added automatically
Adding localhost server by providing iLO credentials
Removing servers

Adding servers through remote iLO

Procedure

1. Access the **UI** using a web browser.
2. Select **Servers** on the left pane.
3. Click **Add server**.

4. On the **Add server** page, select one of the following **Range type** options:
    - **Single HPE iLO address**
    - **Range of HPE iLO addresses**
5. Enter the IP address or IP range, and then click **Add**.
6. Click **Next**.
7. Review the detected servers.

    TIP

    Servers managed by HPE Compute Ops Management and HPE OneView are excluded.

8. (Optional) Configure iLO credentials using one of the following methods:
    - Select **Use same credentials for all iLOs** to use the same login credentials for all the **iLO hostnames/IPv4 address**.
    - Select individual **iLO hostnames/IPv4 address** to configure credentials separately.
9. Click **Next**.
0. Review the servers to be onboarded.
1. Click **Finish and onboard servers**.
2. Click **Close**.

Results

The selected servers are added to the system. You can monitor the progress in the **Activity** page.

More information

Logging in to SUM
Removing servers

Localhost server discovery and onboarding

When the Smart Update Manager (SUM) service starts, it automatically attempts to discover and onboard the localhost server through in-band communication with the local iLO.

The localhost server discovery and onboarding behavior depends on the availability of a supported local iLO, the iLO security configuration, and whether the server is managed by an external management application.

Condition	Behavior
No supported local iLO detected	SUM does not create a localhost server entry.
Managed by HPE Compute Ops Management or HPE OneView	SUM does not create a localhost server entry.
Production (Standard) mode	SUM automatically onboards the localhost server.
High Security, **FIPS**, or **CNSA** mode	SUM creates the server entry but onboarding remains pending.

Requirements for automatic onboarding

Automatic onboarding of localhost server requires the following:

- A supported local iLO is available.
- Required in-band communication components, such as the Channel Interface (CHIF) drivers, are installed.
- No external management application is managing the localhost server.
- The iLO security configuration allows automatic onboarding.

After onboarding completes successfully, the localhost server appears on the **Servers** page with populated server details and is available for firmware lifecycle operations.

Verifying localhost server added automatically

Procedure

1. Start the SUM service.
2. Verify localhost server appears on the **Servers** page.

If SUM detects a supported local iLO operating in **Production (Standard)** security mode, it automatically onboards the localhost server and adds it to the **Servers** page.

3. Verify that the localhost server appears on the **Servers** page.

Results

The localhost server is automatically onboarded and available for firmware update operations.

Adding localhost server by providing iLO credentials

About this task

If the local iLO operates in **High Security**, **FIPS**, or **CNSA** mode, Smart Update Manager (SUM) cannot automatically complete localhost server onboarding. You must provide valid iLO administrator credentials to complete the onboarding process.

Procedure

1. Start the SUM service.
2. Verify that the localhost server appears on the **Servers** page with onboarding pending.
3. If the server is an HPE ProLiant Gen12 and later servers, verify that **CNSA** mode is not enabled.

> **NOTE**
>
> Firmware updates are not supported on HPE ProLiant Gen12 and later servers when CNSA mode is enabled. Change the security mode to **FIPS** or **Production (Standard)** before onboarding the server.

4. From the main menu, select **Servers**.
5. Select the **localhost** server.
6. Select the **Summary** tab, and then click **Enter iLO Credentials**
7. Enter the iLO credentials.
8. Click **Save and connect to iLO**.

9. Verify that the onboarding process completes successfully and that the server status is updated on the **Servers** page.

Results

The localhost server is onboarded successfully and is available for firmware update operations.

More information

Localhost server discovery and onboarding
Verifying localhost server added automatically
Removing servers

Removing servers

About this task

Use this procedure to remove servers that you no longer want Smart Update Manager (SUM) to manage.

Procedure

1. Access the **UI** using a web browser.
2. Select **Servers** on the left pane.
3. Select one or more servers to remove from the **Servers** list.
4. Select **Actions > Remove**.
5. Review the confirmation message.
6. Click **Remove** to confirm.

Results

The selected servers are removed from the system.

More information

Logging in to SUM
Adding servers through remote iLO

Managing firmware baselines

This chapter describes how to download, add, and remove firmware baselines.

Subtopics

Downloading Service pack for HPE ProLiant from HPE website
Adding firmware baseline
Removing firmware baselines
Adding component packages
Removing component packages

Downloading Service pack for HPE ProLiant from HPE website

Prerequisites

- Valid HPE user credentials

> **IMPORTANT**
>
> Access to the Service pack for HPE ProLiant (SPP) is subject to validation through the HPE Support Center. For more information, see the **Service pack for HPE ProLiant (SPP) server support policy**.

About this task

Use this procedure to access and download a Service pack for HPE ProLiant (SPP) or a custom SPP from HPE Support Center. You can create, download, and manage custom SPP from the SPP download page.

Procedure

1. Open a web browser.
2. Navigate to the SPP or custom SPP download page:

   https://spp.hpe.com/ or **https://spp.hpe.com/custom/**
3. If prompted, click **Sign in here**.
4. Enter your HPE user credentials and sign in.
5. Click **Download Software** and save the file to the desired location.

Adding firmware baseline

Prerequisites

- Valid firmware ISO or ZIP file is available on the local system.
- Sufficient system resources are available for upload and processing.
- Configure a firmware baseline prior to performing firmware updates. Uploading a firmware ISO or ZIP enables the system to store the ISO or ZIP, extract firmware metadata, and register the baseline for compliance verification and update operations.

About this task

Follow this procedure to add and configure a firmware baseline by uploading an SPP bundle in the UI. The baseline specifies the target firmware versions that will be used for compliance assessments and firmware updates.

Procedure

1. Access the **UI** using a web browser.
2. In the navigation pane, select **Firmware**.
3. Click **Add firmware baseline**.
4. In the **Add firmware baseline** window, do one of the following:
   - Select the firmware ISO or ZIP file from the local system.
   - Drag and drop the firmware ISO or ZIP file into the window.
5. Click **Continue**.

   The file upload starts.
6. Wait for the upload to reach 100%. You can view the status in the **Activity** window.
7. Click **Close**.

Results

The firmware baseline is added successfully.

More information

Logging in to SUM

Downloading firmware
Removing firmware baselines
Updating firmware remotely using iLO
Updating firmware using localhost

Removing firmware baselines

Prerequisites

- The firmware baseline to be removed is already added to the system.

About this task

Follow this procedure to remove one or more firmware baselines from the SUM appliance when they are no longer needed.

Procedure

1. Access the **UI** using a web browser.
2. Select **Firmware** on the left pane.
3. From the **Firmware** list, click **Remove** for the firmware baseline that you want to remove.
4. Review the confirmation message.
5. Click **Remove** to confirm.

Results

The selected firmware baselines are removed. You can monitor the status in the **Activity** window.

More information

Logging in to SUM
Adding firmware baseline
Downloading firmware
Updating firmware remotely using iLO
Updating firmware using localhost

Adding component packages

Prerequisites

- You have component package in your system.

About this task

Use this procedure to add one or more component packages to the firmware repository. When a component package is selected, its associated metadata and signature files are automatically mapped based on the file name. These component packages can then be included in SUM and later used to generate a custom baseline from an existing SUM firmware baseline.

Procedure

1. Access the **UI** using a web browser.
2. In the left navigation pane, select **Firmware**.
3. Select **Actions > Add component package**.
4. In the **Add component package** window, do one of the following:
   - Select the directory from the local system that has the component package files.
   - Drag and drop the directory into the window that has the component package files.
5. Click **Continue**.

   The uploaded files are validated. If validation fails for one or more component packages, an error message is displayed and the affected file names are highlighted.
6. Select one or more component packages.

