HP Sure Click Enterprise 4.4 Release 8 Update 1 (4.4.19.1662) Release Notes

Contents

Notices 4

Introduction 5

Sure Click Enterprise Requirements 5
Required Software for Installation 5
Additional Requirements 6
Supported Browsers 6
Supported Software 7
Supported Languages 9

HP Wolf Security Controller 10

Supported Languages 10
Supported Browsers 10
On-Premise HP Wolf Security Controller 4.4.177 11
Server Requirements 11
SQL Database Requirements 12

HP Sure Click Enterprise 4.4 Release 8 Updates 13

Upgraded the HP Secure Browser to Chromium 128 13
Added Support for Windows 11 24H2 13
Added Support for Firefox ESR 128 13
Microsoft Internet Explorer 11 13
Sure Access Compatibility 14

Microsoft OS and Office Support timelines 15

Limitations 16

General 16
Web Browsing with Microsoft Edge 16
Web Browsing with Mozilla Firefox 17
Documents 17
Controller 17

HP Sure Click Enterprise End of Life (EOL) Dates 18

Deprecated Features and Platforms 19

Future deprecation announcements 19

Changes in HP Sure Click Enterprise 4.4 Release 8 Update 1 20

Changes in HP Sure Click Enterprise 4.4 Release 8 20

Changes in HP Sure Click Enterprise 4.4 Release 7 22

Changes in HP Sure Click Enterprise 4.4 Release 6 28

Bug Fixes and Reported Issues since Release 5 28
Changes in HP Sure Click Enterprise 4.4 Release 5 30
Bug Fixes and Reported Issues since Release 4 30
Changes in HP Sure Click Enterprise 4.4 Release 4 31
Bug Fixes and Reported Issues since Release 3 31
Changes in HP Sure Click Enterprise 4.4 Release 3 32
Bug Fixes and Reported Issues since Release 2 32
Changes in HP Sure Click Enterprise 4.4 Release 2 34
Bug Fixes and Reported Issues since Release 1 34
Changes in HP Wolf Security Controller 4.4.177 35
Bug Fixes and Reported Issues since the last On-Prem Controller release 35
Getting Help 40
Document History 40
ADDENDUM #1 – Sure Click Enterprise Fixed Lifecycle Policy 41
HP Wolf Security Fixed Lifecycle Policy https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL 41
Fixed Life Cycle Policy 41
Lifecycle phases for products under the Fixed Lifecycle Policy 42
Mainstream Support 42
Beyond End-of-Life Support 43
Requirements and Limitations 43
Sure Click Enterprise Fixed Life Cycle Policy 43
HP Secure Browser Fixed Life Cycle Policy 44
FAQ 44

Notices

November 6, 2024

Introduction

The Release Notes cover the HP Sure Click Enterprise 4.4 product release, and subsequent updates, providing information about new functionality and the requirements for Sure Click Enterprise.

Sure Click Enterprise Requirements

Sure Click Enterprise requires the following hardware and software for this release:

Hardware or Software	Description
CPU	Intel Core i3, i5, i7, i9 and XEON with Intel Virtualization Technology (Intel VT) and Extended Page Tables (EPT) enabled in the system BIOS. AMD processor with Rapid Virtualization Indexing (RVI). Sure Click Enterprise supports most enterprise class AMD CPUs sold since 2011. Supported models are the Ryzen range of CPUs, and models that are of type A4/A6/A8/A10 (followed by a four-digit number in which the first digit is not 3.) HP recommends quad-core AMD CPUs for optimal performance. Computers with vPro chipsets are highly recommended.
Memory	Minimum: 8GB RAM, 16GB RAM Recommended. It is recommended that you check the amount of available memory by logging into a device after it has been powered on for a minimum of 30 minutes and before any applications have been launched. As a baseline, HP recommends that a typical endpoint has at least 4GB of available memory available before installing and enabling isolation on both Windows 10 and 11.
Disk	At least 6GB free disk space.
Operating System	Microsoft Windows versions are supported as documented in the HP Sure Click Enterprise Windows Support policy: https://enterprisesecurity.hp.com/s/article/Windows-Support-Policy You must ensure that HP Sure Click Enterprise is upgraded to the latest version prior to upgrading to a new version of Windows and you have checked the latest version supports the version of the operating system you are upgrading to. The HP Sure Click Enterprise EOL policy can also be referenced here: https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL
Note: Refer to your system manufacturer's documentation for details about enabling virtualization on Intel and AMD processors. If you are using `msiexec` to install Sure Click Enterprise remotely, ensure you include the `SERVERURL` setting, otherwise installation will fail.	

Required Software for Installation

- Microsoft .NET Framework 4.7.2

- Visual Basic for Applications (a shared feature in Microsoft Office installation for secure printing from Office)
- XPS Services must be enabled, and the Microsoft XPS Document Writer must be present to use secure printing

Additional Requirements

HP Sure Click Enterprise installation requires the following:

- An HP cloud-hosted instance of Wolf Security Controller, or a customer on-premise Wolf Security Controller
- Local administrator privileges (if installing on specific machines for evaluation)
- A valid Sure Click Enterprise license, provided by your HP Sales or Customer Support representative

Supported Browsers

- HP Wolf Security Extension for Chrome supports the latest Google-recommended version of Google Chrome
- HP Wolf Security Extension for Firefox supports the latest Mozilla-recommended version of Firefox (ESR (115 and 128) or non-ESR, 64-bit only)
- HP Wolf Security Extension for Edge supports the latest version of the Microsoft Edge Chromium browser only

Note: Chrome support is detailed in the Sure Click Enterprise Support Knowledge Base: https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL

Supported Software

Microsoft Office 2016, MSI/Click-to-Run, x64/x86:

- Standard, ProPlus, Home Business, Home Student, Personal, Professional, O365 ProPlus, O365 Business, O365 Small Business Premium, O365 Home Premium

Microsoft Office 2019, Click-to-Run, x64/x86: (Office 365 / Microsoft 365):

- Standard, ProPlus, Home Business, Home Student, Personal, Professional, 365 ProPlus, 365 Business, 365 Small Business Premium, 365 Home Premium

Microsoft Office 2021, Click-to-Run (Office 365 / Microsoft 365):

- Standard, ProPlus, Home Business, Home Student, Personal, Professional, 365 ProPlus, 365 Business, 365 Small Business Premium, 365 Home Premium

Microsoft 365 Apps for Enterprise:

- Isolation Support for PowerPoint, Excel, Word, Outlook Attachments per previous releases.
- Support for Current, Monthly Enterprise and Semi-Annual channels.

Note: Microsoft Office shared computer activation licensing is supported; however, on some systems, when opening an isolated Word document, users may temporarily see a banner stating Office has not been activated.

Note:
The MSI version of Office is only supported for Office 2016
Retail Licensing – Standard & ProPlus 64bit
Volume Licensing– Standard & ProPlus 64bit

Note: Outlook Cached Exchange mode is required for Outlook protection

Adobe Acrobat Reader versions: DC 2023, 2024

Windows Media Player 12

Oracle VirtualBox:

- While Oracle VirtualBox claims to have nested-VT support, it is implemented in such a way as to be incompatible with HP Sure Click Enterprise and thus running HP Sure Click Enterprise in a guest VM inside VirtualBox is not supported.
- HP Sure Click Enterprise can run alongside Oracle VirtualBox on the host, but only on Intel CPUs and only if Microsoft Hyper-V is disabled – this is not a HP Sure Click limitation.

Support for endpoints running Windows Hypervisor Platform (WHP/HyperV) and Virtualization-Based Security (VBS) with the following configuration:

- Windows Hypervisor Platform - WHP (on Windows 10 21H2 - 19044 and above)

- Windows 64-bit with virtualization-based security (VBS) enabled
- UEFI Secure Boot enabled
- The Fast Startup power option in Windows must be disabled
- Intel vPro 4th generation Core (i3/i5/i7) and newer or AMD Ryzen

Trusted Platform Module (TPM) is recommended

Support for non-vPro Intel chipsets

Note: Running Sure Click Enterprise without VMCS Shadowing will result in performance degradations vs. vPro systems, however HP has taken steps to mitigate performance differentials to all extents possible.

