# HP Sure Access Enterprise

## 8.0 Q2 2022 RELEASE

# Table of Contents

# Notices



13th July 2022

# Introduction

The Release Notes cover the HP Sure Access Enterprise 8.0.125  product release, and subsequent updates, providing information about new functionality and the requirements for Sure Access Enterprise.

## Sure Access Enterprise Requirements

Sure Access Enterprise requires that Sure Click Enterprise is installed in order to function. Sure Access Enterprise uses the HP Wolf Security core virtualization engine from Sure Click and so the core requirements are the same.

If you already have Sure Click Enterprise installed and a controller deployed, you can move ahead to the specific chapter on installing Sure Access Enterprise on top of Sure Click Enterprise.

Sure Access Enterprise has the following hardware and software requirements for this release:

| Hardware or Software | Description |
|---|---|
| CPU/Bios/Features | • Intel Core i5+, 6th generation minimum<br>  • AMD and Intel XEON CPUs are currently not supported<br>• VT-x is required and needs to be enabled<br>• Both vPro and non-vPro versions are supported<br>  • vPro is recommended<br>• UEFI firmware required<br>  • Secure Boot needs to be enabled with the Microsoft 3rd Party UEFI CA permitted<br>  • TCG EFI Protocol and Platform Specification Version 1.2 (minimum) is required<br>• TPM 2.0<br>• IOMMU (Intel VT-d) is recommended<br>• NB: Sure Access Enterprise automatically disables hibernation on the host and hides this capability from the host operating system. This is to maintain security integrity of the solution |
| Memory | Minimum: 8 GB RAM<br><br>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.<br><br>As a baseline, HP recommends that a typical Windows 10/11 64-bit device has 1800 MB available memory prior to installation. |
| Disk | 8 GB free disk space |
| Operating System | Microsoft Windows versions are supported as documented in the HP Sure Access Enterprise Windows Support policy:<br>https://enterprisesecurity.hp.com/s/article/Windows-Support-Policy<br>You must ensure that HP Sure Access 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.<br>The HP Sure Access Enterprise EOL policy can also be referenced here:<br>https://enterprisesecurity.hp.com/s/article/Product-Support-and-End-of-Life-Policy-EOL |

## Additional hardware support

Keyboard protection support:

- PS/2
- USB 1.1+ devices connected via xHCI USB controller are supported

Docking station support

- USB 3+ docking stations are supported
- No support for Thunderbolt 3+ docking stations

## Required Software for Installation

HP Sure Click Enterprise 4.3

- At the time of release the supported version is Sure Click Enterprise 4.3.11.45.
  Please note that this release of Sure Access Enterprise will not work with Release 1 of Sure Click Enterprise (4.3.7.346).
  Please check updated release notes or with support for the latest supported version.
- Please review the Sure Click Enterprise 4.3 Release Notes for its requirements.

## Additional Requirements

HP Sure Access Enterprise installation requires the following:

- Local administrator privileges (if installing on specific machines for evaluation)
- Active Directory administrator privileges (if installing in the enterprise for production use)
- A valid Sure Access Enterprise license, provided by your HP Sales or Customer Support representative.
- Sure Click Enterprise to be installed.  NB This is a technical requirement and does not require a valid Sure Click license, only the binary to be installed.

## Supported Languages

HP Sure Access Enterprise endpoint software supports the following languages on the specified version of Windows:

- Brazilian Portuguese (pt-BR)
- Dutch (nl-NL)
- English US (en-US)
- English UK (en-GB)
- French (fr-FR)
- French Canadian (fr-CA)
- German (de-DE)
- Italian (it-IT)
- Japanese (ja-JP)
    - No IME support in this release
- Portuguese (pt-PT)
- Spanish (es-ES)
- Swedish (sv-SE)

**Note:** HP Sure Access Enterprise supports all Windows locales. If your locale is not listed above, you will need to deploy an English language pack to use Sure Access Enterprise.

# HP Wolf Security Controller

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

If you already have an HP Wolf Security Controller deployed as part of an HP Sure Click Enterprise deployment, you can skip ahead to the chapter on installing Sure Access Enterprise on top of an existing Sure Click deployment.

**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 |
| Memory | 16 GB RAM |
| Software | Microsoft IIS 7.5+ with CGI module, IIS Manager, static content, and anonymous authentication installed<br>.NET 4 Extended (server) |
| SSL | Valid SSL certificate trusted by endpoints<br>(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 2012 SP4+<br>SQL Server 2014 SP3+<br>SQL Server 2016 SP2+<br>SQL Server 2017+<br>SQL Server 2019+<br>Standard and Enterprise editions are supported<br>Server Management Studio (SSMS) as the management suite for the controller database<br>SQL Express should be used in a limited test or evaluation environment only |
| Storage Space | 1 TB available space |

## Supported Languages

With version 4.3.125, 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:

## Additional Controller Information

- If you have a HP cloud hosted Wolf Security Controller and plan on using your own certificate authority to sign the application definitions, please do not upload your certificates. Contact your account team or HP support representative for further information.
    - When using a cloud hosted HP Wolf Security Controller, it is recommended to only use the self-signed certificate for application definitions
- Customers with On-prem controllers can import the certificates to the controller as this uses the windows certificate store to securely store the certificate for signing the application definitions
    - On-prem controllers can use both a self-signed certificate and an uploaded customer certificate to sign the application definitions.