   The corresponding metadata and signature files are automatically mapped based on the file name.
7. In the confirmation window, verify that the component packages are added successfully and click **Close**.

Results

The component packages are added to the repository, and the **Component Packages** tab is displayed with the newly added components.

Removing component packages

About this task

Use this procedure to remove one or more component packages from the firmware repository.

Procedure

1. Access the **UI** using a web browser.
2. In the left navigation pane, select **Firmware**.
3. Click the **Component Packages** tab.
4. Locate the component package that you want to remove.
5. Click **Remove** for the component package.
6. In the **Remove component package** window, click **Remove**.

> **CAUTION**
>
> Removing a component package deletes it from the repository. Ensure that the component package is not required for future firmware operations before you remove it.

Results

The selected component package is removed from the firmware repository and will no longer appear on the **Component Packages** tab. You can monitor the removal status in the **Activity** window.

Managing custom baselines

Smart Update Manager (SUM) supports creation of custom baselines. Creating a custom baseline enables you to:

- Deploy specific updates from Service pack for HPE ProLiant (SPP) releases.
- Minimize the size of baselines or ISO images or ZIP files.
- Standardize the updates that you deploy in your environment.

A custom baseline is created from an HPE-provided firmware baseline that has already been added to the SUM appliance. Custom baselines cannot be created from an existing

custom baseline. Before creating a custom baseline, ensure that a valid HPE-provided baseline is available in the SUM appliance. For information about adding a firmware baseline, see Adding firmware baselines.

- Custom baseline creation requires additional disk space.
- Ensure that the disk space requirements described in Prerequisites for deploying and using SUM are met before creating custom baselines.

NOTE

- SUM creates custom baselines in ISO and ZIP formats that are available for download.
- SUM supports replacing HPE baseline components in a custom baseline. Before creating the custom baseline, add the required components. For information about adding components, see Adding component packages. You can then select those components during the custom baseline creation workflow.
- Install the xorriso application on Linux hosts to create a custom ISO.

Subtopics

Creating a custom firmware baseline
Downloading a custom firmware baseline

Creating a custom firmware baseline

Prerequisites

- A valid HPE-provided baseline is already added to the system.

About this task

Generate a custom firmware baseline from an existing HPE-provided baseline. Custom baselines allow you to customize firmware and component selections to match your environment. Follow this procedure to create a custom firmware baseline, choosing supported server models, OS, and component packages, and deciding whether to include or exclude specific firmware components.

Procedure

1. Access the **UI** using a web browser.
2. In the left navigation pane, select **Firmware**.
3. Select **Actions > Create custom baseline** or click **Create custom baseline**.
4. In the **Create custom baseline** page, specify the custom baseline information:
   a. Enter a name for the custom baseline.
   b. Optional. Enter a description.
   c. Select the **HPE firmware baseline** from which to create the custom baseline.
   d. Optional. View the baseline details to verify the applicable server generations.
   e. Click **Next**.
5. Select the server models to include in the custom baseline.
   a. Select one or more supported server models and click **Next**.
6. Optional. Select the OS to include in the custom baseline.
   a. Select one or more applicable OS and click **Next**.
7. Optional. Add component packages.
   a. Enable **Add components**.
   b. Select the component packages to include and click **Next**.

   NOTE

   Only previously uploaded component packages are available for selection.
8. Select the firmware components to include in the custom baseline.
   a. Review the list of components from the selected HPE baseline.
   b. Clear the components that you do not want to include and click **Next**.
9. Validate the selected components.
   a. Review any validation issues that are reported.
   b. Resolve the validation issues, if applicable.
   c. Click **Next** when validation completes successfully.

0. Review the custom baseline configuration.

    a. Verify the selected baseline settings and click **Next**.

1. Monitor the creation progress in the **Activity** window.
2. Close the confirmation window when the baseline creation process starts.

Results

The custom baseline is added to the firmware baseline inventory. The baseline type is displayed as **Customized**.

Downloading a custom firmware baseline

Prerequisites

- The custom baseline to be downloaded already exists in the system.

About this task

Use this procedure to download a previously created custom firmware baseline in ISO or ZIP format for offline use or deployment.

Procedure

1. Access the **UI** using a web browser.
2. In the left navigation pane, select **Firmware**.
3. Locate the custom baseline and click the **Download** icon.
4. Select the baseline generation and the download format.

    a. Select the required generation.

    b. Select either ISO or ZIP as the file format.

5. Click **Download**.
6. Wait for the download process to complete.
7. When the download confirmation window appears, close the window.

Results

The selected custom firmware baseline is downloaded to your browser's configured download location.

Updating firmware

You can update firmware by using either a remote or localhost workflow. The appropriate method depends on where the Smart Update Manager (SUM) is installed and how the target servers are managed.

Remote

The solution runs on a dedicated management system and updates managed servers through their iLO interfaces. This workflow is recommended for updating one or more servers from a centralized location. You launch SUM from the management server to perform the update.

Localhost

The solution runs on the target server and uses the online update workflow to perform firmware updates. The target server must have a supported OS installed and running. This workflow is recommended for updating a single server. You launch SUM from the target server to perform the update.

Subtopics

Prerequisites to update firmware
Updating firmware remotely using iLO
Updating firmware using localhost

Prerequisites to update firmware

Before performing firmware analysis, compliance checks, or firmware update operations, ensure that the target servers meet the following requirements.

Privileges

- You have administrative or root privileges.

Managed servers

- One or more servers are added to Smart Update Manager (SUM) and are reachable.
- The servers are onboarded successfully and available on the **Servers** page.
- A firmware baseline is available in SUM.

Firmware baselines

- Upload a supported Service pack for HPE ProLiant (SPP) before performing compliance analysis or firmware updates.
- When using a custom SPP, include all required firmware components and variants for the target environment.
- An SPP containing only Smart Component RPM packages is not supported.

AMS and iSUT requirements

If you plan to deploy OS drivers and software together with firmware updates, ensure:

- Agentless Management Service (AMS) is installed and running on the target server.
- Integrated Smart Update Tools (iSUT) is installed and running on the target server.
- The installed iSUT version is supported for the target server generation and OS.

Supported iSUT versions

- Gen12 servers with iLO 7: Version 6.0.0 or later
- Gen10, Gen10 Plus, Gen11, and Gen12 servers with iLO 6: Version 2.9.3 or later
- VMware ESXi servers: Version 4.1.0 or later

iSUT configuration requirements

- Enable iLO queued updates in iSUT.

  ```
  sut -set enableiloqueuedupdates=true
  ```

- Do not configure iSUT in **OnDemand** mode.
- If iSUT on a VMware ESXi server was upgraded from a version earlier than 2.9.3, run the following commands after the upgrade:

  ```
  sut -deregister
  sut -register
  sut -set mode=autodeploy
  ```

VMware ESXi requirements

For VMware ESXi servers:

- Verify that a supported iSUT version is installed.
- Place ESXi hosts in maintenance mode.

- If iSUT was upgraded from an earlier unsupported version, re-register iSUT according to iSUT documentation. For more information, see the Learn more link under **HPE drivers and software** in **Update Firmware Baseline**.

HPE ProLiant Gen12 servers and later

- Firmware updates are not supported when **CNSA** mode is enabled.
- Change the security mode to **FIPS** or **Production (Standard)** before performing firmware updates.
- Optional virtual NIC (vNIC) configuration:
  - Create iSUT application account using the command:

    ```
    sut appaccount create -u <ilo_username> -p <ilo_password>
    ```

  - Configure AMS communication over vNIC using the command:

    ```
    amscli appaccount create -u <ilo_username> -p <ilo_password>
    ```

Downgrade operations

If you enable **Downgrade Components to Match Baseline**, verify that the **iLO Downgrade Policy** is set to **Allow Downgrades**.