For non-vPro chipsets: hibernation / S4 capabilities are disabled and hidden on the host

VDI deployments are supported on:

- VMWare Horizon View 8.x (last validated with version 8 2111 with ESX 7.0)
- Citrix Virtual Desktops 7.x (last validated with version 7 2203 with Citrix Hypervisor 8.2)
- SINA WorkStation 3.5.2 by Secunet Security Networks:
    - Solution verified on SINA Workstation 3.5.2
      If you are unable to run SINA Workstation 3.5.2 due to hardware limitations, the latest 3.5.1 version is also compatible with HP Sure Click Enterprise 4.4.
    - An AppPack is available for Secunet customers for Windows 10 running on verified hardware.

Anti-virus and other 3rd party anti-malware solutions:

- Please consult the HP Sure Click exclusions KB article when using antivirus products with Sure Click to avoid conflicts. The latest information can be found here:
  https://enterprisesecurity.hp.com/s/article/Bromium-and-Third-Party-Software-Interoperability-Guide
- **Important:** Ensure you create appropriate exclusions in the configuration of installed endpoint security products so as not to interfere with or prevent the normal operation of HP products. Necessary actions may consist of excluding all HP Sure Click Enterprise processes and binaries from the third-party endpoint security product. To create exclusions, refer to your third-party product documentation. The absence of exclusions may result in failed Sure Click Enterprise initialization and slow or blocked browsing and opening of untrusted documents. Refer to the HP Sure Click Enterprise Installation and Deployment Guide for information about creating exclusions.

Supported Languages

HP Sure Click Enterprise endpoint software supports the following languages on the specified version of Windows **(** denotes new language in this release):**

• Brazilian Portuguese (pt-BR) • Bulgarian (bg-BG) • Chinese (Simplified) (zh-CN) • Chinese (Traditional) (zh-TW) • Croatian (hr-HR) • Czech (cs-CZ) • Dutch (nl-NL) • Danish (da-DK) • English US (en-US) • English UK (en-GB) • Estonian (et-EE) • Finnish (fi-FL) • French (fr-FR) • French Canadian (fr-CA) • German (de-DE) • Greek (el-GR) • Hungarian (hu-HU)	• Italian (it-IT) • Japanese (ja-JP) • Korean (ko-KR) • Lithuanian (lt-LT) • Latvian (lv-LV) • Norwegian (nb-NO) • Polish (pl-PL) • Portuguese (pt-PT) • Romanian (ro-RO) • Serbian Latin (sr-Latn-RS) • Slovak (sk-SK) • Slovenian (sl-SI) • Spanish (es-ES) • Swedish (sv-SE) • Thai (th-TH) • Turkish (tr-TR) • Ukrainian (uk-UA)

Note:
- HP Sure Click Enterprise supports all Windows locales.
- If your language is not listed above, you will need to deploy the full English language pack (LpCab) to use Sure Click (not the Language Experience Pack (LXP))
- HP Sure Click Enterprise does not support any LXPs.
- If the language is listed above, it means the language is supported both in the micro-vms, for untrusted documents and with the native UI on the host, ie Desktop Console

HP Wolf Security Controller

This section applied to both the HP cloud-hosted Wolf Security Controller as well as the optional customer-hosted on-premise Wolf Security Controller.

Supported Languages

The HP Wolf Security Controller can be configured by users to appear localized in the following languages:

- Brazilian Portuguese
- Dutch
- English
- French
- German
- Italian
- Japanese
- Spanish
- Swedish

The language is saved as a user profile setting and will remain on the selected language until a user changes it. The language selection button is shown after the initial login using the following control in the top left of the controller user interface:

Supported Browsers

The Controller web interface is supported on the latest versions of HP Secure Browser, Edge Chromium, Chrome, and Firefox.

On-Premise HP Wolf Security Controller 4.4.177

The following tables list the hardware and software requirements for the server running the controller and the SQL database on which it relies.

Important: Before installing a new version of the controller, make sure to back up your current database.

Server Requirements

Hardware or Software	Description
CPU	Sandy Bridge Intel Xeon Quad-core or better
Disk	1 TB free disk space
Network	Port 443 on the web server must be available for the endpoints to communicate with the controller.
Internet	The Controller is recommended to have https (port 443) access to the HP Cloud Service in order to receive HP Rules File updates, as well as Threat Intelligence Reports, Malware names and recent attack information. For more information see: https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
Operating System	Windows Server 2016 Windows Server 2019 Windows Server 2022
Memory	16 GB RAM
Software	Microsoft IIS 7.5+ with CGI module, IIS Manager, static content, and anonymous authentication installed .NET 4 Extended (server)
SSL	Valid SSL certificate trusted by endpoints (For testing only, the server may be configured insecurely to run in HTTP mode)

SQL Database Requirements

Hardware or Software	Description
Performance	200 IOPS sustained per 1000 endpoints
Software	SQL Server 2014 SP3+ SQL Server 2016 SP2+ SQL Server 2017+ SQL Server 2019+ SQL Server 2022+ Standard and Enterprise editions are supported Server Management Studio (SSMS) as the management suite for the controller database SQL Express should be used in a limited test or evaluation environment only
Storage Space	1 TB available space

HP Sure Click Enterprise 4.4 Release 8 Updates

Gathering of telemetry data

HP collects license telemetry data and customer experience data for its legitimate business interests, including license compliance.

Customers who enable "HP Threat Intelligence" cloud services connections agree to have their license telemetry data and HP Customer Experience Improvement Program data collated and uploaded automatically to HP Wolf.

Customers who do not enable "HP Threat Intelligence" cloud services connections will be required to submit regular, manual uploads of license telemetry data to HP Wolf. Optionally, the Customer can choose to include HP Customer Experience Improvement Program data with the license telemetry data. All data is generated from the On-Prem Controller user interface and downloaded to the local machine. The file must then be sent manually to HP Wolf.

This is described in detail in KB article: Sending On-Prem Telemetry Data to HP Wolf.

Upgraded the HP Secure Browser to Chromium 128

HP Sure Click Enterprise 4.4 Release 8 updates the HP Secure Browser to Chromium 128.

Added Support for Windows 11 24H2

HP Sure Click Enterprise 4.4 Release 8 supports Windows 11 24H2.

Added Support for Firefox ESR 128

HP Sure Click Enterprise 4.4 Release 8 adds support for Firefox ESR 128.

Microsoft Internet Explorer 11

Internet Explorer 11 is no longer supported by Sure Click Enterprise as an isolated browser. IE11 is however supported as an ingress-application, meaning downloaded files from IE11 can still be configured to be untrusted by default. This can help to reduce risk where IE11 must still be used. HP recommend IE11 is blocked from all internet access due to security concerns and lack of updates.

In a future update to Sure Click, HP is dropping ALL support for Internet Explorer 11, including the support to mark it as an ingress application. IE11 should never be used to access the internet due to security risks as it is no longer maintained or updated by Microsoft.

