



HP Sure Click Enterprise 4.4 Release 1

4.4.1.571

Table of Contents

Notices	4
Introduction	5
Sure Click Enterprise Requirements.....	6
Additional Isolation Requirements	7
Supported Browsers	7
Supported Software.....	8
Supported Languages	11
On Prem HP Wolf Security Controller 4.4.139.....	12
Controller Requirements.....	12
Supported Browsers.....	12
SQL Database Requirements	13
On Prem and Cloud Hosted HP Wolf Security Controller	14
Supported Languages	14
End of Sale (EOS) / End of Life (EOL) Updates.....	14
Sure Click Enterprise 4.4 Updates.....	15
Isolation Support for Google Chrome version 106.....	15
Microsoft Internet Explorer 11	15
Microsoft Windows Operating System Support.....	15
Microsoft Windows LTSC Support	16
Initial installation.....	16
Featured Updates	17
Unified HP Wolf Security Desktop Console	17
HP Secure Browser Audio Conferencing Support.....	19
Updated Allow List Guidance For Thirdparty Interoperability	20
HP Wolf Security Controller	20
Limitations	21
General	21
Web Browsing with Chrome	22
Web Browsing with Firefox	22
Documents.....	22
Controller	22
HP Sure Click Enterprise 4.4 End of Life (EOL) Dates.....	23
Deprecated Features and Platforms	24
New Changes in the HP Sure Click Enterprise 4.4 Release 1	25
BugFixes and Reported Issues.....	25
Additional Features and Changes	25

New Changes in HP Wolf Security Controller 4.4.139	26
<i>BugFixes and Reported Issues since HP Wolf Security Controller 4.3.125</i>	26
<i>Additional Features and Changes since HP Wolf Security Controller 4.3.125</i>	27
Getting Help.....	28
Document History	29

Notices

Copyright © 2023 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The software and accompanying written materials are protected by U.S. and International copyright law. Unauthorized copying of the software, including software that has been modified, merged, or included with other software, or other written material is expressly forbidden. This software is provided under the terms of a license between HP and the recipient, and its use is subject to the terms of that license.

Recipient may be held legally responsible for any copyright infringement that is caused or incurred by recipient's failure to abide by the terms of the license agreement. US GOVERNMENT RIGHTS: Terms and Conditions Applicable to Federal Governmental End Users. The software and documentation are "commercial items" as that term is defined at FAR 2.101. Please refer to the license agreement between HP and the recipient for additional terms regarding U.S. Government Rights.

The software and services described in this manual may be protected by one or more U.S. and International patents.

DISCLAIMER: HP makes no representations or warranties with respect to the contents or use of this publication. Further, HP reserves the right to revise this publication and to make changes in its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Intel® Virtualization Technology, Intel® Xeon® processor 5600 series, Intel® Xeon® processor E7 family, and the Intel® Itanium® processor 9300 series are the property of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Adobe and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

10th January 2023

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.
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 Sure Click Enterprise 4.4 includes Windows 11 support. 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 <code>msiexec</code> to install Sure Click Enterprise remotely, ensure you include the <code>SERVERURL</code> setting, otherwise installation will fail.	

Required Software for Installation

- Microsoft .NET Framework 4.5
- Microsoft .NET Framework 4.6.2 (pre-installed with Windows 10 Anniversary Edition)
- 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 Isolation Requirements

HP Sure Click Enterprise installation requires the following:

- An HP Wolf Security Controller, either on-prem, or an HP cloud hosted instance.
- 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

- Sure Click Secure Browsing Extension for Chrome supports the latest Google-recommended version of Google Chrome
- Sure Click Secure Browsing Extension for Firefox supports the latest Mozilla-recommended version of Firefox (ESR or non-ESR, 64-bit only)
- Sure Click Secure Browsing Extension for Edge supports the latest version of the Microsoft Edge Chromium browser only

Sure Click Chrome Isolation is supported with an N-1 policy such that the current shipping version, and the previous version of the Chrome AppPack are supported. 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>

Sure Click Firefox Isolation supports Mozilla Firefox ESR (64-bit) release 102 only. Please view the HP Product Knowledge base for updated and tested versions of the Firefox releases.