Operational readiness

- Ensure target servers are powered on when HPE Drivers and Software updates are required.
- Review workloads running on the target servers.
- Plan for maintenance windows and potential server restarts.

Updating firmware remotely using iLO

Prerequisites

- You have completed all the prerequisites.
- The remote servers are onboarded and available on the **Servers** page.

About this task

Use this procedure to update server firmware by applying a firmware baseline that is already available in the system.

Procedure

1. Access the **UI** using a web browser.
2. Select **Servers**.
3. Select the servers that you want to update.
4. Select **Actions > Update Firmware**.
5. If some selected servers are not eligible for a firmware update, review the affected servers in the **Update Firmware Baseline** dialog box, and then click **Continue** to proceed to update only the eligible servers.
6. Select a firmware baseline from the **Choose a SPP Bundle** list.
7. Optional. Configure **HPE Drivers and Software**:
   - **Enabled**: Updates firmware, drivers, and software. Servers must be powered on and meet the AMS and iSUT requirements. Servers that do not meet these requirements are automatically excluded.
   - **Disabled**: Updates firmware only.
8. Optional. Configure **Downgrade Components to Match Baseline**:
   - **Disabled (Default)**: Updates only components that are older than the selected baseline. Components with newer versions remain unchanged.
   - **Enabled**: Updates older components and downgrades newer components to match the selected baseline.
9. Select a reboot option:
   - **Automatic Reboot**
   - **Manual Reboot**

   NOTE

   If you select **Manual Reboot**, the **Power Off Server After Update** option is unavailable.
0. Optional. Enable **Power Off Server After Update** to automatically power off servers that are powered on when the firmware update completes.
1. Click **Next**.

The **Select Servers** page validates the selected servers against the update requirements. Servers that do not meet the requirements are automatically removed from the update.

2. Optional. Review the **Last Analysis Operation** report before starting the update.
   a. Select the required server.
   b. Click the **Firmware** tab.
   c. Review the **Last Analysis Operation** report.

      The report identifies the planned update actions and any conditions that must be resolved before proceeding with the firmware update.
3. On the **Review** page, verify your selections and click **Start the Update**.
4. Optional. Monitor the progress of the update on the **Activity** page.
5. Verify the firmware update.
   a. Select **Servers**.
   b. Select the required server.
   c. Click the **Firmware** tab.
   d. Review the last analysis operation report in the **Last analysis operation** section.

Results

The firmware baseline is applied to the eligible servers. The last analysis operation report shows the update results, component status, selected baseline, update options, and completion status. The analysis operation does not install firmware

More information

Logging in to SUM
Adding firmware baseline
Removing firmware baselines
Downloading firmware
Updating firmware using localhost

Updating firmware using localhost

Prerequisites

- You have completed all the prerequisites.
- The remote servers are onboarded and available on the **Servers** page.

About this task

Use this procedure to update firmware on the server where Smart Update Manager (SUM) is installed.

Procedure

1. Access the **UI** using a web browser
2. Select **Servers**.
3. Select the localhost server.
4. Select **Actions > Update Firmware**.
5. If the **Update Firmware Baseline** dialog box displays ineligible servers, review the details and click **Continue** to proceed with the eligible servers.
6. From the **Choose a Base SPP Bundle** list, select the firmware baseline to apply.
7. Optional. Configure **HPE Drivers and Software**:
   - **Enabled**: Updates firmware, drivers, and software. Eligible servers must be powered on and meet the AMS and iSUT requirements.
   - **Disabled**: Updates firmware only.
8. Optional. Configure **Downgrade Components to Match Baseline**:
   - **Disabled (Default)**: Updates only components that are older than the selected baseline. Components with newer versions remain unchanged.
   - **Enabled**: Updates older components and downgrades newer components to match the selected baseline.
9. Select the reboot behavior for components that require a restart:
   - **Automatic Reboot**

- **Manual Reboot**

> **NOTE**
>
> If you select **Manual Reboot**, the **Power Off Server After Update** option is unavailable.

0. Optional. Enable **Power Off Server After Update** to automatically power off servers that are powered on when the firmware update completes.
1. Click **Next**.

   The **Select Servers** page validates the selected servers against the update requirements. Servers that do not meet the requirements are automatically removed from the update.
2. Optional. Review the **Last Analysis Operation** report before starting the update.
   a. Select the required server.
   b. Click the **Firmware** tab.
   c. Review the **Last Analysis Operation** report.

      The report identifies the planned update actions and any conditions that must be resolved before proceeding with the firmware update.
3. On the **Review** page, verify your selections and click **Start Update**.
4. Optional. Monitor the progress of the update on the **Activity** page.
5. Verify that the localhost server is available after the firmware update completes.

> **TIP**
>
> If the firmware update includes components that require a restart, the localhost server restarts as part of the firmware update process and the SUM session ends. When the server becomes available, start the SUM service and log in to the SUM UI.

6. Verify the update.
   a. Select **Servers**.
   b. Select the required server.
   c. Click the **Firmware** tab.

d. Review the last analysis operation report in the **Last Update Operation** section.

Results

The selected firmware baseline is applied to the localhost server. The last analysis operation report shows the update actions and any conditions that must be resolved before the selected baseline can be applied. The analysis operation does not install firmware

More information

Launching SUM from SPP for Windows
Launching SUM from SPP for Linux
Logging in to SUM

Smart Update Manager CLI

The Smart Update Manager (SUM) provided through the `smartupdate` executable installed with the SUM service, supports scripting and automation of firmware update operations while maintaining backward compatibility with key CLI commands.

NOTE

The `smartupdate` CLI must run on the same host as the SUM service. Running the CLI from a remote host is not supported.

Command syntax

```
smartupdate [--silent] --target <iLO-IP> --user <username> --passwd
<password>
            --use_location <path-to-SPP-ISO>
            [options]
```

Command options

Target options

Flag	Description
`--target <ip>`	Repeat the option for each target server. O R Specify this option multiple times to upd ate multiple servers.
`--user <user>`, `--username <user>`	iLO username

Flag	Description
`--passwd <pwd>`, `--password <pwd>`	iLO password

NOTE

- For localhost updates, set the `--target` value to `localhost` .
- If the security state of the local iLO is **Production (Standard)**, iLO credentials are not required.
- If the security state of the local iLO is **High Security**, **FIPS**, or **CNSA** mode, provide iLO credentials.

Firmware baseline options

Flag	Description
`--use_location <path>, -u <path>`	Path to the SPP ISO or ZIP file on the SUM host. If the ISO or ZIP has already been uploaded, SUM reuses the existing bundle automatically

Installation control options

Flag	Description
`--downgrade, -g`	Downgrade components with versions that are higher than the baseline version.
`--install_sw_drivers`	Include software and driver components in addition to firmware during the update
`--power_off`	Powers off the server after the firmware update completes (Default: False; server remains powered on). `--reboot` option must be specified for power off
`--reboot, -r`	Automatically reboot the server if required to complete the update (Default: False; reboot is left to the user)
`--dryrun`	Analyze firmware compliance without applying any changes. Prints the analysis result and exits

Flag	Description
`--continue_on_error`	When updating multiple targets, continue i f at least one target succeeds. Exit code re flects the successful targets
`--on_failed_dependency <val>`	Attempt the firmware updates even with d ependency failures. Only force val is suppo rted

Reporting

Flag	Description
`--report`	Generate a deploy preview report (JSON/X ML); exits without deploying updates
`--installed_report`	Generate a report (JSON/XML) of compone nts installed this session
`--reportdir <path>`	Directory to save report/installed_report fil es

Logging options

Flag	Description
`--verbose , -v`	Enable verbose logging
`--silent , -s`	Silent mode (Mandatory parameter)

Input file options

Flag	Description
`--inputfile <path>`	Path to a SUM-format input file containing f lags and target definitions (see Input file fo rmat)
`--deleteinputfile`	Delete the input file after processing

Exit codes

The following table lists the exit codes returned by the `smartupdate` CLI.