Sure Access Compatibility

HP Sure Click Enterprise 4.4 Release 8 is compatible with the following Sure Access Enterprise releases (SAE):

- HP Sure Access Enterprise Release 8.1 Release 4 (8.1.2.215)
- Max VHV 4.9.0

Microsoft OS and Office Support timelines

HP regularly updates which operating system versions are supported based on the latest information from Microsoft: https://docs.microsoft.com/en-gb/windows/release-information/. Removal of support for an operating system will be documented in Release Notes at least one release/version prior to the removal. The overall HP Sure Click Enterprise Windows support policy can be found online at: https://enterprisesecurity.hp.com/s/article/Windows-Support-Policy

Supported:

Windows 11

- Windows 11 Version 24H2 – OS Build 26100 (EOL October 2027)
- Windows 11 Version 24H2 LTSC (EOL October 2029)
- Windows 11 Version 23H2 – OS Build 22631 (EOL November 2026)
- Windows 11 Version 22H2 – OS Build 22621 (EOL October 2025)
- Windows 11 Version 21H2 – OS Build 22000 (EOL October 2024)

Windows 10

- Windows 10 Version 22H2 – OS Build 19045 (EOL October 2025)
- Windows 10 Version 21H2 – OS Build 19044 (EOL June 2024)
- Windows 10 Version 21H2 LTSC (EOL Jan 2027)
- Windows 10 Version 1809 LTSC OS Build 17763 (EOL Jan 2029)**
- Windows 10 Version 1607 LTSC (Not Supported)
- Windows 10 Version 1507 LTSC (Not Supported)

Microsoft Office

- Microsoft Office M365 Continual Support while updated
- Microsoft Office 2016 (EOL October 2025)
- Microsoft Office 2019 (EOL October 2025)
- Microsoft Office 2021 (EOL October 2026)

** Available as a separate downloadable AppPack

Limitations

General

- Excel 2019 files shared using 'Send as PDF' file sends the email with a text file attachment instead of a PDF.
- Applications opened in isolation (that is, in a micro-VM) are not available to assistive technology such as JAWS and ZoomText Magnifier/Reader. HP is working to add accessibility support to untrusted documents and webpages in a future release.
- Do not install Sure Click Enterprise software from a removable drive, such as a USB drive. Removable drives are not trusted by default and, when the initialization stage occurs, the installer will fail because it can no longer read the data on the removable drive.
- Saving to and opening untrusted documents from the cloud is not supported for Office 0365.
- If isolation is not already initialized on the system, users that have roaming profiles will see initialization occur the first time they log in to the system.
- To install Symantec Endpoint Protection after Sure Click Enterprise, restart the machine first.
- Temporary trust operation will not trust sites that use "guce-advertising.com" redirect capabilities. The redirects used by this advertising network break lots of web and software workflows. HP is working to resolve this, but it is a workflow introduced by Verizon Media on most of their web properties. https://legal.yahoo.com/ie/en/yahoo/privacy/advertising/index.html

Web Browsing with Microsoft Edge

- Microsoft Edge's support for Microsoft Defender Application Guard does not include extensions which use native messaging.

  This means that the HP Wolf Security Extension (WSX) (formerly "SBX") and the older standalone Credential Protection extensions do not work in Edge Application Guard. WSX enters an error state because it cannot connect to its native messaging host.

  This is a Microsoft browser issue and not one that can be resolved by HP.

  Skype extension is not supported.

  Please note that as of 4th April 2024, Microsoft Defender Application Guard is no longer supported and is considered deprecated by Microsoft – See https://learn.microsoft.com/en-us/deployedge/microsoft-edge-security-windows-defender-application-guard

Web Browsing with Mozilla Firefox

- If Firefox is already installed on endpoints and has not been launched prior to installing Sure Click Enterprise, you must do the following to ensure browser sessions are isolated in a micro-VM:
    - Launch Firefox to create a new profile for the user. If you have multiple users or if you create new users, you must launch Firefox for each new or additional user.
    - Close Firefox and restart Sure Click Enterprise.
    - You can now launch Firefox in an isolated micro-VM.
    - These steps also need to be performed if you create more than one Firefox profile per user.
- An issue occurs where Firefox is configured as a virtualized browser and set as the default handler for untrusted browser (.html) files. When the file is opened a tab erroneously appears stating that a navigation has been blocked

Documents

- Sure Click Enterprise isolates documents from accessing corporate resources or files stored on the desktop or intranet. As a result, if a document opens in isolation attempts to connect to a database on the intranet or a linked file on the desktop, it will fail and produce an error. To enable this functionality, you must remove Sure Click Enterprise protection from the document.
- ASX video files and Windows Update Standalone Installer (MSU) files cannot be opened in micro-VMs.
- Isolation does not support multiple, simultaneous Microsoft Office installations of the same version.
- Users may receive an error when opening an isolated file with paths that exceed the Operating System limits.

Controller

- The controller continues to display the last-known device health status even when the device has not been recently reconnected. Be sure to check the connectivity information and last check-in date for the device.

HP Sure Click Enterprise End of Life (EOL) Dates

Versions are classified as follows:

- Major Version [DOT] Minor Version [DOT] Update version. (for example, 4.4.18)

Product Support Policy:

- The latest update of the current Major Version of the Product is Supported.

Product Name	Release Date	EOL Date	Status
HP Sure Click Enterprise Release 8 Update 1 (4.4.19.1662)	6th Nov 2024	6th May 2025	Current GA
HP Sure Click Enterprise 4.4 Release 8 (4.4.19.1546)	18th Oct 2024	6th Nov 2024	EOL
HP Sure Click Enterprise 4.4 Release 7 (4.4.18.284)	5th Sept 2024	5th Mar2025	Mainstream
HP Sure Click Enterprise 4.4 Release 6 (4.4.14.323)	3rd May 2024	3rd Nov 2024	EOL
HP Sure Click Enterprise 4.4 Release 5 (4.4.12.501)	16th Feb 2024	16th Aug 2024	EOL
HP Sure Click Enterprise 4.4 Release 4 (4.4.8.370)	31st Oct 2023	16th Aug 2024	EOL
HP Sure Click Enterprise 4.4 Release 3 (4.4.7.405)	27th Sept 2023	30th Apr 2024	EOL
HP Sure Click Enterprise 4.4 Release 2 (4.4.3.274)	27th June 2023	27th Mar 2024	EOL
HP Sure Click Enterprise 4.4 Release 1 (4.4.1.571)	10th Jan 2023 (Initial Release)	27th Dec 2023	EOL
HP Sure Click Enterprise 4.3 (4.3.12.9)	19th Oct 2022	27th Dec 2023	EOL

Full Product Support and End of Life Policy (EOL):

https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL

Deprecated Features and Platforms

Older platforms and features are being deprecated from the latest versions of HP Sure Click Enterprise. Customers should read the KB article that explains the platforms and features being deprecated and the timeframes/versions in scope.

The latest information regarding deprecated features and platforms:

https://enterprisesecurity.hp.com/s/article/Deprecated-Features

The following features are no longer supported and have been removed in Sure Click Enterprise 4.4 Release 8 after being announced deprecated in previous release notes.

- Isolated Firefox Support – ESR 102

Future deprecation announcements

Features and support that will be deprecated and removed in a future version of Sure Click Enterprise:

Microsoft SQL Server (Applies to on-prem HP Security Controller only)

- SQL Server 2014 — Removal from product in December 2024
- SQL Server 2016 — Removal from product in December 2026
- SQL Server 2017 — Removal from product in April 2028
- SQL Server 2019 — Removal from product in July 2030
- SQL Server 2022 — Removal from product in July 2033

Operating Systems (Generally removed 6 months after Microsoft makes them End of Life)

- Windows 10 Version 22H2 – OS Build 19045 — Removal from product in April 2026
- Windows 10 Version 21H2 – OS Build 19044 — Removal from product in January 2025

Citrix Hypervisor (VDI)

- Nested Virualization Support — Not supported in Citrix Hypervisor 8.2.1

  https://support.citrix.com/s/article/CTX560749-nested-virtualization-statement-for-citrix-hypervisor?language=en_US

Microsoft Office / O365 / M365

- Microsoft Office 2016 (All Versions) — Removal from product in October 2025
- Microsoft Office 2016 (All Versions) — Removal from product in October 2025
- Microsoft Office 2019 (All Versions) — Removal from product in October 2025
- Microsoft Office 2021 (All Versions) — Removal from product in October 2026

Changes in HP Sure Click Enterprise 4.4 Release 8 Update 1

The following endpoint tickets were added at this release:

Reference	Type	Description
89917	Customer Fix	Fixed an issue that caused excessive initializations on certain devices resulting in excessive disk usage.