Supported Software

- Microsoft Office 2013 Service Pack 1, Click-to-Run x64/x86:

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

(Please Note: Office 2013 support will be dropped in the next release of HP Sure Click Enterprise)

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

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

(Please Note: Office 2016 support will be dropped in the next release of HP Sure Click Enterprise)

- 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

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: MSI versions of Office are only supported for 2013, 2016 and 2019

Retail Licensing – Standard & ProPlus (32bit & 64bit)

Volume Licensing – Standard & ProPlus (32bit & 64bit)

- Adobe Acrobat Reader versions: DC 2017, 2018, 2019, 2020, 2021, 2022
- Windows Media Player 12 (32-bit and 64-bit)
- Oracle Java 8 (32-bit)
- 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 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 1903 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: Sure Click Enterprise previously required vPro chipsets supporting Intel VMCS Shadowing, a feature that improves performance of hypervisors running nested virtual machines by reducing nesting-induced VM exits. Version 4.1.4 introduced support for Intel-based chipsets without this technology. 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.

Limitations of support 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 2212 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 4.3.
- Windows Defender Credential Guard
- 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.

HP recommend excluding HP Sure Click related directories from scans performed by third-party security products. If a product does not support exclusions at the directory level, exclusions should instead be created for all associated executables. To create exclusions, refer to your third-party product documentation.

The absence of exclusions will result in performance related issues, failed Sure Click Enterprise initialization and slow or blocked browsing and opening of isolated documents. Refer to the [Configure Exclusions and Whitelisting for Third-Party Security Software](#) KB article for additional information.

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)
- Dutch (nl-NL)
- * Danish (da-DK)
- English US (en-US)
- English UK (en-GB)
- * Finnish (fi-FL)
- French (fr-FR)
- French Canadian (fr-CA)
- German (de-DE)
- * Hungarian (hu-HU)
- Italian (it-IT)
- Japanese (ja-JP)
- * Norwegian (nb-NO)
- * Polish (pl-PL)
- Portuguese (pt-PT)
- Spanish (es-ES)
- Swedish (sv-SE)

Note: HP Sure Click Enterprise supports all Windows locales. If your locale is not listed above, you will need to deploy the full English language pack (LpCab) to use Sure Click. The English Local Experience pack (LXP) is not supported.

On Prem HP Wolf Security Controller 4.4.139

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.

Controller 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 to the controller.
Internet	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/Bromium-Threat-Intelligence-Cloud-Service for more information
Operating System	Windows Server 2012, Windows Server 2012 R2, 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)

Supported Browsers

The Controller web interface is supported on the latest versions of Edge Chromium, Chrome, and Firefox. Internet Explorer 11 is not supported for viewing the HP Wolf Security Controller.

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+ 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

On Prem and Cloud Hosted HP Wolf Security Controller

Supported Languages

With version 4.4.139, 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:



End of Sale (EOS) / End of Life (EOL) Updates

Per HP Sure Click Enterprise EOL policy (<https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL>), EOL is the process of discontinuing sales, support and maintenance for a specific version of the Product.

EOS means that product can be used, but customers are expected to try to replicate any reported issue on the latest version of the software. Any fixes released will be applicable to the latest version only and code fixes will not be applied to any version that is already EOS or EOL. Code fixes and patches will only be released for the latest GA versions.

Updates to the End-of-Life Policy triggered by 4.4 Release 1 are show below:

HP Sure Click 4.4

No changes – initial 4.4 release

Sure Click Enterprise 4.4 Updates

Isolation Support for Google Chrome version 106

HP Sure Click Enterprise 4.4 supports Google Chrome version 106 when using the HP Secure Browser.

From HP Sure Click 4.3, HP announced it will only support even numbered Chrome releases, in accordance with the Google Enterprise/OEM roadmap and EOL policy.

Microsoft Internet Explorer 11

In previous versions of Sure Click Enterprise 4.3, HP announced that it would drop support for the IE browser completely in Sure Click Enterprise 4.4.