Description Exit status
Success - all firmware updates applied; no reboot required 0
Success - updates applied; a reboot is required to activate one or more components 1
Not required - all firmware components are already at the target version; no changes made 3
General failure - authentication error, server unreachable, or other fatal condition 255
Bad parameter - a required flag is missing or invalid 254
Component failed - one or more firmware component installations failed on the target 253
Command failed - job submission, polling timeout, or job canceled 252

NOTE
The exit codes are the same for both SUM 12.x and SUM 20.x.

Command examples

Update firmware on a single server

```
smartupdate -s \
  --target 192.168.1.100 \
```

```
  --user Administrator --passwd Yourpassword \
  --use_location /var/baselines/SPP2026.iso
```

Update firmware on localhost

```
smartupdate -s \
--target localhost --use_location
/var/baselines/SPP2026.iso
```

Dry run — analyze compliance without applying changes

```
smartupdate -s \
  --target 192.168.1.100 \
  --user Administrator --passwd Yourpassword \
  --use_location /var/baselines/SPP2026.iso \
  --dryrun
```

Update multiple servers in parallel

```
smartupdate -s \
  --target 192.168.1.100 --user Administrator --passwd Yourpassword \
  --target 192.168.1.101 --user Administrator --passwd Yourpassword1 \
  --use_location /var/baselines/SPP2026.iso
```

All targets are processed simultaneously. When `--continue_on_error` is specified, a failure on one target does not stop the others.

Downgrade the components to match the baseline

```
smartupdate -s \
  --target 192.168.1.100 \
  --user Administrator --passwd Yourpassword \
  --use_location /var/baselines/SPP2026.iso \
  --downgrade
```

Power off server after update; requires --reboot

```
smartupdate -s \
  --target 192.168.1.100 \
  --user admin --passwd Yourpassword \
--use_location /mnt/spp.iso \
--reboot --power_off
```

Verbose output

```
smartupdate -s \
  --target 192.168.1.100 \
  --user Administrator --passwd Yourpassword \
  --use_location /var/baselines/SPP2026.iso \
  --verbose
```

Deploy preview report

```
smartupdate --silent \
--target 192.168.1.100 \
--user admin --passwd Yourpassword \
--use_location /mnt/spp.iso \
--report --reportdir /etc/user/reports
```

Installed report

```
smartupdate --silent \
--target 192.168.1.100 \
--user admin --passwd Yourpassword \
--use_location /mnt/spp.iso \
--installed_report \
--reportdir /etc/user/reports
```

On failed dependency

```
smartupdate --silent \
--target 192.168.1.100 \
--user admin --passwd Yourpassword \
--use_location /mnt/spp.iso \
--on_failed_dependency force
```

Input file format

You can supply all flags in a text file instead of on the command line. This approach is useful for scheduled jobs or when managing many targets.

```
SILENT = YES
USE_LOCATION = /var/baselines/SPP2026.iso
CONTINUE_ON_ERROR=YES

[TARGETS]
HOST = 192.168.1.100
UID  = Administrator
PWD  = Admin123
[END]

[TARGETS]
HOST = 192.168.1.101
HOST = 192.168.1.102
UID  = Administrator
PWD  = Admin456
[END]
```

Input file rules

- Global lines (`KEY = VALUE`) set flags for the whole run. CLI flags take precedence over values in the file.
- Each `[TARGETS]...[END]` block defines one set of credentials.
- Multiple `HOST =` lines inside a block share the same username and password.
- Supported global keys: `USE_LOCATION`, `DOWNGRADE`, `DRYRUN`, `VERBOSE`, `INSTALL_SW_DRIVERS`, `POWER_OFF`, `CONTINUE_ON_ERROR`, `REBOOT`, `REPORT`, `INSTALLED_REPORT`, `REPORTDIR` and `ON_FAILED_DEPENDENCY`.

Run with an input file

```
smartupdate --inputfile /var/scripts/update.txt
```

Delete the input file after processing

```
smartupdate --inputfile /var/scripts/update.txt --deleteinputfile
```

Subtopics

About SUM user.yaml configuration file

About SUM user.yaml configuration file

SUM () stores user-configurable settings in the `user.yaml` file. This file controls settings such as the SUM service port, firmware depot location, log storage locations, and diagnostic parameters.

Use the `user.yaml` file to customize SUM behavior for your environment. Most users need to modify only a small number of settings, such as storage locations and network ports.

Changes to the `user.yaml` file take effect only after the SUM service is restarted.

NOTE

- Modify only the settings documented in the `user.yaml` file.
- Do not modify `system.yaml` . SUM manages this file and may overwrite it during installation or upgrade operations.
- Change iLO communication, timeout, and retry settings only when directed by HPE Support.

Subtopics

Modify SUM user.yaml settings
SUM user.yaml configuration parameters

Modify SUM user.yaml settings

Procedure

1. Stop the SUM service.

- Linux: `sudo /opt/sum/bin/sum-service-control.sh` stop
- Windows: `C:\Program Files\SUM\bin\sum-service-control.bat` stop

2. Open the `user.yaml` configuration file.
3. Update the required parameter values.
4. Save the file.
5. Start the SUM service.
   - Linux: `sudo /opt/sum/bin/sum-service-control.sh` start
   - Windows: `C:\Program Files\SUM\bin\sum-service-control.bat` start
6. Verify that the SUM service is running.
   - Linux: `sudo /opt/sum/bin/sum-service-control.sh` status
   - Windows: `C:\Program Files\SUM\bin\sum-service-control.bat` status

Results

SUM applies the updated configuration settings after the service restarts.

SUM user.yaml configuration parameters

Server settings

Parameter	Default value	Description	When to change
server.host	0.0.0.0	Network address that SUM binds to. `0.0.0.0` allows SUM to listen on all network interfaces.	Change only if SUM must listen on a specific interface, such as `127.0.0.1` for local-only access.
server.port	63002	TCP port used for HTTPS access to the SUM web UI, REST API, and local CLI communication.	Change if port `63002` is already in use or your environment requires another port. Open the same port in the host firewall.

Firmware baseline settings

Parameter	Default value	Description	When to change
baseline.depot_path	Empty	Location where firm ware baselines, pac kages, and related d epot content are sto red. If empty, SUM u ses the operating sys tem default location.	Change if the defaul t depot volume does not have enough spa ce or if firmware con tent must be stored on a dedicated volu me.

Logging settings

Parameter	Default value	Description	When to change
logging.dir	Empty	Directory for SUM lo g files. If empty, SU M uses the operating system default log di rectory.	Change when logs must be stored in a specific location.
logging.level	info	Logging level. Supp orted values are `deb ug`, `info`, `warn`, a nd `error`.	Use `debug` only for troubleshooting. Use `info` or higher for n ormal operation.
logging.max_size_m b	100	Maximum size, in MB , of a single log file b efore rotation.	Increase for longer t roubleshooting wind ows; decrease to lim it disk usage
logging.max_backup s	5	Number of rotated lo g files to retain.	Adjust based on disk space and troublesh ooting retention nee ds.
logging.artifact_dir	Empty	Directory for operati on artifacts, such as per-server update a rtifacts. If empty, SU M uses the log direct ory.	Change if operation artifacts must be sto red separately from l ogs.

iLO communication settings

c

Parameter	Default value	Description	When to change
ilo.communication	cli	Default iLO communication backend	Change only when directed by HPE Support.
ilo.iLO5	cli	iLO 5 communication backend.	Change only when directed by HPE Support.
ilo.iLO6	cli	iLO 6 communication backend.	Change only when directed by HPE Support.
ilo.iLO7	cli	iLO 7 communication backend.	Change only when directed by HPE Support.
ilo.cli_version	`v2`	iLO CLI adapter version used by SUM	Change only when directed by HPE Support.

iLO timeout settings

Parameter	Default value	Description	When to change
ilo.timeouts.default_ms	600000	Default timeout, in milliseconds, for iLO operations.	Change only when directed by HPE Support, for example in slow networks.
ilo.timeouts.ilo_upload_timeout_ms	600000	Additional timeout, in milliseconds, for iLO upload operations.	Change only when directed by HPE Support.
ilo.timeouts.flash_fwpkg_ms	3600000	Timeout, in milliseconds, for firmware package flashing operations.	Change only when directed by HPE Support.

iLO retry settings

Parameter	Default value	Description	When to change
default_count	3	Default retry count for iLO operations.	Change only when directed by HPE Support.