Changes in HP Sure Click Enterprise 4.4 Release 8

The following endpoint tickets were added at this release:

Reference	Type	Description
84675	Support Removed	Removed support for Legacy Edge as an ingress application.
86071	Customer Fix	Fixed an issue in MS Excel when opening an untrusted document saved with "Page Layout" view.
82972	Improvement	Increased the default size limit from 25MB to 50MB for host log files, and from 2MB to 5MB for all other log files.
84293	Customer Fix	Added new configuration option (Untrusted.ArchiveCodePageOverride) which can be used to override the code page used to decode file names in untrusted Zip and Tar archives that don't contain files names in UTF-8. For example, if this config is set to 932 (Shift-JIS) then file names in archives with Shift-JIS encoding will correctly decode to Japanese characters.
85950	Customer Fix	Fixed an issue so that the user has the same behaviour as upstream chrome if "Browser.Chrome.AllowGuestToggleKeyboardLock" is set to 1. That is, the ESC key will not be pre-handled in host and will not exit full screen.
15036	Platform Fix	Machines won't enter modern standby whilst a template is being created, but they will be allowed to enter modern standby once the template completes
88588	Customer Fix	Sure Click will no longer start a new template whilst a machine is in modern standby since doing so would often result in the template failing
76814	Platform Update	Added support for Windows 11 24H2.
78228	Customer Fix	Only admin users can add protection to files for which they don't have write access.
81712	Customer Fix	WSX for Firefox now installs correctly.
84251	New Feature	Added support for Firefox ESR 128.

Reference	Type	Description
84251	Support Removed	Remove support for Firefox ESR 102.
84675	Support Removed	Removed support for Legacy Edge as an ingress application.
86071	Customer Fix	Fixed an issue with opening an untrusted MS Excel document that was saved with "Page Layout" view.
88028	Customer Fix	Fixed an issue causing BSOD after installing the Microsoft KB4052623 Update for Microsoft Defender Antivirus anti-malware platform.
88806	Customer Fix	Fixed issue causing unexpected closure of an application when Open/Save File Dialogs were shown.
82232	Update	Added support for Chromium 128.
86815	Customer Fix	Fixed an issue with winver that resulted in different Windows versions being reported from host and uVM.
85729	Customer Fix	Fixed an issue with Persistent Storage errors being reported after installing Microsoft KB5036893.

Changes in HP Sure Click Enterprise 4.4 Release 7

The following Controller updates apply to this release.

Reference	Type	Description
66900	UI Update	Added a missing Sure Sense Icon into the Threats UI. This was previously missing for events such as 'Behavioural Protection'.
75920	Feature Update	Updated the Device Properties tab to include the Windows edition as the Operating System Product name.
76290	Security	The HP Wolf Controller now disables logins on a growing time delay when incorrect credentials are used. This blocks robots and scripts from brute forcing logins.
76298	Security	Updated security so that Controller passwords must now be NIST/NCSC compliant.
76917	Customer Fix	Corrected the category for the 'Corrupted local group policy...' management action. It is now set to 'Environmental', which aligns with the documentation.
76917	UI Update	Corrected the category for the 'Corrupted local group policy...' management action. It is now set to 'Environmental', which aligns with the documentation.
77608	Improvement	Added a new remote command to reset the software channel update status on any given endpoint. This will allow it to retry the software update service.
77743	Improvement	Added 2 new management actions for software update failures which will be visible in the dashboard.
78521	Management Action	Added new 'FirmwareFeatures' management actions to report items for administrator consideration.
78939	Customer Fix	Resolved an issue which could see Management Actions listed twice in the dashboard and Management Actions pages
78989	Customer Fix	Isolation status colors have been restored on the Devices table
79020	Improvement	When clicking through to view Management actions, devices can now be grouped and remote commands send, directly from the Management Actions page.
79470	Improvement	Updated the built-in 'Trust Microsoft Office 365' policy with the latest Microsoft URLs.
80001	Management Action	Added a new management action to communicate when the Google Widevine DRM library is no available for the HP Secure Browser to show DRM content.
80197	Fix	Resolved an issue where endpoints from South Africa could report management actions in French.
80270	Improvement	Fixed an issue where on-prem controllers might not be able to see Fullscreen controller health graphs.

Reference	Type	Description
80450	Security	Updated various third-party components to mitigate known vulnerability: CVE-2023-38325
80706	Security	Updated various third-party components to mitigate known vulnerabilities: CVE-2023-2602, CVE-2023-35945, CVE-2023-37920, CVE-2017-10784, CVE-2023-36617
81106	Management Action	Added a new management action to communicate when the unsupported MS Outlook BETA is in use and not protected by isolation.
81188	UI Update	Updated several HP Security Controller pages for working with management actions.
81342	UI Update	Updated the 'Device Properties' tab. This now includes the status for GPU hardware rendering.
81344 81345	Feature Update	Added support for GPU properties for devices: • The Devices table now includes the device GPU Device and GPU Driver properties, which can be used for sorting of devices. • The detailed Device view now includes the GPU property. Hovering over the GPU property shows full details for the GPU. • It is now possible to create an automatically synchronized group based on GPU Device or GPU Driver.
81728	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2023-2249, ALAS-2023-2257, ALAS-2023-2259, GHSA-v8qr-m533-qhj9, CVE-2022-48174, CVE-2023-38039
81960	UI Update	Renamed 'Device Security' in the in the navigation bar and page title. These now read 'Device Management'. These are both localized into all supported languages.
81980	Policy Update	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
81980	Policy Update	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
82063	Security Update	Updated various third-party components to mitigate known vulnerabilities. ALAS2-2023-2312, ALASSELINUX-NG-2023-001, CVE-2023-44487, ALAS-2023-2271, ALAS-2023-2280
82360	Fix	On the Devices page, the Filter now has a maximum text length of 4000 characters.
82487	Updated Policies	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.

Reference	Type	Description
82742	Feature Update	Updated the Software Channels UI in the policy to make it clearer which packages and versions are included in any given channel.
82958	UI Update	On the Devices page, the Filter now has a maximum text length of 3900 characters.
83012	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2023-2350, ALAS-2023-2351, ALAS-2023-2357, ALAS-2023-2369, CVE-2023-5678 CVE-2023-49083
83012	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2023-2350, ALAS-2023-2351, ALAS-2023-2357, ALAS-2023-2369, CVE-2023-49083, CVE-2023-5678
83210	Updated Policies	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
83300	UI Update	Updated the color coding of status indicators so that grey is not used in error.
83360	Localization Update	Replaced a single appearance of Japanese characters in the French translation of Policy pages.
83590	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2380, ALAS-2024-2385, ALAS-2024-2400, ALAS-2024-2412, CVE-2023-52323
83600	New Feature	Added support for TPM version and TPM model for devices. These appear in device details alongside CPU and GPU, and can be used to evaluate compatibility.
83920	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2419, CVE-2023-6129, CVE-2023-6237, CVE-2024-0727
83976	Feature Update	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
84188	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2442, CVE-2023-52071, CVE-2024-0853, GHSA-3ww4-gg4f-jr7f, GHSA-xxj9-f6rv-m3x4
84190	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2442, CVE-2023-52071, CVE-2024-0853, GHSA-3ww4-gg4f-jr7f, GHSA-xxj9-f6rv-m3x4
84465	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2456, GHSA-6vqw-3v5j-54x4
84607	Customer Fix	Updated reporting to ensure malware names are included in Sure Click threats.