As such, with the initial release of Sure Click Enterprise 4.4, no versions of Microsoft Internet Explorer are supported and the browser is considered EOL.

Microsoft Windows Operating System Support

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 (1) 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>

(* denotes support stopped in this release)

(** denotes support will be stopped in the next release)

Supported:

- Windows 11 Version 22H2 – OS Build 22621
- Windows 11 Version 21H2 – OS Build 22000
- Windows 10 Version 22H2 – OS Build 19045
- Windows 10 Version 21H2 – OS Build 19044
- Windows 10 Version 20H2 – OS Build 19042
- Windows 10 Version 1809 – OS Build 17763
 - NB: LTSC version supported on Secunet SINA Workstations only

Not supported:

- Windows 7 (x86 & x64)
- Windows 8.1 (x86 & x64)
- Windows 10 Version 1607 – OS Build 14393 – Redstone 1
- Windows 10 Version 1507 – OS Build 10240 – Threshold 1
- Windows 10 Version 1511 – OS Build 10586 – Threshold 2
- Windows 10 Version 1703 – OS Build 15063 – Redstone 3

- Windows 10 Version 1709 - OS Build 16299 – Redstone 4
- Windows 10 Version 1803 - (OS Build 17134) - Redstone 4
- Windows 10 Version 19H1 - 1903 OS Build 18362
- Windows 10 Version 19H2 – OS Build 18363
- Windows 10 Version 20H1 – OS Build 19041
- Windows 10 Version 21H1 – OS Build 19043*

Microsoft Windows LTSC Support

In line with Microsoft's updated recommendations for LTSC use (<https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview>), HP will be deprecating support for LTS releases. Sure Click Enterprise will however maintain support for the standard enterprise support dates. Please see the Windows support knowledge base article for up-to-date information: <https://enterprisesecurity.hp.com/s/article/Windows-Support-Policy>

Initial installation

By default, the initial installation of the endpoint software will result in the software being disabled and unconfigured. As a result, the endpoint must connect to an HP Wolf Security Controller to receive its configuration and license which may happen during installation (at the prompt or using msixec parameters) or post-installation using the "brmanage" command: *"brmanage management-server <controller name>"*.

Until the endpoint receives a license, the software will remain in a disabled state. Once the endpoint has been correctly configured to communicate with a controller, it will receive a license and initial configuration via policy. At this point, the endpoint software will initialize and will then be available for use (unless marked explicitly as disabled).

This allows the administration team to roll out the endpoint software onto all endpoints in a benign state. The administrator is then able to move devices into Device Groups to receive their license and configuration. An admin can now see the entire endpoint estate with enabled/disabled devices in one simple view. This allows customers to complete a single rollout, but phased enablement of software as all disabled devices will appear in the controller.