Parameter	Default value	Description	When to change
ilo_unavailable_count	8	Retry count used when iLO is temporarily unavailable.	Change only when directed by HPE Support.
delay_ms	2000	Initial retry delay, in milliseconds. The delay may increase between retries.	Change only when directed by HPE Support.
update_service_max_delay_min	2	Maximum retry delay, in minutes, for update service operations.	Change only when directed by HPE Support.

IMPORTANT

Modify iLO communication, timeout, and retry settings only when directed by HPE Support.

Default file locations

Setting	Linux default location	Windows default location
Firmware depot	/var/lib/sum/depot	%PROGRAMDATA%\SUM\depot
Log files	/var/tmp/sum/20_0_0/logs	%PROGRAMDATA%\SUM\20_0_0\logs
Operation artifacts	Same location as logging.dir	Same location as logging.dir

Configuration examples

- **Change the SUM service port**

  The following example changes the default SUM service port from `63002` to `443`.

  ```
  server:
    host: "0.0.0.0"
    port: 443
  ```

  After changing the port:

  - Restart the SUM service.
  - Allow the configured port through the host firewall and network security policy.
  - Access SUM by using the configured port.

```
https://localhost:443
```

Changing the SUM service port does not affect communication with target iLO devices. SUM continues to use TCP port `443` to communicate with managed iLO interfaces.

- **Configure a custom firmware depot location**

  Windows:

  ```
  baseline:
    depot_path: "D:\\SUM\\depot"
  ```

  Linux:

  ```
  baseline:
    depot_path: "/data/sum/depot"
  ```

  Use a custom depot location when the default storage location does not have sufficient capacity or when firmware content must be stored on dedicated storage.

- **Configure custom log and artifact locations**

  Windows:

  ```
  logging:
    dir: "D:\\SUM\\logs"
    artifact_dir: "D:\\SUM\\artifacts"
  ```

  Linux:

  ```
  logging:
    dir: "/var/tmp/sum/logs"
    artifact_dir: "/var/tmp/sum/artifacts"
  ```

Use custom locations to separate logs and operation artifacts from the default storage location.

NOTE

- Modify only settings documented in the `user.yaml` file.
- Do not edit `system.yaml`. SUM manages this file and may overwrite it during installation or upgrade operations.
- Ensure that the SUM service account has read and write access to any custom directories.
- Back up the `user.yaml` file, SUM database, and firmware depot before changing storage locations.
- Ensure that sufficient free space is available in custom depot, log, and artifact locations.
- Use HPE Support guidance before modifying iLO communication, timeout, or retry settings.

Reports

This chapter describes how to view firmware analysis and update reports, review operation status and preconditions, and export report data for troubleshooting and support activities.

Subtopics

Viewing the last analysis operation report and reviewing analysis preconditions
Viewing the last update operation report

Viewing the last analysis operation report and reviewing analysis preconditions

About this task

The **Last analysis operation** report shows the results of the most recent firmware analysis performed on a server. The analysis compares the installed firmware with a selected baseline and identifies the changes and conditions that would apply if the baseline were updated. The analysis does not install firmware.

The **Analysis preconditions** section lists any conditions identified during the analysis. Review the reported conditions and recommended actions before submitting a firmware update

Procedure

1. Select **Servers**.
2. Select the checkbox of the required server.
3. Click the **Firmware** tab.
4. Under **Last analysis operation**, click **View the report** link.
5. Optional. Click Export to download.

   The report identifies what an update would do and the conditions that must be resolved before the selected baseline can be applied. The analysis does not install firmware.
6. Optional. Save the JSON file when prompted by the browser.
7. In the **Analysis preconditions** section, review the summary and recommendation for each reported condition.
8. Resolve any reported preconditions before submitting the firmware update operation.

Results

The **Last analysis operation** report displays the expected update actions and any conditions that must be resolved before the selected firmware baseline can be applied. The report provides analysis results only and does not install firmware.

Viewing the last update operation report

About this task

The **Last update operation** report is generated automatically when a firmware update starts and is updated with the final status when the update is complete.

The report shows the results of the most recent firmware update performed on a server. Use the report to review the firmware baseline, update options, and component-level results.

Procedure

1. Select **Servers**.
2. Select the checkbox of the required server.
3. Click the **Firmware** tab.
4. Under **Last update operation**, click **View the report** link.
5. Optional. Click Export to download.

   The report is generated automatically when a firmware update operation ends and updated with the final status when the operation reaches a terminal state.
6. Optional. Save the JSON file when prompted by the browser.

Subtopics

Last update operation status

Last update operation status

Remote server with automatic reboot

- When a firmware update requires a reboot, the **Last update operation** report remains in the **PENDING_REBOOT** state until the updated firmware becomes active.
- After the server restarts, Smart Update Manager (SUM) verifies the installed firmware against the selected baseline and updates the report status accordingly:
  - The status changes to **OK** when the installed component version matches the selected baseline.
  - The status changes to **FAILED** when the component version does not match the selected baseline or when post-reboot verification fails.

Localhost server with automatic reboot

When a localhost firmware update requires a reboot, the **Last Update Operation** report remains in the **PENDING_REBOOT** state even after the server restarts. Unlike remote servers update that uses automatic reboot, the localhost post-reboot workflow does not automatically change the status to **OK** or **FAILED**.

Manual reboot

For both remote and localhost servers configured for manual reboot, the report remains in **PENDING_REBOOT**.

Smart Update Manager API

For API documentation, see **Smart Update Manager API reference**.

Log files and directory locations

This chapter describes the locations of configuration files, firmware baselines, certificates, logs, and other application data used by Smart Update Manager (SUM). It also identifies the installation and data directories used for administration and troubleshooting tasks.

Subtopics

Default file and directory locations
Application logs and log locations
Audit logs and logging configuration
GatherLogs utility

Default file and directory locations

The following table lists the default file and log locations.

Purpose	Linux	Windows
Install root	/opt/sum	`%ProgramFiles%\SUM`

Purpose	Linux	Windows
user.yaml	/opt/sum/config/user.yaml	%ProgramData%\SUM\config\user.yaml
system.yaml	/opt/sum/config/system.yaml	%ProgramData%\SUM\config\system.yaml
Database	/opt/sum/data/sum.db	%ProgramData%\SUM\data\sum.db
Install logs	/var/log/sum/install.log	%ProgramData%\SUM\install.log
Node summary log	/var/tmp/sum/20_1_0/logs/prod_id-ser_num/server.log /var/tmp/sum/20_1_0/logs/localhost/server.log	%ProgramData%\SUM\20_1_0\logs\prod_id-ser_num\server.log %ProgramData%\SUM\20_1_0\logs\localhost\server.log
Debug/runtime logs root	/var/tmp/sum/<version>/logs **Example:** /var/tmp/sum/20_1_0/logs	%ProgramData%\SUM\<version>\logs **Example:** %ProgramData%\SUM\20_1_0\logs
Firmware depot	/var/lib/sum/depot	%ProgramData%\SUM\depot
Audit logs	Linux syslog/journald	Windows Event Log
Service logs	/var/log/sum/service/sum_service.log /var/log/sum/service/dse_service.log	%ProgramData%\SUM\20_1_0\logs\
Custom baseline service	/var/log/sum/service/ custom baseline_service.log	
Local CA certificate	/opt/sum/data/ca.crt	C:\Program Files\SUM\data\ca.crt

Data and storage location

The solution stores application data locally on the SUM host. This data includes configuration files, the local database, uploaded firmware baselines, log files, operational artifacts, and database backups.