Reference	Type	Description
84807	Security Update	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2478, ALAS-2024-2479, ALAS-2024-2487, ALAS-2024-2490
85182	Security Update	Updated various third-party components to mitigate known vulnerability: GHSA-vmqv-47j8-qwv8
85302	Enhancement	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
85619	Security Update	Updated various third-party components to mitigate known vulnerability: GHSA-67hx-6x53-jw92 (https://nvd.nist.gov/vuln/detail/CVE-2023-45133)
85945	Security Update	Updated various third-party components to mitigate known vulnerabilities: CVE-2024-2511, ALAS-2024-2512, ALAS-2024-2519, GHSA-2m57-hf25-phqg, GHSA-v5h6-c2hv-hv3r, GHSA-w3h3-4rj7-4ph4
85966	Security Fix	Updated various third-party components to mitigate known vulnerability: GHSA-mr82-8j83-vxmv
86095	Security Fix	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2521, ALAS-2024-2523, ALAS-2024-2526
86689 85962	Security Update	Updated various third-party components to mitigate known vulnerabilities: CVE-2023-42363, CVE-2023-42364, CVE-2023-42365, CVE-2023-42366, GHSA-2qr8-3wc7-xhj3, GHSA-6c5p-j8vq-pqhj, GHSA-9wx4-h78v-vm56, GHSA-cjwq-qfpm-7377, GHSA-vq3r-rm7w-2xqh
87408	Security Update	Updated various third-party components to mitigate known vulnerabilities: CVE-2023-42364, CVE-2023-42365

The following Sure Click updates apply to this release

Reference	Type	Description
51871	Customer Fix	Fixed issue where Word unexpectedly closes when trying to pin a folder to the Quick Access list in the Save As menu.
54130	Customer Fix	Fixed an issue that caused the Users tab on the Devices page to display an incorrect AAD username after a change of login.
54266	New Feature	Fixes an issue with the propagation of display settings between the host and uVMs. When a high-contrast display is now selected on the host, this setting will now also be used in uVMs.

Reference	Type	Description
64957	Customer Fix	Fixed issue with JPG image files created on Android systems. These files would not render in the Windows Photo Viewer because of a damaged ICC profile metadata in the source files. Local copies of these files are now created with corrected metadata, and these local copies display correctly.
67466	Customer Fix	Updated PDF support so that PDFs embedded in an untrusted PDF can now be opened inside the same uVM.
68355	New Feature	Fixed an issue when attempting to attach a malicious file to an email. The expected warning pop-up window now appears correctly.
72426	Customer Fix	Fixed an issue with "Save Image As" and "Save Page As" context menu commands in Firefox.
80916	Security Updates	Updated various third-party components to mitigate known vulnerability: CVE-2023-20588
81155	Customer Fix	Fixed an issue so that password protected Outlook email attachments can now be saved when trust-on-ingress is enabled.
81308	Security Updates	Updated various third-party components to mitigate known vulnerabilities: CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-1255, CVE-2023-2650
82258	Customer Fix	Updated handling to prevent incorrect reporting of Code Integrity events.
82662	Update	Different wordings for different documents. • For WPS: "HP Wolf security products now require .NET 4.7.2, which is shipped with all HP Wolf-supported versions of Windows 10." • For SAE: "HP Sure Access Enterprise now requires .NET 4.7.2, which is shipped with all HP Sure Access Enterprise-supported versions of Windows 10." • For SCE: "HP Sure Click Enterprise now requires .NET 4.7.2, which is shipped with all HP Sure Click Enterprise-supported versions of Windows 10."
83157	Improvement	Optimized disk usage for Copy-on-Write (COW) operations. A machine can now reinitialize when COW usage reaches a configurable limit.
83381	Customer Fix	Fixed issue with policy path handling. Policy paths can now be UNC paths (including those to DFS drives) and paths with mapped drive letters.
83694	Customer Fix	Fixed issue where Excel unexpectedly closes after clicking the Browse button on the Save As menu.
83706	Accessibility Support	Added support for Adobe Acrobat Reader specific accessibility settings in guest.
84031	Customer Fix	Fixed issue where untrusted links received through Outlook did not redirect to the Secure Browser.

Reference	Type	Description
84162	Customer Fix	Fixed issue where links sent to the Secure Browser would not load.
84794	Threat Classification Update	Fixed an issue arising from a Chrome update to prevent False Positive threat alerts from being raised.
84861	Security Updates	Upgrade Secure Browser to support Chrome 122. Includes updates for various third-party components to mitigate known vulnerabilities: CVE-2024-0808, CVE-2024-0809, CVE-2024-0810, CVE-2024-0811, CVE-2024-0814, CVE-2024-1077, CVE-2024-1675, CVE-2024-2400
84865	New Feature	Updated Secure Browser to support the following Chrome group policies: *HttpsOnlyMode*, *HttpsUpgradesEnabled*, *HttpAllowlist*, and *InsecureContentAllowedForUrls*. These policies control the HTTP-HTTPS upgrade behavior in an enterprise setting.
84883	Customer Fix	Fixed an issue where third party shell extensions implemented in .NET could cause HP Sure Click to stop unexpectedly.
84933	Fix	Fixed an issue arising from an Acrobat Reader update. This prevents a 'New look' popup to be displayed in Untrusted PDF VMs.
85191	Security Fix	Updated various third-party components to mitigate known vulnerability: CVE-2022-27672
85359	Customer fix	Fixed an issue with Sure Click that prevented Zoom Outlook Plugin from updating.
85406	Customer Fix	Fixed an issue that caused a file in an untrusted location to become transiently trusted if an Alternate Data Stream (ADS) was created on the file.
85639	Customer Fix	Fixed inconsistent behavior when a file type is configured to be both escaped out and to be trusted on ingress.
85750	Update	Updated HP Secure Browser to Chrome 124.
86323	New Feature	Added basic support for configuring New Outlook as an ingress application.
87226	Update	Updated HP Secure Browser to Chrome 126.

Changes in HP Sure Click Enterprise 4.4 Release 6

Bug Fixes and Reported Issues since Release 5

Reference	Type	Description
54266	New Feature	Fixes an issue with the propagation of display settings between the host and uVMs. When a high-contrast display is now selected on the host, this setting will now also be used in uVMs.
64957	Customer Fix	Fixed issue with JPG image files created on Android systems. These files would not render in the Windows Photo Viewer because of a damaged ICC profile metadata in the source files. Local copies of these files are now created with corrected metadata, and these local copies display correctly.
68335	New Feature	Fixed an issue when attempting to attach a malicious file to an email. The expected warning pop-up window now appears correctly.
80389	Customer Fix	Resolves an issue where changing the audio settings for a suspended VM fails.
80525	Customer Fix	Fixed issue caused by Adobe's unified Reader/Pro installer. Untrusted PDFs now open correctly inside an instance of Adobe Reader in a VM.
81111	Customer Fix	Fixed issue where downloaded Excel files were Trusted in error. This only affected SCE customers that added Teams and an ingress application.
81377 81508	Security Update	Updated Secure Browser. This now respects the Chrome Group Policy settings *RequireOnlineRevocationChecksForLocalAnchors* and *EnableOnlineRevocationCheck* in both trusted and untrusted pages, so that handling of certificate revocation is always the same as in upstream Chromium.
81583	Bug Fix	Updates the Secure Browser to ensure hyphenation is displayed correctly.
81618	Customer Fix	Fixed issue where the SCE Outlook Add-In did not start automatically.
82070	Customer Fix	Resolves an issue where accessible archive files were blocked from opening.
82071	Customer Fix	Fixed issue where an Untrusted file became Trusted in error after it was relocated.
82539	New Feature	Resolves an issue where Threat Containment failed to initialize.
82662	Update	HP Sure Click Enterprise now requires .NET 4.7.2, which is shipped with all HP Sure Click Enterprise-supported versions of Windows 10.
82737	Performance Improvement	Improved memory usage on machines running Sure Click in Windows Hypervisor Platform (WHP) mode when the machine is low on memory.
82954	Customer Fix	Added a fallback method of configuring the guest network. This is required when network-related PowerShell cmdlets are broken.