Featured Updates

Unified HP Wolf Security Desktop Console

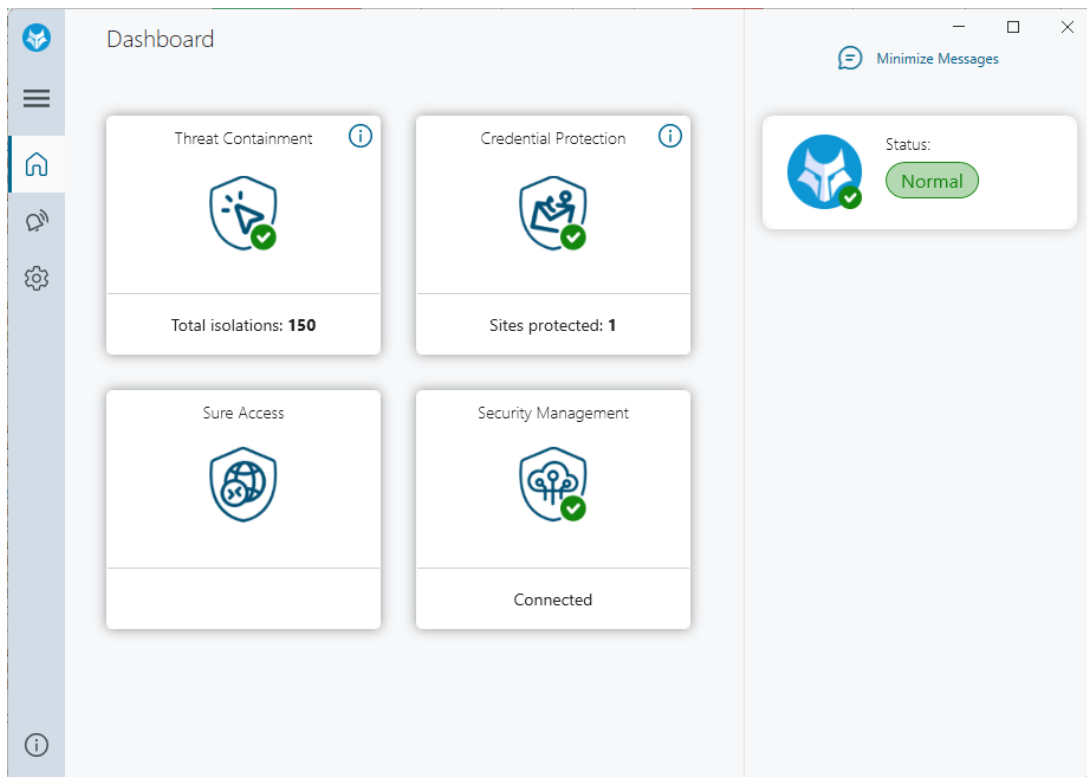
With the introduction of Sure Click Enterprise 4.4, HP brings a new, updated, unified and modern end user UI to Sure Click. This brings the endpoint UI inline with that of other HP Wolf Security products, such as Wolf Pro Security, or Wolf Security for Business.

All the previous features of the 4.3 and older Desktop Console are still there but may be in different places in the UI.

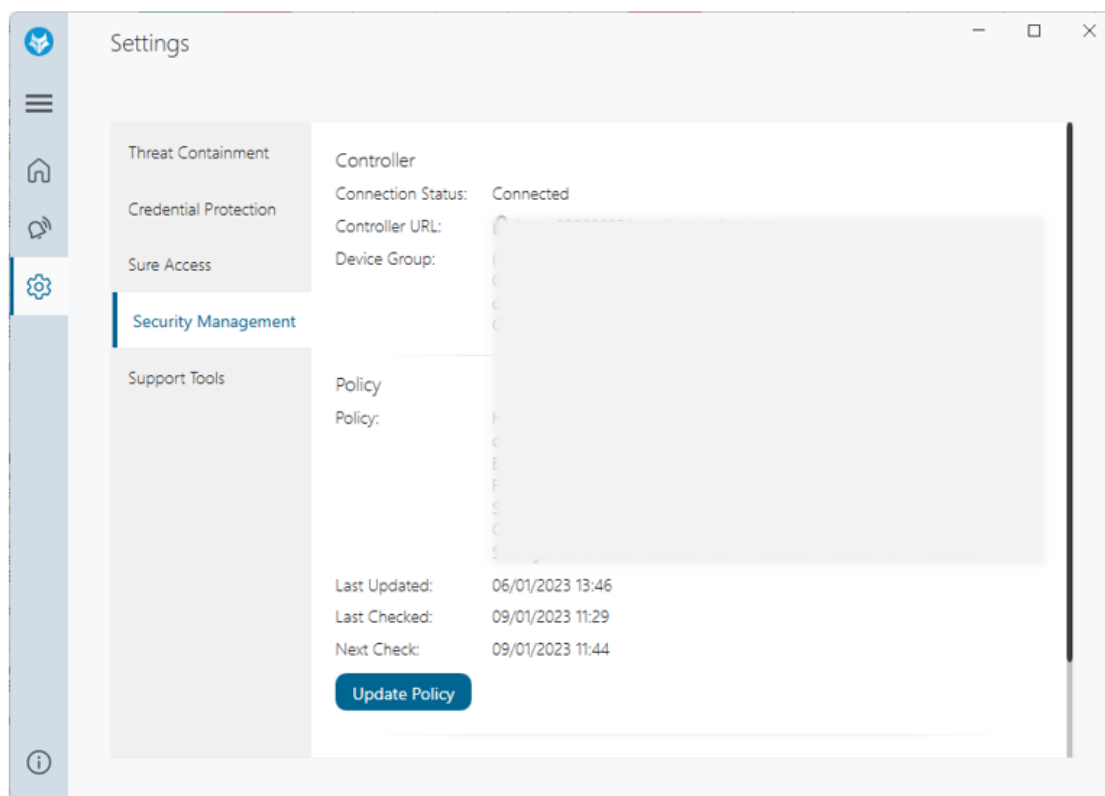
The new HP Wolf Security Desktop Console is installed as a new binary on the system. This means that shortcuts or pinned links to the older 4.3 Desktop Console are no longer valid and Windows may well draw an empty icon here. This is expected and is how windows deals with dead links. To resolve this, you can simply remove the old pinned link or shortcut and replace it when a new pinned link when the new HP Wolf Security Desktop Console is launched. You can still launch this via the Windows Start menu, or by the HP Wolf icon in the systray:



The HP Wolf Desktop Console is dynamic and will represent known installed HP Wolf Security Products with tiles on the main view. In the example below, both Sure Click Enterprise (Threat Containment, Credential Protection and Security Management) and Sure Access Enterprise are installed, hence seeing the 4 tiles shown below.



To view system details, as per the old version of Desktop Console, click on the cog icon on the left and then navigate through the features to see the new representation of the data in the HP Wolf Security Desktop Console:



All of the previous functionality of the old Desktop Console is supported by the new console on HP Sure Click Enterprise 4.4.

With the change in updated user experience there are some changes to the product installation and packages. These make no difference to the operation of the product, and the change in architecture here allows future features to be supported on the platform for customer benefit in a future release. associated executables.

Additional changes include updates in the Add/Remove programs listing which you may see if you programmatically access this list. Whereas previously there would be only one entry of “HP Sure Click Enterprise”, there are now 3, one for each of the product areas. This allows easier updating, simpler product delivery and a more robust architecture for customers. The additional lines in Add/Remove programs are as shown below:

 HP Wolf Security	HP Inc.
 HP Wolf Security - Console	HP Inc.
 HP Security Update Service	HP Inc.

The new HP Wolf Security Desktop Console will automatically replace the old console on an upgrade from 4.x to a 4.4 version.

If you want to manually uninstall the packages, they should be uninstalled in the following order:

- 1 - HP Wolf Security
- 2 - HP Wolf Security – Console
- 3 - HP Security Update Service

HP Secure Browser Audio Conferencing Support

HP Sure Click 4.4 introduces the ability to join an audio conference from inside a hardware isolated micro-vm using the HP Secure Browser. This feature allows end users to participate in audio conferences without requiring 3rd party installers to be used or present on the system.

This feature is only supported in the HP Secure Browser when running Chrome 106 and above (included in 4.4 Release 1).

This feature only supports the audio portion of the conference. Webcams are not supported in this version. Desktop or application sharing is not supported due to security concerns. Hardware Isolated Micro-VMs do not have access to the host computer desktop as this is a hard security boundary within the HP Sure Click Security architecture to stop anything potentially malicious within a micro-VM accessing real user data, network or applications.

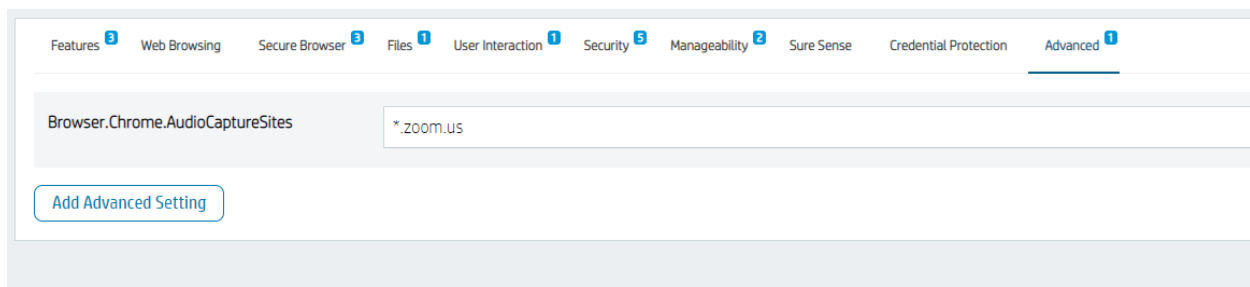
Supported Audio Conferencing Web Applications:

- Jitsi Meet
- Teams
- Zoom

HP Sure Click Enterprise normally blocks access to a media capture device or screen share in the HP Secure Browser. This is to prevent any potential unauthorized use of your microphone, camera, or monitoring of your screen. The HP Secure Browser provides a greater level of protection than a standard browser via microVM's. The web page runs completely isolated from the rest of your machine so that no malicious content can enable a media capture device and monitor you without your knowledge.

CONFIGURATION OPTIONS

Microphone access can only be enabled via the HP Wolf Security Controller. Navigate to the advanced section in your controller policy and add a new advanced parameter named: **Browser.Chrome.AudioCaptureSites** then set the required URL as the value. The example in the screenshot below shows the configuration for microphone support in Zoom:



For security reasons, it is recommended you only apply this setting using a limited delta policy to users that require audio conferencing access. Further details on this feature can be seen in the knowledge base:

<https://enterprisesecurity.hp.com/s/article/HP-Sure-Click-has-blocked-access-to-a-media-capture-device-in-the-HP-Secure-Browser>

Updated Allow List Guidance For Third-party Interoperability

HP recommend excluding HP Sure Click related directories from scans performed by third-party security products. If a product does not support exclusions at the directory level, exclusions should instead be created for all associated executables. HP Sure Click Enterprise 4.4 includes additional executables and directories that should be excluded from third-party security products. Please refer to the [Configure Exclusions and Whitelisting for Third-Party Security Software](#) KB article for our best practice recommendations.

HP Wolf Security Controller

The Wolf Security Controller for 4.4 Release 1 has been updated to include the latest 4.4.139.230 build. Changes, fixed, features and updates for this new controller release can be seen later on in these release notes. HP recommends updating the controller and will maintain backward compatibility between the 4.4 version of the Controller and previous supported versions of the Sure Click software.

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 an upcoming 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.
- If you are using RDP to access a physical system, you may not be able to interact with the Sure Click Enterprise Desktop Console, Download Manager or Live View because they are "transparent." To resolve this issue, install .NET 4.0 on the endpoint.
- Saving to and opening untrusted documents from the cloud is not supported for Office 2013/ 2016 / 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://www.verizonmedia.com/policies/ie/en/verizonmedia/privacy/topics/adserving/index.html>
- Microsoft Edge's support for Microsoft Defender Application Guard does not include extensions which use native messaging (see MS link : <https://docs.microsoft.com/en-us/deployedge/microsoft-edge-security-windows-defender-application-guard#my-extension-doesnt-seem-to-work-in-edge-application-guard>).
 - This means that the 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.

Web Browsing with Chrome

- Skype extension is not supported

Web Browsing with 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.

Documents

- Isolation prevents users from opening any isolated files that cannot be opened by one of the supported applications. If a downloaded file is not currently supported but is known to be trustworthy, right-click the file and select the “Remove Protection” file menu option.

Note: This operation may require administrative access.

- Sure Click Enterprise isolates documents from accessing corporate resources or files stored on the desktop or intranet. As a result, if a document open 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 containing more than 214 characters.

Controller

- The controller continues to display 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 4.4 End of Life (EOL) Dates

Versions are classified as follows:

- Major Version [DOT] Minor Version [DOT] Update version. (e.g. 4.4.1)

Product Support Policy

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

Product Name	Release Date	EOS Date	EOL Date	Status
HP Sure Click Enterprise 4.4 Release 1 (4.4.1.571)	10 th Jan 2023 (Initial Release)			GA / Current

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

We are deprecating older platforms and features 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.

Specific examples of removed platforms are Microsoft Windows 7, Microsoft Internet Explorer and all x86 platforms.