During installation or the first service startup, SUM creates a local SQLite database. When you upload firmware baselines, such as Service pack for HPE ProLiant (SPP) ISO or ZIP files, through the SUM web UI, SUM stores them in the local firmware depot for processing and use in compliance and update operations.

Subtopics

Local database
Firmware baseline storage
Configuration notes

Local database

Smart Update Manager (SUM) uses a local SQLite database to store application state and operational data, including:

- Server records
- Firmware baseline records
- Job records
- Activity records
- Inventory information
- Encrypted iLO credential data

The database location is defined in the `user.yaml` file:

```
database:
  path: "data/sum.db"
  backup_path: "data/backups"
  max_backup_count: 10
```

If the database path is relative, SUM resolves it from the installation root directory.

Firmware baseline storage

Upload firmware baselines through the Smart Update Manager (SUM) web UI. When you upload an SPP ISO or ZIP file, SUM validates, extracts, processes, and registers the baseline before storing it in the firmware depot.

The default firmware depot locations are:

- **Linux:** `/var/lib/sum/depot`

- **Windows:** `%PROGRAMDATA%\SUM\depot`

> **NOTE**
> Do not manually copy SPP files into the firmware depot unless instructed by HPE Support. Always use the SUM web UI to upload firmware baselines.

Disk space planning for SPP uploads

SPP ISO or ZIP upload and processing operations require additional temporary disk space.

Reserve at least **2.5 times the SPP ISO or ZIP size plus 2 GB of free space** on the depot volume.

For example: For a 5 GB SPP ISO or ZIP: `(5 GB × 2.5) + 2 GB = 14.5 GB`
Insufficient free space can cause firmware baseline upload or processing operations to fail.

Configuration notes

Use the following guidelines when modifying SUM configuration settings:

- Edit only `user.yaml` for customer-configurable settings such as database paths and log settings.
- Do not edit `system.yaml` unless instructed by HPE Support. This file contains system-managed settings, including:
  - Firmware depot path
  - Job limits
  - Authentication policies
- Restart the SUM service after changing configuration settings.

Application logs and log locations

The solution generates application logs and debug logs that record internal processing details, baseline information, node activity, and operations performed during a session. These logs support troubleshooting and diagnostic analysis.

The solution writes application logs to the directory specified in `config/user.yaml`. If `logging.dir` is not specified, it uses the default log locations.

Default log locations

OS	Default log directory
Windows	`%PROGRAMDATA%\SUM\logs`
Linux	`/var/tmp/sum/logs`

Primary log file

The primary application log file is sum.log. Rotated log files share the same base name and are kept based on the retention settings specified in `config/user.yaml`.

Attribute	Value
File name	sum.log
Scope	Session-wide
Records	Baseline details, node additions, and operations performed during a session
Node association	Not node-specific
Behavior on restart	Continues writing to the same file
Session separation	Timestamp added to separate entries between sessions

Audit logs and logging configuration

Audit log locations

The solution records audit events in the native OS logging framework.

Platform	Location
Windows	Windows Event Log
Linux and VMware	Syslog

NOTE
Use OS tools to export and collect audit logs.

Logging configuration parameters

Parameter	Description
`logging.dir`	Specifies the directory for application log fi les
`logging.file`	Specifies the application log file name
`logging.artifact_dir`	Specifies the directory for operation artifac ts

IMPORTANT
If `logging.artifact_dir` is not defined, the application stores operation artifacts in the directory specified by `logging.dir`.

Logging configuration examples

To change the location of the log files and operation artifacts, update the logging settings in `config/user.yaml` and restart the service.

Windows example:

```
logging:
dir: "D:\SUM\logs"
file: "SUM.log"
artifact_dir: "D:\SUM\artifacts"
```

Linux example:

```
logging:
dir: "/var/tmp/sum/logs"
file: "sum.log"
artifact_dir: "/var/tmp/sum/artifacts"
```

Viewing service logs

Platform	Method
Windows	Use **Services** to check status and **Event Viewer** for logs
Linux	`sudo journalctl -u sum--since "24 hours ago"`

More information

Starting, stopping, and verifying the SUM service

GatherLogs utility

Smart Update Manager (SUM) provides the gatherlogs utility to simplify troubleshooting. The utility collects SUM configuration files, SUM application logs, SUM service logs, installer logs, SUT logs, AMS logs, database files, and optional OS diagnostic information into a single support bundle.

During collection, gatherlogs copies files to a current working directory, removes sensitive information of the copied SUM configuration files, SUM application logs, and SUM service logs, and then packages the copied files. Gatherlogs does not modify the original files on the host.

> **IMPORTANT**
> The current implementation includes the SUM database by default. Database files, SUT logs, AMS logs, and OS diagnostic files may still contain sensitive information. Review the support bundle accordance with your organization's security policy before sharing it outside your environment. If support does not require the database, run gatherlogs with `--include-db=false`.

Gatherlogs executable locations

OS	Installed command
Windows	%ProgramFiles%\SUM\bin\x64\gatherlogs.exe
Linux	/opt/sum/bin/x64/gatherlogs

On Linux, the RPM package also creates a /usr/local/bin/gatherlogs symbolic link when the gatherlogs binary is included in the package.

Default gatherlogs output location

By default, gatherlogs writes the support bundle archive to the current working directory where the command is run. To write the archive to a different location, use the `--output-dir` option.

Common commands

Table 1. Collect support bundle

OS	Command
Windows PowerShell	`.\gatherlogs.exe --verbose`
Linux bash	`sudo gatherlogs --verbose`

Table 2. Save to a custom location

OS	Command
Windows PowerShell	`.\gatherlogs.exe --output-dir "$env:TEMP\SUM\support-bundles" --verbose`
Linux bash	`sudo gatherlogs --output-dir /var/tmp/sum/support-bundles --verbose`

Collect logs for a specific time range

By default, gatherlogs collects logs from the previous 360 hours. The following example limits collection to the previous 10 days: `sudo gatherlogs --since 240h --verbose`

Exclude OS diagnostics in restricted environments

Use the `--no-os-commands` option to skip OS diagnostic commands.

```
sudo gatherlogs --no-os-commands --verbose
```

Additional options

Option	Description
`--output-dir <path>`	Writes the support bundle archive to the s pecified directory
`--install-dir <path>`	Uses the specified SUM installation directo ry when locating configuration and databa se files
`--since <duration>`	Includes logs newer than the specified du ration and the default value is 360 hours
`--include-db=false`	Excludes the SUM database and database backups from the support bundle
`--no-os-commands`	Skips OS diagnostic command collection
`--verbose`	Prints detailed collection progress

Support bundle naming convention

Gatherlogs generates archive files using the following format:

```
text
SUM_Gatherlogs_<hostname>_<YYYY-MM-DD_HH-MM-SS>_<os>
```

The generated archive uses the following formats:

OS	Archive format
Windows	.zip
Linux	.tar.gz

Troubleshooting

This chapter describes common issues that you might encounter when installing, configuring, onboarding, and using Smart Update Manager (SUM). It provides information about possible causes, recommended actions, and recovery procedures to help you diagnose and resolve problems.