Reference	Type	Description
83101	Customer Fix	Fixed issue with endpoint reinitialization caused in rare cases by a major Windows update.
83200	Customer Fix	Resolves an issue where an Adobe Reader update caused the Adobe Reader app to fail to virtualize.
83564	Update	Updated file housekeeping. Windows app packs that are no longer required on an endpoint are uninstalled automatically when the endpoint is rebooted.
83960	Customer Fix	Fixed issue when opening, attaching or sharing Office files over email.
84031	Customer Fix	Fixed issue where untrusted links received through Outlook did not redirect to the Secure Browser.
84162	Customer Fix	Fixed issue where links sent to the Secure Browser would not load.
84794	Threat Classification Update	Fixed an issue arising from a Chrome update to prevent False Positive threat alerts from being raised.
84861	Security	Upgrade Secure Browser to support Chrome 122. Includes updates for various third-party components to mitigate known vulnerabilities: CVE-2024-0808, CVE-2024-0809, CVE-2024-0810, CVE-2024-0811, CVE-2024-0814, CVE-2024-1077, CVE-2024-1675, CVE-2024-2400, CVE-2023-6508, CVE-2023-6509, CVE-2023-6510, CVE-2023-6511, CVE-2023-6512, CVE-2023-6702, CVE-2023-6703, CVE-2023-6704, CVE-2023-6705, CVE-2023-6706, CVE-2023-6707, CVE-2023-7024, CVE-2024-0222, CVE-2024-0223, CVE-2024-0224, CVE-2024-0225, CVE-2024-0333
84865	New Feature	Updated Secure Browser to support the following Chrome group policies: *HttpsOnlyMode*, *HttpsUpgradesEnabled*, *HttpAllowlist*, and *InsecureContentAllowedForUrls*. These policies control the HTTP-HTTPS upgrade behavior in an enterprise setting.
84933	Fix	Fixed an issue arising from an Acrobat Reader update. This prevents a 'New look' popup to be displayed in Untrusted PDF VMs.

Changes in HP Sure Click Enterprise 4.4 Release 5

Bug Fixes and Reported Issues since Release 4

Reference	Type	Description
77139	Platform	Remove support for Windows 20H2, OS Build 19042 (EOL May 2023).
77383	Improvement	Updated HP Secure Browser Firefox support to Firefox ESR 115.
77917	Improvement	Updated HP Secure Browser to Chrome 120.
78192	Customer Fix	Resolved an issue where a threat was detected if Firefox opened many MSEDGE instances.
78530	Customer Fix	Resolved an issue where an untrusted PDF viewed in the Secure Browser only printed in black/white and not full color.
80616	Customer Fix	Resolved an issue where a document with corrupted metadata was not able to have its isolation protection removed.
80725	Locale Support	Added support for Korean, Simplified Chinese and Taiwanese languages inside the isolated micro-vms.
81940	New Feature	Added support for Windows 11 23H2.
82490	Customer Fix	Resolved an issue where a management action concerning a missing Widevine component is missing, in error.
82490	Customer Fix	Resolved an issue where the endpoint would report that “WidevineCDM component is missing” until the second initialization.
83155	Improvement	Added support for AMDs new Threadripper CPUs.
83200	Customer Fix	Updated the Adobe Reader support to include new files required to initialize.
83960	Customer Fix	Resolved an issue where an updated version of Outlook created an additional attachment with Bromium_MAPI.
82108 81644	Customer Fix	Resolved a customer issue where loading the HP Sure Click Outlook plug-in caused Outlook to crash in certain situations.

Changes in HP Sure Click Enterprise 4.4 Release 4

Bug Fixes and Reported Issues since Release 3

Reference	Type	Description
73711	Customer Fix	Resolved an issue where initialization could fail if 32bit Acrobat Reader, or Microsoft Office was installed.
77913	Platform Update	Support for Office 2016 has been re-instated in this version.
78675	Secure Browser	HP Secure Browser has been updated to Chrome 116.
80092	Customer Fix	HP Software Update Service will always be upgraded when the Sure Click Enterprise installer is used. Previously it might not upgrade if not required.
80890	New Feature	The endpoint will now raise a new management action on the controller when an incompatible version of Outlook is installed.
80953	Customer Fix	Resolved an issue where some customers saw initialization issues showing “SECOND_BOOT_POWER_ON_FAILURE”.

Changes in HP Sure Click Enterprise 4.4 Release 3

Bug Fixes and Reported Issues since Release 2

Reference	Type	Description
64546	Improvement	Improved UX when r-click and 'remove protection' is invoked on a file that would be auto-trusted by default if double-clicked on.
68608	Customer Feature	Added the ability to unzip all compressed files as untrusted (rather than remove protection). Added the ability to remove protection from a folder structure (perhaps created by the unzip operation above) in Windows File Explorer.
72339	Customer Fix	Untrusted PDFs will now correctly ask for a PIN when signing from within the isolated application and using a certificate that requires a PIN.
73310	Customer Fix	Copying and pasting an untrusted file attachment from outlook into OneNote is now correctly blocked. Previously, dragging a dropping an untrusted file from outlook into OneNote was correctly blocked but copying and pasting the same file from outlook into OneNote was incorrectly being allowed.
75128	Firefox Security Update	Firefox fix for CVE-2018-25032.
75764	Improvement	Allow applications like Teams, which are configured as "Ingress Applications" to honor the Trusted Download Sites list.
77911	Improvement	HP Secure Browser is now updated to Chromium 114.
77962	Customer Fix	Powershell ISE and Powershell Core (pwsh.exe) are now prevented from accessing untrusted files. This blocks their use for creating trusted copies of untrusted files.
78148	Customer Fix	BrGuestSvr.exe crashes when removing protection in certain circumstances.
78220	Customer Fix	Users are now able to select a large number of untrusted documents and print successfully in one action.
78322	Customer Fix	Resolved an issue where renaming a file in a save-as dialog in HP Secure Browser could remove the isolation protection from the file.
78675	Customer Fix	Unable to copy/paste a mix of untrusted & trusted files into Outlook email.
78953	Improvement	Added untrusted support for the following languages: ar-SA, bg-BG, cs-CZ, el-GR, et-EE, he-IL, hr-HR, lt-LT, lv-LV, ro-RO, sk-SK, sl-SI, sr-Latn-RS, th-TH, tr-TR, and uk-UA.
79202	Improvement	Office version info is now displayed in the 'System Information' box on the desktop console.

Reference	Type	Description
79420	Improvement	Add support for workstation with >1TB of memory.
79444	Customer Fix	Fixes an issue where the "SCE has not been added to Defender exclusions" warning is seen even when an advanced config that should suppress this message has been set.
79551	Chrome Security Updates	Chrome fixes for CVE-2023-2725, CVE-2023-2930, CVE-2023-2940, CVE-2023-3079.
79713 79465	Improvement	This resolves an issue where the configuration to "Trust on Ingress" does not apply to sites on the trusted sites list for the HP Secure Browser.
79887	Improvement	Resolves an issue where the configuration to "Trust on Ingress" does not apply to sites on the trusted sites list for the HP Secure Browser.
80014	Fix	Resolved an issue that stopped a user being allowed to insert an image file into an untrusted word document.
80092	Improvement	Sure Click will now always upgrade the Software Update Service to the latest version on upgrade.
80230	Improvement	Printing is now faster from untrusted documents due to an improvement in this subsystem.

Changes in HP Sure Click Enterprise 4.4 Release 2

Bug Fixes and Reported Issues since Release 1

Reference	Type	Description
62908	Improvement	Significant performance improvement on low memory machines by allowing micro-VMs to size according to available memory.
74244	Fixed	Fixed an issue where printing an untrusted document could fail in some circumstances.
75117	Secure Browser Fix	Fixed an issue when scanning a QR code in the Secure Browser and it doesn't autofill a webform.
76747	Fixed	Removed all dependencies on Internet Explorer 11.
77791	Fixed	Resolved an issue where a file behaves as untrusted when attached in new email in outlook by dragging and dropping.