## Installing Sure Access Enterprise

- You do not require a valid license for HP Sure Click Enterprise, unless you are installing Sure Access Enterprise on top of an existing Sure Click deployment.
- If you are installing Sure Access Enterprise as a fresh deployment, you should have been given a Sure Access Enterprise license with your evaluation or purchase.

1. Sure Click Enterprise should be deployed in accordance with the Deployment Guide found on the documentation website Product Documentation
2. The Sure Access Enterprise MSI can be deployed with the Sure Click MSI using SCCM or can be installed after. The Sure Access Enterprise MSI can be deployed in the following ways
    a. Using the "Remote Install" remote command from the controller to push the MSI to the targeted endpoints
    b. Installing the MSI manually on supported endpoints
    c. Installing the MSI via SCCM or other Microsoft supported delivery mechanism to deploy MSI files to endpoints in your organization.
3. Once endpoint software is deployed and connected to the controller, make sure the HP Wolf Security Controller has been configured to support the Sure Access Enterprise product release. If you do not see the "Sure Access Enterprise" navigation item on the Controller menu, please contact your HP Technical account team or customer support for assistance.

## Initial configuration

- In order to use Sure Access Enterprise, the virtualization engine must be initialized correctly depending on use. There are two built in polices on the controller to help with this step.
    - If you are using Sure Access Enterprise combined with Sure Click Enterprise malware isolation product, then you should only use the “Sure Access Enterprise” built in policy on top of your existing Sure Click policies for the endpoints using both products. This will allow both Sure Click and Sure Access Enterprise to function together.
    - If you are using Sure Access Enterprise without using Sure Click functionality, then you should apply the “Sure Access Enterprise (standalone)” policy to the built in “All Devices” group. This will ensure the virtualization environment is configured correctly for Sure Access Enterprise use.
    - If you are unsure about any of the built-in policies, please contact your HP Enterprise account team or Customer Support team for assistance.

## Intel and AMD 'RetBleed' Vulnerabilities

On July 12th 2022, Intel and AMD disclosed design vulnerabilities in certain CPUs from both companies. These vulnerabilities were named "RetBleed". HP has worked with both vendors to make sure that this release of HP Sure Click Enterprise contains the recommended mitigations for both CPU types.

CVEs and CVS scores for the published vulnerabilities mitigated in this release:

| CVE ID | CVS 3.0 | Vector | VendorID |
|---|---|---|---|
| CVE2022-23816 | 5.6 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N | AMD-SB-1037 |
| CVE-2022-23825 | 5.6 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N | AMD-SB-1037 |
| CVE-2022-28693 | 4.7 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N | INTEL-SA-00707 |
| CVE-2022-29901 | 4.7 | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N | INTEL-SA-00702 |

The HP bulletin relating to the vulnerabilities can be found here:
https://support.hp.com/us-en/document/ish_6545619-6545663-16

All versions of HP Sure Click Enterprise prior to 4.3.11.45 are un-mitigated, and customers are recommended to upgrade as soon as they are able. Please contact your HP account or support team for advice on this if required.

# 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/

The overall HP Sure Access Enterprise Windows support policy:
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 10 Version 21H2 – (OS Build 19044)
- Windows 10 Version 21H1 – (OS Build 19043)
- Windows 10 Version 20H2 – (OS Build 19042)
- Windows 10 Version 19H2 – (OS Build 18363) **

### Preview Support

- Windows 11 Version 21H2 – (OS Build 22000)
    - This will be fully supported in an upcoming release.

### Not supported:

- Windows 7 (x86 & x64)
- Windows 8.1 (x86 & x64)
- Windows 10 Version 1507 - (OS Build 10240) –Threshold 1
- Windows 10 Version 1511 - (OS Build 10586) – Threshold 2
- Windows 10 Version 1607 - (OS Build 14393) – Redstone 1
- Windows 10 Version 1703 - (OS Build 15063) - Redstone 2
- Windows 10 Version 1709 - (OS Build 16299) - Redstone 3
- Windows 10 Version 1803 - (OS Build 17134) – Redstone 4
- Windows 10 Version 1809 – (OS Build 17763) – Redstone 5
- Windows 10 Version 1903 - (OS Build 18362) – 19H1
- Windows 10 Version 20H1 – (OS Build 19041) – 20H1

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

- Per HP Sure Access 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.
- Sure Access Enterprise supports an N-1 support policy. Once a new version is announced GA, the previous version will automatically become EOS. 3 months after being EOS, versions will become EOL.

## Deprecated Features and Platforms

- As HP deprecate older platforms and features from the latest versions of HP Sure Access 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

## 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