Subtopics

Localhost record created with incomplete details

Localhost onboarding skipped
Service does not start because port 63002 is already in use
Custom baseline service does not start because port 63003 is already in use
Service does not start or exits immediately
Browser displays a certificate warning during HTTPS access
Cannot log in with valid credentials
Firmware upload does not complete successfully
Target iLO endpoints are not discovered or onboarding fails
Custom SPP creation or component package operations are unavailable
User account is temporarily locked after repeated login attempts
API requests return authentication errors after token expiration
ZIP firmware baseline upload is rejected
Firmware baseline is marked invalid after startup verification
Browser displays old SUM UI content after upgrade
SUM next-generation page does not open

Localhost record created with incomplete details

Symptom

A localhost server record is created in Smart Update Manager (SUM), but the server details are not populated.

Cause

HPE iLO is configured in **High Security**, **FIPS**, or **CNSA** mode.

Action

1. Switch the security mode to **Production (Standard)**.
2. Onboard the localhost server by providing valid iLO administrator credentials.
3. Verify that the localhost server is rediscovered and the details are populated correctly in the **Servers** page.

More information

Localhost server discovery and onboarding
Verifying localhost server added automatically
Adding localhost server by providing iLO credentials

Localhost onboarding skipped

Symptom

Smart Update Manager (SUM) skips localhost onboarding when the localhost system does not meet the requirements for automatic onboarding. SUM displays an activity message indicating either of the following conditions.

Solution 1

Cause

No supported iLO is detected on the localhost system.

Action

No action is available. Localhost onboarding requires a supported iLO.

Solution 2

Cause

An external management application is managing the localhost system.

Action

No action is available. Localhost onboarding is not supported for externally managed systems.

Service does not start because port 63002 is already in use

Symptom

The service does not start and displays a bind error related to port 63002.

Cause

Another process is already listening on port 63002 and prevents the service from binding to the required port. This condition blocks the service from initializing correctly.

Action

1. Identify the process using port 63002.
2. Stop the process.

3. Start the service again.

Custom baseline service does not start because port 63003 is already in use

Symptom

The custom baseline service does not start and displays a bind error related to port 63003.

Cause

Another process is already listening on port 63003 and prevents the service from binding to the required port. This condition blocks the service from initializing correctly.

Action

1. Identify the process using port 63003.
2. Stop the process.
3. Start the service again.

Service does not start or exits immediately

Symptom

The SUM service remains stopped or ends unexpectedly after you attempt to start it. The service does not stay active and might end without clear indication. Logs might show initialization issues.

Cause

The issue can occur when the configuration contains invalid settings or paths, or when a required service dependency is unavailable.

Action

1. Verify that the service account has the required privileges.
2. Review the service logs for error messages.

3. Validate the configuration file syntax and file paths.
4. Start the service again and review the logs.

Browser displays a certificate warning during HTTPS access

Symptom

When you access the application using HTTPS, the browser displays a certificate trust warning. The warning indicates that the connection is not trusted.

Cause

The certificate is self-signed or not trusted by the browser or system.

Action

1. Verify that you are using the following URLs:

   https://localhost:63002

   https://<hostname>:63002
2. Import a trusted certificate if required by your organization policy.
3. Proceed according to your organization security guidelines.

Cannot log in with valid credentials

Symptom

You cannot log in even when you enter valid credentials. The authentication attempt is not successful, and access is denied. The issue may continue across multiple login attempts without any change in behavior.

Cause

This issue can occur for one or more of the following reasons:

- The credentials provided for the host are incorrect or invalid.
- The user account does not have sufficient permissions to access the host.

- Host authentication policies or access restrictions prevent login, even when the credentials are valid.

Action

1. Verify the username and password on the host OS.
2. Confirm that the user has the required administrative privileges.
3. Review authentication logs for additional details or restrictions affecting the login attempt.

Firmware upload does not complete successfully

Symptom

The firmware ISO or ZIP file does not upload or process successfully. The upload activity might remain incomplete or stop before the firmware baseline is added.

Cause

The issue can occur for one or more of the following reasons:

- The ISO or ZIP file is incomplete or corrupted.
- The Smart Update Manager (SUM) host does not have sufficient disk space for upload and processing.
- The firmware package is not supported.

Action

1. Verify the integrity of the ISO or ZIP file to ensure that it is not corrupt or incomplete.
2. Check that sufficient disk space is available for the upload and processing.
3. Retry the upload and monitor the activity status to confirm completion.

Target iLO endpoints are not discovered or onboarding fails

Symptom

Target HPE iLO endpoints are not discovered during the discovery process or the onboarding process does not complete successfully.

Cause

This issue can occur if network connectivity to the target endpoints is not available or is incorrectly configured. Invalid or incorrect iLO credentials can also prevent successful discovery. In some cases, restrictions or settings on the iLO endpoints may block onboarding requests.

Action

1. Verify that network connectivity to the target endpoints is available and routing is correctly configured.
2. Ensure that the iLO credentials entered are valid and have the required permissions.
3. Retry the onboarding process with a smaller set of target endpoints to isolate the issue.

Custom SPP creation or component package operations are unavailable

Symptom

Custom Service pack for HPE ProLiant (SPP) creation, component package upload, component package listing, or component package retrieval does not complete successfully. These operations might be unavailable or terminate unexpectedly when Smart Update Manager (SUM) cannot access the custom baseline service.

Cause

Custom SPP creation and component package operations depend on the Custom Baseline service. If the service is stopped, unavailable, or cannot communicate with SUM, SUM cannot process custom baselines or component packages.

Action

1. Verify that the custom baseline service is running.

On Linux: `sudo /opt/sum/bin/sum-service-control.sh status`

On Windows: `sum-service-control.bat status`

2. If the service is not running, restart SUM and any dependent services.
3. Verify that sufficient disk space is available on the host system.
4. Retry the custom SPP creation or component package upload operation.

User account is temporarily locked after repeated login attempts

Symptom

You cannot sign in to Smart Update Manager (SUM) even when using valid credentials. Authentication requests continue to be rejected following multiple unsuccessful login attempts.

Cause

SUM uses host OS authentication. Repeated unsuccessful login attempts can trigger a temporary account lockout according to the OS security policy.

Action

1. Verify that the username and password are correct.
2. For Windows domain accounts, use one of the supported username formats:
   - `domain_name\user_name`
   - `user_name@example.com`
3. Wait for the lockout period to expire.
4. If access is still unavailable, contact the system administrator to unlock the account according to the OS policy.
5. Review authentication logs if login attempts continue to be rejected.

API requests return authentication errors after token expiration

Symptom

REST API requests return authentication errors such as HTTP 401 Unauthorized. Long-running automation or API client operations terminate unexpectedly after a period of normal operation.

Cause

Smart Update Manager (SUM) REST APIs use bearer-token-based authentication, and access tokens are valid for a limited time. Requests that use expired access tokens are rejected by the authentication service.

Action

1. Configure API clients to detect authentication errors.
2. If a refresh token is available, use the refresh token workflow to obtain a new access token.
3. If a refresh token is unavailable or the token refresh does not complete successfully, authenticate again and obtain a new access token.
4. Use the new access token for all subsequent API requests.
5. Do not reuse expired access tokens.

ZIP firmware baseline upload is rejected

Symptom

A ZIP firmware baseline upload does not complete successfully. Smart Update Manager (SUM) rejects the uploaded archive during validation before processing begins.

Cause

SUM validates uploaded ZIP firmware baselines before extraction. The archive might contain an invalid internal directory structure, unsafe paths, path traversal entries such as `../`, absolute paths, symbolic links, or other unsupported content.