Changes in HP Wolf Security Controller 4.4.177

Bug Fixes and Reported Issues since the last On-Prem Controller release

Reference	Type	Description
66900	UI Updates	Added a missing Sure Sense Icon into the Threats UI. This was previously missing for events such as 'Behavioral Protection'.
75872	Customer Fix	Moved the "Permit users to disable HP Wolf Security Features" to the "General" tab.
75920	Feature Update	Updated the Device Properties tab to include the Windows edition as the Operating System Product name.
76290	Security Updates	The HP Wolf Controller now disables logins on a growing time delay when incorrect credentials are used. This blocks robots and scripts from brute forcing logins.
76298	Security Updates	Updated security so that Controller passwords must now be NIST/NCSC compliant.
76917	UI Updates	Corrected the category for the 'Corrupted local group policy...' management action. It is now set to 'Environmental', which aligns with the documentation.
76917	Customer Fix	Corrected the category for the 'Corrupted local group policy...' management action. It is now set to 'Environmental', which aligns with the documentation.
77577	Improvements	The Wolf Pro Security Controller welcome page has been updated to use the latest designs from HP.
77608	Improvements	Added a new remote command to reset the software channel update status on any given endpoint. This will allow it to retry the software update service.
77743	Improvements	Added two new management actions for software update failures which will be visible in the dashboard.
78232	Upgrades	To upgrade from a Controller build older than 4.2.87, you cannot go straight to the latest release (4.4.177). Instead, you must first upgrade to a build between 4.2.87 and 4.4.155 inclusive. You can then upgrade to 4.4.177.
78401	Improvements	Added some addition configuration options to allow HP Wolf Security to be disabled should it be installed on a system with known incompatible 3rd party software.
78521	New Management Actions	Added new 'FirmwareFeatures' management actions to report items for administrator consideration.
78939	Customer Fix	Resolved an issue which could see Management Actions listed twice in the dashboard and Management Actions pages.
78989	Customer Fix	Isolation status colors have been restored on the Devices table.

Reference	Type	Description
79020	Improvements	When clicking through to view Management actions, devices can now be grouped and remote commands send, directly from the Management Actions page.
79184	Customer Fix	Resolved an issue that stopped users navigating back to the HP Security Portal from the controller.
79470	Improvements	Updated the built-in 'Trust Microsoft Office 365' policy with the latest Microsoft URLs.
79732	New Feature	Updates tenant settings with new customer data collection. Business/personal use must now be provided. For business use, address details and a company name must be provided. For both business/personal use contact information must be provided. A toast appears linking to the settings page if this information has not been provided.
79832	Improvements	WPS default policy updated such that WPS Controller users have the disable-on-conflict feature **off** by default but have the ability to change the settings themselves.
80001	New Management Action	Added a management action to communicate when the Google Widevine DRM library is no available for the HP Secure Browser to show DRM content.
80197	Fix	Resolved an issue where endpoints from South Africa could report management actions in French.
80270	Improvements	Fixed an issue where on-prem controllers might not be able to see Fullscreen controller health graphs.
80450	Security Updates	Updated various third-party components to mitigate known vulnerabilities. CVE-2023-38325.
80706	Security Updates	Updated various third-party components to mitigate known vulnerabilities. CVE-2023-2602, CVE-2023-35945, CVE-2023-37920, CVE-2017-10784, CVE-2023-36617
81106	New Management Action	Added a management action to communicate when the unsupported MS Outlook BETA is in use and not protected by isolation.
81176	Fix	Updated the navigation from the 'Device Security Dashboard'. Now, when the 'Sure Click' bar in the 'Deployment Status' section is clicked, the main dashboard displays a filtered device list.
81188	UI Updates	Updated several HP Security Controller pages for working with management actions.
81342	UI Updates	Updated the 'Device Properties' tab. This now includes the status for GPU hardware rendering.

Reference	Type	Description
81363	Customer Feature	Added support for Manufacturer and Model properties for devices: • The Devices table now includes the device Manufacturer and Model, which can be used for sorting of devices. • The detailed Device view now includes the device Manufacturer and Model. • It is now possible to create an automatically-synchronized group based on Manufacturer or Model rules.
81728	Security Updates	Updated various third-party components to mitigate known vulnerabilities. ALAS-2023-2249, ALAS-2023-2257, ALAS-2023-2259, GHSA-v8qr-m533-qhj9, CVE-2022-48174 CVE-2023-38039
81960	UI Updates	Renamed 'Device Security' in the in the navigation bar and page title. These now read 'Device Management'. These are both localized into all supported languages.
81977	New Feature	Added Zoom and Teams links to the allowed protocols for the WPS default policy.
81980	Policy Updates	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
81980	Policy Updates	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
82063	Security Updates	Updated various third-party components to mitigate known vulnerabilities. ALAS-2023-2271, ALAS-2023-2280, ALAS2-2023-2312, ALASSELINUX-NG-2023-001, CVE-2023-44487
82360	Customer Fix	On the Devices page, the Filter now has a maximum text length of 4000 characters.
82487	Updated Policies	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
82566	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS2-2023-2320, ALAS2-2023-2321, ALAS2-2023-2330, CVE-2023-28154, CVE-2023-41164, CVE-2023-43665, CVE-2023-46695, CVE-2023-5363
82716	New Feature	Updated the permissions for WPS Customer Administrators and Partner Administrators. They can now remotely reset the channel state on endpoint devices.
82958	UI Updates	On the Devices page, the Filter now has a maximum text length of 3900 characters.
83012	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2023-2350, ALAS-2023-2351, ALAS-2023-2357, ALAS-2023-2369, CVE-2023-49083, CVE-2023-5678

Reference	Type	Description
83012	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2023-2350, ALAS-2023-2351, ALAS-2023-2357, ALAS-2023-2369, CVE-2023-5678, CVE-2023-49083
83210	Updated Policies	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
83300	UI Updates	Updated the color coding of status indicators so that grey is not used in error.
83360	Localization Updates	Replaced a single appearance of Japanese characters in the French translation of Policy pages.
83590	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2380, ALAS-2024-2385, ALAS-2024-2400, ALAS-2024-2412, CVE-2023-52323
83600	New Feature	Added support for TPM version and TPM model for devices. These appear in device details alongside CPU and GPU, and can be used to evaluate compatibility.
83920	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2419, CVE-2023-6129, CVE-2023-6237, CVE-2024-0727
83976	Feature Updates	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
84188	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2442, CVE-2023-52071, CVE-2024-0853, GHSA-3ww4-qq4f-jr7f, GHSA-xxj9-f6rv-m3x4
84190	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2442, CVE-2023-52071, CVE-2024-0853, GHSA-3ww4-qq4f-jr7f, GHSA-xxj9-f6rv-m3x4
84276	Security Updates	Updated various third-party components to mitigate known vulnerabilities: GHSA-3ww4-qq4f-jr7fv, GHSA-9v9h-cqj8-h64p
84465	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2456, GHSA-6vqw-3v5j-54x4
84607	Customer Fix	Updated reporting. The result documents are now parsed to identity the malware analysis and file. Those are then added to the Stix report.
84807	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2478, ALAS-2024-2479, ALAS-2024-2487, ALAS-2024-2490

Reference	Type	Description
85182	Security Updates	Updated various third-party components to mitigate known vulnerability: GHSA-vmqv-47j8-qwv8
85302	Enhancements	Updated the HP Supplied Policy 'Trust Microsoft Office 365'. It now includes the latest set of URLs from Microsoft.
85619	Security Updates	Updated various third-party components to mitigate known vulnerability: GHSA-67hx-6x53-jw92
85945	Security Updates	Updated various third-party components to mitigate known vulnerabilities: CVE-2024-2511, ALAS-2024-2512, ALAS-2024-2519, GHSA-2m57-hf25-phqg, GHSA-v5h6-c2hv-hv3r, GHSA-w3h3-4rj7-4ph4
85966	Security Updates	Updated various third-party components to mitigate known vulnerability: GHSA-mr82-8j83-vxmv
86095	Security Updates	Updated various third-party components to mitigate known vulnerabilities: ALAS-2024-2521, ALAS-2024-2523, ALAS-2024-2526
87408	Security Updates	Updated various third-party components to mitigate known vulnerabilities: CVE-2023-42364, CVE-2023-42365
81344 81345	Feature Updates	Added support for GPU properties for devices: • The Devices table now includes the device GPU Device and GPU Driver properties, which can be used for sorting of devices. • The detailed Device view now includes the GPU property. Hovering over the GPU property shows full details for the GPU. • It is now possible to create an automatically-synchronized group based on GPU Device or GPU Driver.
86689 85962	Security Updates	Updated various third-party components to mitigate known vulnerabilities: CVE-2023-42363, CVE-2023-42364, CVE-2023-42365, CVE-2023-42366, GHSA-2qr8-3wc7-xhj3, GHSA-6c5p-j8vq-pqhj, GHSA-9wx4-h78v-vm56, GHSA-cjwg-qfpm-7377, GHSA-vq3r-rm7w-2xqh