The latest information regarding deprecated features and platforms:

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

New Changes in the HP Sure Click Enterprise 4.4 Release 1

BugFixes and Reported Issues

Fixed	75589	Resolved an issue where a double title bar could be seen on some untrusted PDF files opened in a micro-vm
Fixed	73048	Fixed a customer reported issue where an incompatibility caused some native, legacy MS IE 11 applications to not work.
Fixed	74507 72326	Resolved an interoperability issue between Microsoft Outlook and Sure Click Enterprise that could cause the "HP Sure Click Outlook Add-in is disabled" management action to show when it shouldn't.
Fixed	70002	HP resolved a reported security vulnerability for a potential privilege escalation
Fixed	69450	Resolved a customer issue pertaining to reporting whether a version of an AppPack was active or not to a controller.

Additional Features and Changes

None	Initial Release of 4.4 platform
------	---------------------------------

New Changes in HP Wolf Security Controller 4.4.139

BugFixes and Reported Issues since HP Wolf Security Controller 4.3.125

Fixed	60038	Updated some areas of the UI which showed Management Actions where tooltips were previously missing, so they now show tooltips on the coloured icon.
Fixed	74196	It is now significantly faster exporting CSV files from large tables in the Controller UI
Fixed	73654	When using Sure Access Enterprise, Memory Protection is set ON by default now. Previously this was OFF.
Fixed	73297	When using Sure Access Enterprise and creating initial Application Definitions (AppDefs), the built in certificate was use to validate but not to sign the AppDefs. This has now been updated to sign the AppDefs by default, providing additional security and Application validation on the endpoint.
Fixed	41586	On the device information page, the version of Chromium is now displayed alongside the AppPack version number.
Fixed	71761	Administrators are now able to slide and hide the left menu on the Controller based on preferences. This can be controlled by the 'hamburger' menu (top right) and the user preferences. A mouse-over will restore the menu to full width to use the menu.
Fixed	65558	If a customer is using the HP Threat Intelligence services to automatically classify and tag threats, this has been expanded. When a file hash is marked as True Positive, it is now expanded to all threats which contain the same hash will now automatically be labelled the same. Same rules apply to Unknown or False Positive. This provides greater coverage for automatic threat classification and improves FP/TP notifications.
Fixed	70014	Improved report layout and pagination when printing to PDF from the Controller Malware→Reports area

Additional Features and Changes since HP Wolf Security Controller 4.3.125

Update	Updated fonts across the controller UI to be in line with HP guidelines and products.
Update	Improve UI spacing and readability where lists of versions and counts might be too close together in dashboards
Update	When creating a new policy, customers will only now see one option, rather than previously being able to create a "base" or "delta" policy. This single option can be used to create either types of policy but the default is a delta policy.
Update	Customers are now able to great device groups based on the version of active and/or installed AppPacks.
Update	Remote-commands have been updated to allow the uninstall of a specific version of an AppPack, rather than all installed versions.
Update	Controllers now have an addition Remote Command to allow endpoints to connect to a different controller without requiring access to the endpoint.
Update	The "Microsoft Office 365" built in policy has been updated with the latest URLs from Microsoft.
Update	The HP Supplied Policy 'Trust Microsoft Office 365' has been updated to the latest set of URLs from Microsoft.
Update	Resolved an issue where multiple Resultant Set of Policy windows could be launched causing UI confusion
Feature	Syslog and Email destinations for events can now be split using specific permissions. This means they each appear under their own navigation menu on the Events tab depending on the user permissions granted.
Feature	If a device is configured to receive software updates from the HP Cloud Service, customers will be able to see status with an additional UI that has been added to the Device page. A new tab called "Channel Status" will provide status and health information pertaining to updates and software delivered using the update channel.
Feature	Add Controller localization support for Italian, Dutch, Swedish and Portuguese and Brazilian
Feature	Added the ability to select the threat component when generating the Threat Report
BETA Feature	Provisional support for the Controller API – Please contact your HP Support or Account team for more information pertaining to this BETA.

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

0.1	Initial version
-----	-----------------