Action

1. Verify that the ZIP file is a valid firmware baseline package obtained from a trusted source.

2. Do not manually modify the internal structure of the ZIP archive.
3. If the archive is damaged or contains unsupported entries, recreate or download an new copy of the ZIP file.
4. Retry the upload using a valid ZIP firmware baseline package.
5. Alternatively, use a supported SPP ISO.

Firmware baseline is marked invalid after startup verification

Symptom

A registered firmware baseline is marked as invalid after Smart Update Manager (SUM) starts. The baseline cannot be used for firmware analysis or update operations.

Cause

During startup, SUM verifies registered firmware baselines and validates the associated files and metadata in the firmware depot. A baseline can be marked invalid if required files are missing, modified, removed, or inconsistent with the stored metadata.

Action

1. Do not manually modify, move, or delete files in the firmware depot.
2. Remove the invalid baseline from SUM.
3. Upload the firmware baseline again by using the SUM UI.
4. If the issue occurs after a restore or migration operation, verify that the firmware depot, database, and related application data were restored together.

Browser displays old SUM UI content after upgrade

Symptom

After upgrading Smart Update Manager (SUM), the browser might continue to use cached SUM UI content. As a result, the UI might display old data or unexpected behavior. For example, firmware baseline changes or updated server inventory values might not appear in a standard browser window.

Cause

The browser is using previously cached SUM UI content instead of loading the updated content after the upgrade. This can cause the UI to display outdated information.

Action

1. Clear the browser cache for the SUM site.
2. Close all SUM browser tabs.
3. Relaunch SUM.
4. If the issue persists, open SUM in a private or incognito browser window to determine whether the issue is related to cached browser content.

SUM next-generation page does not open

Symptom

In HPE Synergy Service Packs (SSP) 26.10.01, the browser page does not open when you run `launch_sum.bat` and select Smart Update Manager next generation.

Cause

These releases include only the legacy version of Smart Update Manager (SUM) and do not contain the SUM next generation application.

Action

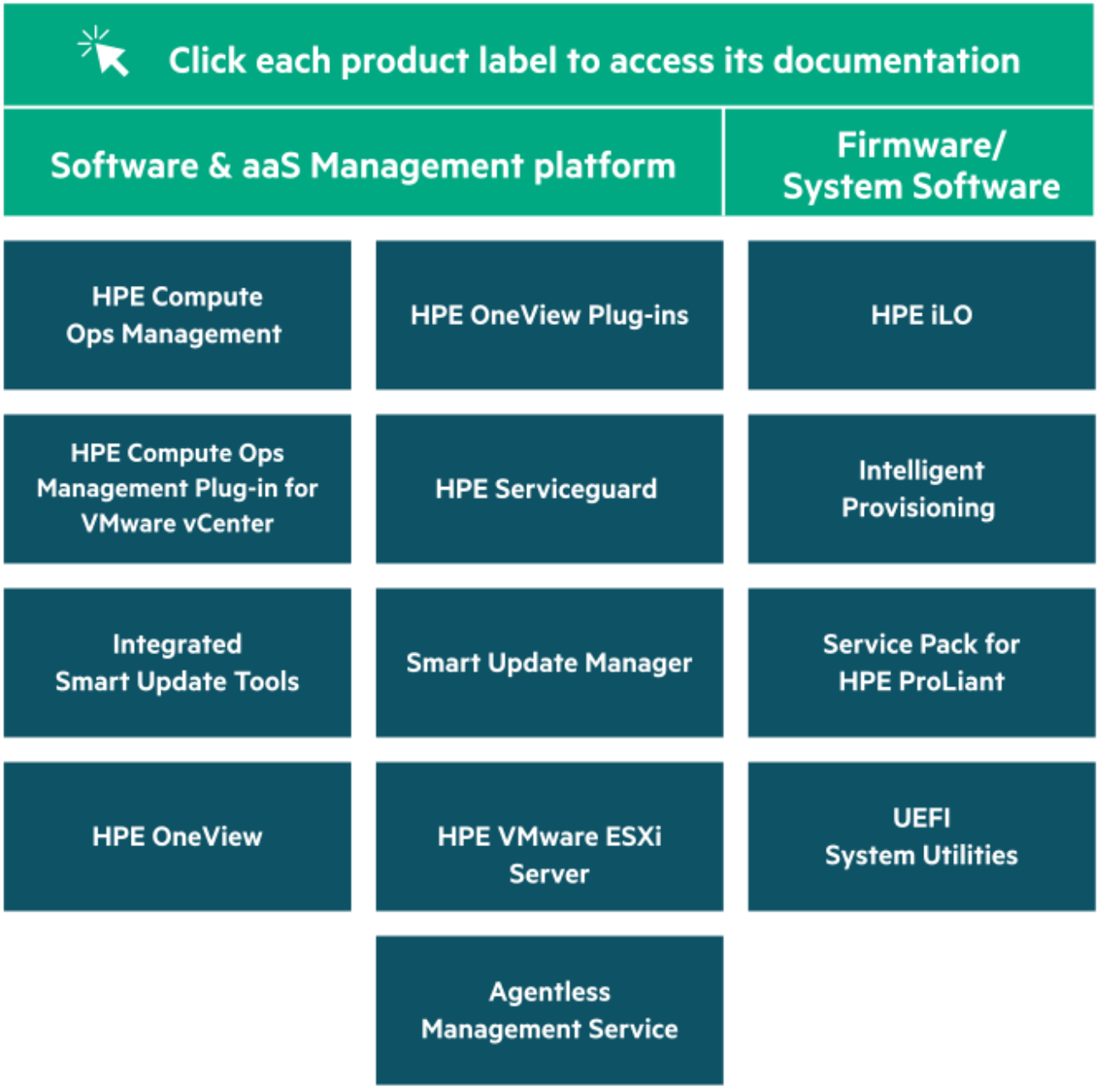
Select **Smart Update Manager** from the launch menu. If no option is selected, the legacy version of SUM starts automatically after 14 seconds.

> **NOTE**
> The issue is limited to HPE SSP 26.10.01 and earlier releases. HPE SSP releases later than 26.10.01 include next generation SUM support and are not affected.

HPE Compute Software and Firmware Product Documentation Quick Links

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

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



Navigating the Hewlett Packard Enterprise Support Center

-
  Navigation and workspace
-
  Search and product knowledge

Websites

General websites

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

https://www.hpe.com/storage/spock

Technical papers and analyst reports

https://www.hpe.com/us/en/resource-library

For additional websites, see Support and other resources.

Support and other resources

Subtopics

Accessing Hewlett Packard Enterprise Support
HPE product registration
Accessing updates
Remote support
Warranty information
Regulatory information
Documentation feedback

Accessing Hewlett Packard Enterprise Support

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

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

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

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

Information to collect

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

HPE product registration

To gain the full benefits of the Hewlett Packard Enterprise Support Center and your purchased support services, add your contracts and products to your account on the HPESC.

- When you add your contracts and products, you receive enhanced personalization, workspace alerts, insights through the dashboards, and easier management of your environment.
- You will also receive recommendations and tailored product knowledge to self-solve any issues, as well as streamlined case creation for faster time to resolution when you must create a case.

To learn how to add your contracts and products, see **https://www.hpe.com/info/add-products-contracts**.

Accessing updates

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

  Hewlett Packard Enterprise Support Center

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

  My HPE Software Center

  https://www.hpe.com/software/hpesoftwarecenter
- To subscribe to eNewsletters and alerts:

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

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

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

Remote support

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

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

HPE Get Connected

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

HPE Tech Care Service

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

HPE Complete Care Service

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

Warranty information

To view the warranty information for your product, see the **warranty check tool**.

Regulatory information

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

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

Additional regulatory information

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

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

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

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

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

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

Documentation feedback

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

Documentation feedback

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