Getting Help

If you have questions that are not covered in the documentation, please contact HP Support:

- Visit https://enterprisesecurity.hp.com
  If you need an account, please contact your Account Executive or Customer Support
- Email questions to: enterprise.support@hpwolf.com
- Call HP Enterprise Security Customer Support at 1-800-518-0845
- Call your technical account representative directly

Document History

1.0	Release version.
1.1	Added Release 8 Update 1

ADDENDUM #1 – Sure Click Enterprise Fixed Lifecycle Policy

HP Wolf Security Fixed Lifecycle Policy

https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL

In this article:

- Fixed Life Cycle Policy
- Lifecycle phases for products under the Fixed Lifecycle Policy
- Mainstream Support
- Beyond End-of-Life Support
- Requirements and Limitations
- Sure Click Enterprise Fixed Life Cycle Policy
- HP Secure Browser Fixed Life Cycle Policy
- FAQ

Fixed Life Cycle Policy

The Fixed Lifecycle Policy applies to the Wolf Security Software products currently available from HP. A Fixed Life Cycle policy provides a defined support and servicing Lifecycle timeline at the time of product launch for all software updates.

To be eligible for support, customers are required to deploy the latest update.

HP is committed to providing products with improved security. Although we strive to remove vulnerabilities during development, software vulnerabilities remain a fact today and we must be prepared to respond when they are discovered. HP advises customers to install the latest product releases, security updates, and app packs to remain as secure as possible as soon as they are available. Older products may not meet today's demanding security requirements or provide the same degree of protection or functionality. HP may be unable to provide security updates for older products.

The Fixed Lifecycle Policy applies to all products unless stated otherwise. Product-specific support and servicing dates are available at the end of this article.

Lifecycle phases for products under the Fixed Lifecycle Policy

Type of support	Mainstream Support	Beyond End of Life
Incident support	Available	Limited
Request to change product design and features	Available	Not Available
Security updates	Available	Not Available
Non-security updates	Available	Not Available
Self-help support [1]	Available	Available

[1] Self-Help Online Support is available throughout a product's lifecycle and for a minimum of 12 months after the product reaches the end of its support. HP online Knowledge Base articles, FAQs, troubleshooting tools, documentation and other resources, are provided to help customers resolve common issues

Mainstream Support

Mainstream Support is the first phase of the product lifecycle. At the supported update version, Mainstream Support for products and services includes:

- Incident support
    - HP will work with customers to analyze, understand, and root cause issues with the Product.
    - Product fixes, when required, will be scheduled for inclusion in a future update.
        - HP does not commit to releasing a fix in the next available update.
        - HP will assess the criticality of a reported issue and schedule it in an appropriate release in line with other planned changes.
- Security update support
- The ability to request product feature enhancements (RFEs).
    - Note: Non-security enhancements will be reviewed and considered in line with future product roadmaps. HP makes no commitment to adding support for submitted RFEs or if considered when support may be added. If a non-security RFE is approved, it will be added to a future release. It will be required that Customers will update to a newer update to receive the non-security update.

Note: Enrolment in a maintenance program may be required to receive these benefits for certain products.

Beyond End-of-Life Support

This phase follows Mainstream Support. At the supported software update level beyond End-of-Life Support for products and services includes:

- Self-help support
- Limited commercially reasonable efforts incident support [2]

Note:

- HP will not accept requests for warranty support, non-security product enhancements, design changes, or new features during the Beyond End-of-Life phase.
- Enrolment in a paid support program may be required to receive these benefits for certain products.

[2] Limited complimentary support may be available (varies by product and requires the customer to have a valid support entitlement).

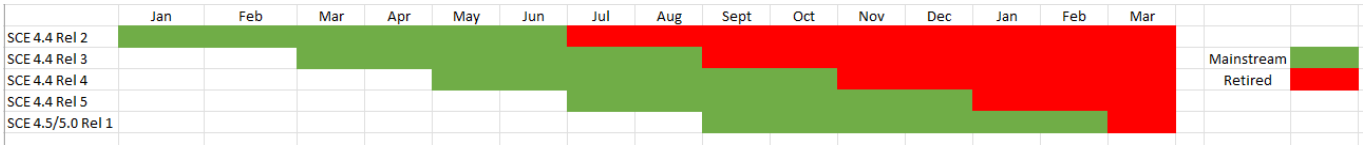
Requirements and Limitations

HP reserves the right to deprecate features, functionality, platform, and operating system support when releasing new minor or major versions of Products (and AppPacks). Whenever feasible, HP endeavors to give advance notice when discontinuing support for specific features, functionality, platform, or operating systems. In cases where advance notice is viable, the deprecation announcement will be made in the release preceding its removal.

Note: In some cases deprecating a version or a feature will be entirely dependent on 3rd party depreciation events.

Sure Click Enterprise Fixed Life Cycle Policy

Sure Click Enterprise releases will have a Mainstream support period of 6 months from their release. Following their mainstream support period, support for the release will end and the release will be considered end of life. It is expected that customers plan to upgrade their devices at least every 6 months. This will ensure your devices stay as secure as possible.



HP Secure Browser Fixed Life Cycle Policy

HP Secure Browser utilizes Google Chromium “Extended Stable” releases designed for enterprise customers and OEM partners. As such, Secure Browser releases will be based on even-numbered Chromium releases to maintain compatibility and security updates for our customers. A Secure Browser AppPack will be released approximately every 10 weeks based on the current Google schedule.

Mainstream support is provided for the current shipping release of Secure Browser. Once a new release of Secure Browser is released, the previous version immediately moves to end of life.

FAQ

How am I supported if I'm NOT on the latest release, but it is not End of Life yet?

- The product is supported, but customers will be expected to replicate any reported issue on the current GA version of the software in their environment.
- If an issue is resolved on the current GA version of the software, customers will be advised to upgrade to the version that already contains a fix for the reported issue. The Product team will conduct root cause analysis on the version currently in use, even if it’s not the currently shipping version of the product. As part of this analysis, the customer may be required to upgrade to a more recent version to assist the analysis.
- Product fixes, when required, will be scheduled for inclusion in a future update. HP does not commit to releasing a fix in the next available update. HP will assess the criticality of a fix and schedule it in an appropriate release in line with other planned changes.

How am I supported if I am on a version which is End of Life and I have a valid software subscription or support and maintenance agreement?

- HP understands that at times a customer may be limited to running End of Life software due to compatibility or environmental reasons. In these situations, HP may provide limited commercial reasonable efforts to support these devices.

- Customers can still submit support incidents and they will be assessed.
    - If an issue is known and there is an option to mitigate this, it will be provided.
    - If an issue is unknown and further investigation is needed, a customer may be asked to upgrade to a supported release to confirm if the issue has been resolved in a subsequent release or to collect additional troubleshooting data. If they are unable to upgrade to a newer release, it may stall the progression of the ticket.
- There will be no additional updates End of Life software releases (this includes but is not limited to Secure Browser updates and new OS support).
- In the event of a breaking issue, for example, a third-party update breaks existing compatibility or introduces a new issue, and this issue cannot be mitigated using configuration options, mitigations could be limited to disabling features, disabling the software or uninstalling the software.